Network Vulnerability Scanner Report

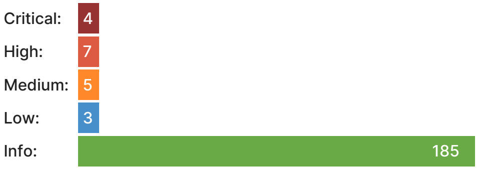
✓ pentest-ground.com

Summary

Overall risk level:

Critical

Risk ratings:



Scan information:

Start time:	May 20, 2025 / 18:26:05 UTC+03
Finish time:	May 20, 2025 / 21:20:23 UTC+03
Scan duration:	2 hrs, 54 min, 18 sec
Tests performed:	204/204
Scan status:	Finished

Findings

Redis - Remote Code Execution (CVE-2022-0543)

port 6379/tcp

CONFIRMED

We managed to detect this vulnerability by evaluating the payload that contains the `id` command:
eval 'local io_l = package.loadlib("/usr/lib/x86_64-linux-gnu/liblua5.1.so.0", "luaopen_io"); local io = io_l(); local f = io.popen("id", "r"); local res = f:read("*a"); f:close(); return res' 0

Data received:
uid=0(root) gid=0(root) groups=0(root)

Details

Vulnerability description:
We found that the target server is vulnerable to CVE-2022-0543, a Remote Code Execution vulnerability in the Redis caching service. The root cause of this vulnerability consists in an unexpected sandbox escape on Debian systems because of the dynamically load of the Lua interpreter. Therefore, an unauthenticated remote attacker can connect to the Redis service, evaluate a library load and execute shell commands.
We have detected this vulnerability by connecting to the Redis service, loading `liblua5.1.so.0` library, executing `id` command and reading the command response from the output.

Risk description:
The risk exists that a remote unauthenticated attacker can fully compromise the server in order to steal confidential information, install ransomware or pivot to the internal network.

Recommendation:
We recommend upgrading the Redis service to a version equal to or higher than 5:5.0.14-1+deb10u2 for the oldstable version, or 5:5.0.14-1+deb10u2 for the stable distribution.

References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0543
https://nvd.nist.gov/vuln/detail/CVE-2022-0543

Classification:
CVE : CVE-2022-0543
CVSS : 10
CVSS V3 : 10

Oracle Weblogic - Remote Code Execution (CVE-2018-2894)

port 7001/tcp

CONFIRMED

We managed to detect this vulnerability using the following request, by extracting the current user using the whoami/id command:
HTTP Request:
GET /ws_utc/css/config/keystore/1747755188723_dhveihjhrebrbhy.jsp HTTP/1.1
Host: pentest-ground.com
HTTP Response:
HTTP 200
oracle

Details

Vulnerability description:

We found that the target server is vulnerable to CVE-2018-2894, a Remote Code Execution vulnerability, affecting the Oracle Weblogic server.
This vulnerability is affecting the WLS subcomponent because the path of `/ws_utc/config.do` is reachable without authentication, meaning that the Weblogic server is in the development mode. The attacker can set a new Work Home Directory which needs to be writable and then upload JKS Keystores, which are Java Server Pages (JSP) files. Uploading a webshell as a JKS, the attacker can successfully achieve Remote Code Execution on the server.
We have detected this vulnerability by changing the Work Home Directory to a writable one sending an HTTP POST request, then uploading the webshell as a command interpreter with an HTTP POST request, and finally sending an HTTP GET request to the webshell to read the command response from the output.

Risk description:

The risk exists that a remote unauthenticated attacker can fully compromise the server in order to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:

We recommend upgrading the Oracle Weblogic to the latest version.

References:

https://nvd.nist.gov/vuln/detail/cve-2018-2894
https://www.oracle.com/security-alerts/cpujul2018.html

Classification:

CVE : CVE-2018-2894
CVSS : 7.5
CVSS V3 : 9.8

DVWA Default Login

CONFIRMED

port 4280/tcp

We managed to detect that the target server is set up with a default credential pair.
We extracted the following information from the target: **https://pentest-ground.com:4280/index.php**

Username: **"admin"**
Password: **"password"**

Details

Vulnerability description:

Damn Vulnerable Web App (DVWA) is a test application for security professionals. The hard coded credentials are part of a security testing scenario.

Risk description:

The risk exist that a remote attacker could take advantage of the default credentials for taking over the default account. If an authenticated vulnerability is present on the machine, it could also be leveraged to exploit the target, compromising the underlying system.

Recommendation:

Change the default login credentials. Use a strong password, at least 10 characters long, preferably randomly generated. Unless the login panel is intended to be exposed to the internet, we strongly recommend placing it behind a firewall.

References:

https://opensourcelibs.com/lib/dvwa

Oracle WebLogic Server - Remote Code Execution (CVE-2020-2551)

CONFIRMED

port 7001/tcp

We managed to detect this vulnerability using the following Request / Response chain.
Endpoint: **https://pentest-ground.com:7001/console/login/LoginForm.jsp**

Details

Vulnerability description:

Oracle WebLogic Server (Oracle Fusion Middleware (component: WLS Core Components) is susceptible to a remote code execution vulnerability. Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 2.2.1.3.0 and 12.2.1.4.0. This easily exploitable vulnerability could allow unauthenticated attackers with network access via IIOP to compromise Oracle WebLogic Server.

Risk description:

The risk exists that a remote unauthenticated attacker can fully compromise the server to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:

Apply the latest security patches provided by Oracle to mitigate this vulnerability.

References:

https://github.com/hktalent/CVE-2020-2551
https://nvd.nist.gov/vuln/detail/CVE-2020-2551
https://www.oracle.com/security-alerts/cpujan2020.html

https://github.com/neilzhang1/Chinese-Charts
https://github.com/pjgmonteiro/Pentest-tools

Classification:

CVE : CVE-2020-2551
CVSS V3 : 9.8

Oracle WebLogic - Remote Code Execution (CVE-2023-21839)

CONFIRMED

port 7001/tcp

We managed to detect this vulnerability using GIOP protocol in Oracle Server by sending a payload containing **whoami** command:
Data received on handler
oracle

Details

Vulnerability description:

We found that the target server is vulnerable to CVE-2023-21839, a Remote Code Execution inside the Core component of Oracle WebLogic Server. The root cause of this vulnerability is an insecure deserialization via T3, IIOP protocol that could allow an unauthenticated attacker to take control of the server. The attacker can send a crafted JNDI/RMI malicious object in order to achieve access to the server. We have detected this vulnerability by sending a crafted RMI object to the server with whoami payload and fetching the server response that was sent to one of our loggers. We send the response to a logger because this is an Out-of-Band vulnerability, meaning that the output of the command is not reflected in the response.

Risk description:

The risk exists that a remote unauthenticated attacker can fully compromise the server in order to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:

We recommend upgrading the Oracle WebLogic to a version higher than 12.2.1.4.0 or 14.1.1.0.0 , which can be done from the administrator panel.

References:

https://nvd.nist.gov/vuln/detail/CVE-2023-21839
https://www.oracle.com/security-alerts/cpujan2023.html

Classification:

CVE : CVE-2023-21839
CVSS : 7
CVSS V3 : 7.5

Oracle Fusion Middleware WebLogic Server Administration Console - Remote Code Execution (CVE-2020-14883)

port 7001/tcp

CONFIRMED

We managed to detect this vulnerability using the following Request / Response chain.
Endpoint: **https://pentest-ground.com:7001/console/images/%252e%252e%252fconsole.portal**

Details

Vulnerability description:

The Oracle Fusion Middleware WebLogic Server admin console in versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0 is vulnerable to an easily exploitable vulnerability that allows high privileged attackers with network access via HTTP to compromise Oracle WebLogic Server.

Risk description:

The risk exists that a remote unauthenticated attacker can fully compromise the server to steal confidential information, install ransomware, or pivot to the internal network.

Recommendation:

Apply the necessary patches or updates provided by Oracle to mitigate this vulnerability.

References:

https://packetstormsecurity.com/files/160143/Oracle-WebLogic-Server-Administration-Console-Handle-Remote-Code-Execution.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14883
https://www.oracle.com/security-alerts/cpuoct2020.html
http://packetstormsecurity.com/files/160143/Oracle-WebLogic-Server-Administration-Console-Handle-Remote-Code-Execution.html
https://github.com/1n7erface/PocList

Classification:

CVE : CVE-2020-14883
CVSS V3 : 7.2

Redis - Default Logins

CONFIRMED

port 6379/tcp

We managed to detect that the target server is set up with a default credential pair.
We extracted the following information from the target: **pentest-ground.com:6379**
Authentication was performed without credentials.

Username: ""
Password: ""
Details

Vulnerability description:
Redis service was accessed with easily guessed credentials.

Risk description:
The risk exist that a remote attacker could take advantage of the default credentials for taking over the default account. If an authenticated vulnerability is present on the machine, it could also be leveraged to exploit the target, compromising the underlying system.

Recommendation:
Change the default login credentials. Use a strong password, at least 10 characters long, preferably randomly generated. Unless the login panel is intended to be exposed to the internet, we strongly recommend placing it behind a firewall.

Redis Server - Unauthenticated Access

CONFIRMED

port 6379/tcp

We managed to detect a Redis Server - Unauthenticated Access, using the following Request / Response chain.
Details

Vulnerability description:
Redis server without any required authentication was discovered.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://redis.io/topics/security

Classification:
CVSS V3 : 7.2

Vulnerabilities found for Redis Key-Value Store 5.0.7

UNCONFIRMED

port 6379/tcp

Risk level	CVSS	CVE	Summary	Exploit
●	9	CVE-2021-32762	Redis is an open source, in-memory database that persists on disk. The redis-cli command line tool and redis-sentinel service may be vulnerable to integer overflow when parsing specially crafted large multi-bulk network replies. This is a result of a vulnerability in the underlying hiredis library which does not perform an overflow check before calling the calloc() heap allocation function. This issue only impacts systems with heap allocators that do not perform their own overflow checks. Most modern systems do and are therefore not likely to be affected. Furthermore, by default redis-sentinel uses the jemalloc allocator which is also not vulnerable. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14.	N/A
●	7	CVE-2022-24834	Redis is an in-memory database that persists on disk. A specially crafted Lua script executing in Redis can trigger a heap overflow in the cjson library, and result with heap corruption and potentially remote code execution. The problem exists in all versions of Redis with Lua scripting support, starting from 2.6, and affects only authenticated and authorized users. The problem is fixed in versions 7.0.12, 6.2.13, and 6.0.20.	N/A

🟠	6.8	CVE-2022-24735	Redis is an in-memory database that persists on disk. By exploiting weaknesses in the Lua script execution environment, an attacker with access to Redis prior to version 7.0.0 or 6.2.7 can inject Lua code that will execute with the (potentially higher) privileges of another Redis user. The Lua script execution environment in Redis provides some measures that prevent a script from creating side effects that persist and can affect the execution of the same, or different script, at a later time. Several weaknesses of these measures have been publicly known for a long time, but they had no security impact as the Redis security model did not endorse the concept of users or privileges. With the introduction of ACLs in Redis 6.0, these weaknesses can be exploited by a less privileged users to inject Lua code that will execute at a later time, when a privileged user executes a Lua script. The problem is fixed in Redis versions 7.0.0 and 6.2.7. An additional workaround to mitigate this problem without patching the redis-server executable, if Lua scripting is not being used, is to block access to `SCRIPT LOAD` and `EVAL` commands using ACL rules.	N/A
🟠	6.5	CVE-2021-32626	Redis is an open source, in-memory database that persists on disk. In affected versions specially crafted Lua scripts executing in Redis can cause the heap-based Lua stack to be overflowed, due to incomplete checks for this condition. This can result with heap corruption and potentially remote code execution. This problem exists in all versions of Redis with Lua scripting support, starting from 2.6. The problem is fixed in versions 6.2.6, 6.0.16 and 5.0.14. For users unable to update an additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done using ACL to restrict EVAL and EVALSHA commands.	N/A
🟠	6.5	CVE-2021-21309	Redis is an open-source, in-memory database that persists on disk. In affected versions of Redis an integer overflow bug in 32-bit Redis version 4.0 or newer could be exploited to corrupt the heap and potentially result with remote code execution. Redis 4.0 or newer uses a configurable limit for the maximum supported bulk input size. By default, it is 512MB which is a safe value for all platforms. If the limit is significantly increased, receiving a large request from a client may trigger several integer overflow scenarios, which would result with buffer overflow and heap corruption. We believe this could in certain conditions be exploited for remote code execution. By default, authenticated Redis users have access to all configuration parameters and can therefore use the "CONFIG SET proto-max-bulk-len" to change the safe default, making the system vulnerable. **This problem only affects 32-bit Redis (on a 32-bit system, or as a 32-bit executable running on a 64-bit system).** The problem is fixed in version 6.2, and the fix is back ported to 6.0.11 and 5.0.11. Make sure you use one of these versions if you are running 32-bit Redis. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent clients from directly executing `CONFIG SET`: Using Redis 6.0 or newer, ACL configuration can be used to block the command. Using older versions, the `rename-command` configuration directive can be used to rename the command to a random string unknown to users, rendering it inaccessible. Please note that this workaround may have an additional impact on users or operational systems that expect `CONFIG SET` to behave in certain ways.	N/A
🟠	6	CVE-2021-32627	Redis is an open source, in-memory database that persists on disk. In affected versions an integer overflow bug in Redis can be exploited to corrupt the heap and potentially result with remote code execution. The vulnerability involves changing the default proto-max-bulk-len and client-query-buffer-limit configuration parameters to very large values and constructing specially crafted very large stream elements. The problem is fixed in Redis 6.2.6, 6.0.16 and 5.0.14. For users unable to upgrade an additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the proto-max-bulk-len configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command.	N/A
🟠	6	CVE-2021-32628	Redis is an open source, in-memory database that persists on disk. An integer overflow bug in the ziplist data structure used by all versions of Redis can be exploited to corrupt the heap and potentially result with remote code execution. The vulnerability involves modifying the default ziplist configuration parameters (hash-max-ziplist-entries, hash-max-ziplist-value, zset-max-ziplist-entries or zset-max-ziplist-value) to a very large value, and then constructing specially crafted commands to create very large ziplists. The problem is fixed in Redis versions 6.2.6, 6.0.16, 5.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the above configuration parameters. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command.	N/A
🟠	6	CVE-2021-32687	Redis is an open source, in-memory database that persists on disk. An integer overflow bug affecting all versions of Redis can be exploited to corrupt the heap and potentially be used to leak arbitrary contents of the heap or trigger remote code execution. The vulnerability involves changing the default set-max-intset-entries configuration parameter to a very large value and constructing specially crafted commands to manipulate sets. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the set-max-intset-entries configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command.	N/A

●	6	CVE-2021-41099	Redis is an open source, in-memory database that persists on disk. An integer overflow bug in the underlying string library can be used to corrupt the heap and potentially result with denial of service or remote code execution. The vulnerability involves changing the default proto-max-bulk-len configuration parameter to a very large value and constructing specially crafted network payloads or commands. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from modifying the proto-max-bulk-len configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command.	N/A
●	6	CVE-2021-32761	Redis is an in-memory database that persists on disk. A vulnerability involving out-of-bounds read and integer overflow to buffer overflow exists starting with version 2.2 and prior to versions 5.0.13, 6.0.15, and 6.2.5. On 32-bit systems, Redis `*BIT*` command are vulnerable to integer overflow that can potentially be exploited to corrupt the heap, leak arbitrary heap contents or trigger remote code execution. The vulnerability involves changing the default `proto-max-bulk-len` configuration parameter to a very large value and constructing specially crafted commands bit commands. This problem only affects Redis on 32-bit platforms, or compiled as a 32-bit binary. Redis versions 5.0.`3m 6.0.15, and 6.2.5 contain patches for this issue. An additional workaround to mitigate the problem without patching the `redis-server` executable is to prevent users from modifying the `proto-max-bulk-len` configuration parameter. This can be done using ACL to restrict unprivileged users from using the CONFIG SET command.	N/A
●	5.9	CVE-2021-31294	Redis before 6cbea7d allows a replica to cause an assertion failure in a primary server by sending a non-administrative command (specifically, a SET command). NOTE: this was fixed for Redis 6.2.x and 7.x in 2021. Versions before 6.2 were not intended to have safety guarantees related to this.	N/A
●	5.5	CVE-2022-36021	Redis is an in-memory database that persists on disk. Authenticated users can use string matching commands (like `SCAN` or `KEYS`) with a specially crafted pattern to trigger a denial-of-service attack on Redis, causing it to hang and consume 100% CPU time. The problem is fixed in Redis versions 6.0.18, 6.2.11, 7.0.9.	N/A
●	5.5	CVE-2023-25155	Redis is an in-memory database that persists on disk. Authenticated users issuing specially crafted `SRANDMEMBER`, `ZRANDMEMBER`, and `HRANDFIELD` commands can trigger an integer overflow, resulting in a runtime assertion and termination of the Redis server process. This problem affects all Redis versions. Patches were released in Redis version(s) 6.0.18, 6.2.11 and 7.0.9.	N/A
●	5.5	CVE-2023-28856	Redis is an open source, in-memory database that persists on disk. Authenticated users can use the `HINCRBYFLOAT` command to create an invalid hash field that will crash Redis on access in affected versions. This issue has been addressed in in versions 7.0.11, 6.2.12, and 6.0.19. Users are advised to upgrade. There are no known workarounds for this issue.	N/A
●	5	CVE-2021-32675	Redis is an open source, in-memory database that persists on disk. When parsing an incoming Redis Standard Protocol (RESP) request, Redis allocates memory according to user-specified values which determine the number of elements (in the multi-bulk header) and size of each element (in the bulk header). An attacker delivering specially crafted requests over multiple connections can cause the server to allocate significant amount of memory. Because the same parsing mechanism is used to handle authentication requests, this vulnerability can also be exploited by unauthenticated users. The problem is fixed in Redis versions 6.2.6, 6.0.16 and 5.0.14. An additional workaround to mitigate this problem without patching the redis-server executable is to block access to prevent unauthenticated users from connecting to Redis. This can be done in different ways: Using network access control tools like firewalls, iptables, security groups, etc. or Enabling TLS and requiring users to authenticate using client side certificates.	N/A
●	5	CVE-2015-8080	Integer overflow in the getnum function in lua_struct.c in Redis 2.8.x before 2.8.24 and 3.0.x before 3.0.6 allows context-dependent attackers with permission to run Lua code in a Redis session to cause a denial of service (memory corruption and application crash) or possibly bypass intended sandbox restrictions via a large number, which triggers a stack-based buffer overflow.	N/A
●	5	CVE-2021-3470	A heap overflow issue was found in Redis in versions before 5.0.10, before 6.0.9 and before 6.2.0 when using a heap allocator other than jemalloc or glibc's malloc, leading to potential out of bound write or process crash. Effectively this flaw does not affect the vast majority of users, who use jemalloc or glibc malloc.	N/A
●	5	CVE-2020-21468	A segmentation fault in the redis-server component of Redis 5.0.7 leads to a denial of service (DOS). NOTE: the vendor cannot reproduce this issue in a released version, such as 5.0.7	N/A
●	4	CVE-2021-32672	Redis is an open source, in-memory database that persists on disk. When using the Redis Lua Debugger, users can send malformed requests that cause the debugger’s protocol parser to read data beyond the actual buffer. This issue affects all versions of Redis with Lua debugging support (3.2 or newer). The problem is fixed in versions 6.2.6, 6.0.16 and 5.0.14.	N/A

●	4	CVE-2020-14147	An integer overflow in the getnum function in lua_struct.c in Redis before 6.0.3 allows context-dependent attackers with permission to run Lua code in a Redis session to cause a denial of service (memory corruption and application crash) or possibly bypass intended sandbox restrictions via a large number, which triggers a stack-based buffer overflow. NOTE: this issue exists because of a CVE-2015-8080 regression.	N/A
●	3.6	CVE-2023-45145	Redis is an in-memory database that persists on disk. On startup, Redis begins listening on a Unix socket before adjusting its permissions to the user-provided configuration. If a permissive umask(2) is used, this creates a race condition that enables, during a short period of time, another process to establish an otherwise unauthorized connection. This problem has existed since Redis 2.6.0-RC1. This issue has been addressed in Redis versions 7.2.2, 7.0.14 and 6.2.14. Users are advised to upgrade. For users unable to upgrade, it is possible to work around the problem by disabling Unix sockets, starting Redis with a restrictive umask, or storing the Unix socket file in a protected directory.	N/A
●	2.1	CVE-2022-24736	Redis is an in-memory database that persists on disk. Prior to versions 6.2.7 and 7.0.0, an attacker attempting to load a specially crafted Lua script can cause NULL pointer dereference which will result with a crash of the redis-server process. The problem is fixed in Redis versions 7.0.0 and 6.2.7. An additional workaround to mitigate this problem without patching the redis-server executable, if Lua scripting is not being used, is to block access to `SCRIPT LOAD` and `EVAL` commands using ACL rules.	N/A
●	1.8	CVE-2022-3647	** DISPUTED ** A vulnerability, which was classified as problematic, was found in Redis up to 6.2.7/7.0.5. Affected is the function sigsegvHandler of the file debug.c of the component Crash Report. The manipulation leads to denial of service. The complexity of an attack is rather high. The exploitability is told to be difficult. The real existence of this vulnerability is still doubted at the moment. Upgrading to version 6.2.8 and 7.0.6 is able to address this issue. The patch is identified as 0bf90d944313919eb8e63d3588bf63a367f020a3. It is recommended to apply a patch to fix this issue. VDB-211962 is the identifier assigned to this vulnerability. NOTE: The vendor claims that this is not a DoS because it applies to the crash logging mechanism which is triggered after a crash has occurred.	N/A

Details

Risk description:

These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one) for any of these vulnerabilities and use it to attack the system.

Notes:

- The vulnerabilities are identified based on the server's version.
- Only the first 30 vulnerabilities with the highest risk are shown for each port.

Since the vulnerabilities were discovered using only version-based testing, the risk level for this finding will not exceed "high" severity. Critical risks will be assigned to vulnerabilities identified through accurate active testing methods.

Recommendation:

We recommend you to upgrade the affected software to the latest version in order to eliminate the risks imposed by these vulnerabilities.

Classification:

CVE : CVE-2023-45145, CVE-2023-28856, CVE-2023-25155, CVE-2022-3647, CVE-2022-36021, CVE-2022-24834, CVE-2022-24736, CVE-2022-24735, CVE-2021-41099, CVE-2021-3470, CVE-2021-32762, CVE-2021-32761, CVE-2021-32687, CVE-2021-32675, CVE-2021-32672, CVE-2021-32628, CVE-2021-32627, CVE-2021-32626, CVE-2021-31294, CVE-2021-21309, CVE-2020-21468, CVE-2020-14147, CVE-2015-8080
CVSS V3 : 9

Redis Server No Password

port 6379/tcp

UNCONFIRMED

No evidence to display.

Details

Risk description:

The remote Redis server is not protected with a password.
It was possible to login without a password.
This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Recommendation:

Set password.

Classification:

CVSS : 7.5

Free Articles Directory RFI Vulnerability

port 4280/tcp

UNCONFIRMED

No evidence to display.

Details

Risk description:

Free Articles Directory is prone to a remote file include (RFI) vulnerability.
Free Articles Directory fails to sanitize user input to the 'page' parameter in index.php. An unauthenticated attacker may be able to read arbitrary local files or include a file from a remote host that contains commands which will be executed by the vulnerable script, subject to the privileges of the web server process.

Recommendation:

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

References:

http://archives.neohapsis.com/archives/bugtraq/2006-03/0396.html
http://www.securityfocus.com/bid/17183

Classification:

CVE : CVE-2006-1350
CVSS : 7.5

SSH service exposed to the Internet

port 4445/tcp

CONFIRMED

We managed to detect a publicly accessible SSH service.

```
Starting Nmap ( https://nmap.org ) at 2025-05-20 18:29 EEST
Nmap scan report for pentest-ground.com (178.79.134.182)
Host is up (0.013s latency).
rDNS record for 178.79.134.182: 178-79-134-182.ip.linodeusercontent.com

PORT     STATE SERVICE VERSION
4445/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u5 (protocol 2.0)
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
```

Details

Vulnerability description:

We found that the SSH service with username/password authentication is publicly accessible. Network administrators often use remote administration protocols to control devices like switches, routers, and other essential systems. However, allowing these services to be accessible via the Internet can increase security risks, creating potential opportunities for attacks on the organization.

Risk description:

Exposing this service online with username/password authentication can enable attackers to launch authentication attacks, like guessing login credentials, and potentially gaining unauthorized access. Vulnerabilities, such as unpatched software, protocol flaws, or backdoors could also be exploited. An example is the CVE-2024-3094 (XZ Utils Backdoor) vulnerability.

Recommendation:

We recommend turning off SSH with username/password authentication access over the Internet and instead using a Virtual Private Network (VPN) that mandates two-factor authentication (2FA). If the SSH service is essential for business purposes, we recommend limiting access only from designated IP addresses using a firewall. Furthermore, it is advisable to utilize SSH Public Key Authentication since it employs a key pair to verify the identity of a user or process.

Redis service exposed to the Internet

port 6379/tcp

CONFIRMED

We managed to detect a publicly accessible Redis service.

```
PORT STATE SERVICE VERSION
6379/tcp open redis Redis key-value store 5.0.7
```

Details

Vulnerability description:

We found that the Redis service is publicly accessible. This service often holds critical organizational data, making it a potential prime target for determined attackers.

Risk description:
The risk exists that an attacker exploits this issue by launching a password-based attack on the Redis service. If an attacker identifies a correct set of login details, they could gain access to the database and start enumerating, potentially revealing confidential information. Moreover, such vulnerabilities could lead to other forms of attacks, including privilege escalation, allowing attackers to run system commands and move laterally to other systems in the internal network.

Recommendation:
We recommend ensuring that the Redis service is not publicly accessible. The Redis service should be safeguarded behind a firewall or made available only to users connected through a Virtual Private Network (VPN) server. However, if the Redis service is required to be directly accessible over the Internet, we recommend reconfiguring it such that it is accessible only from known IP addresses.

Vulnerabilities found for jQuery 3.4.1

port 81/tcp

UNCONFIRMED

Risk level	CVSS	CVE	Summary	Exploit
●	4.3	CVE-2020-11023	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	N/A
●	4.3	CVE-2020-11022	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	N/A

Details

Risk description:
These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one) for any of these vulnerabilities and use it to attack the system.

Notes:

- The vulnerabilities are identified based on the server's version.
- Only the first 30 vulnerabilities with the highest risk are shown for each port.

Since the vulnerabilities were discovered using only version-based testing, the risk level for this finding will not exceed "high" severity. Critical risks will be assigned to vulnerabilities identified through accurate active testing methods.

Recommendation:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risks imposed by these vulnerabilities.

Classification:
CVE : CVE-2020-11023, CVE-2020-11022
CVSS V3 : 4.3

phpinfo() Output Reporting (HTTP)

port 4280/tcp

UNCONFIRMED

The following files are calling the function phpinfo() which disclose potentially sensitive information:

```
https://pentest-ground.com:4280/phpinfo.php
Concluded from:
<title>PHP 8.4.7 - phpinfo()</title>
<tr><td class="e">Configuration File (php.ini) Path </td>
<h2>PHP Variables</h2>
https://pentest-ground.com:4280/phpinfo.php
Concluded from:
<title>PHP 8.4.7 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></head>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>
<h2>PHP Variables</h2>
```

Details

Risk description:
Reporting of files containing the output of the phpinfo() PHP function previously detected via HTTP.
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.
Some of the information that can be gathered from this file includes: The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.

Recommendation:
Delete the listed files or restrict access to them.

References:
https://www.php.net/manual/en/function.phpinfo.php

Classification:
CVE : CVE-2008-0149, CVE-2023-49282, CVE-2023-49283
CVSS : 5
CVSS V3 : 5.3

awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check

UNCONFIRMED

port 4280/tcp

Vulnerable URL: https://pentest-ground.com:4280/vulnerabilities/fi/index.php?page=/etc/passwd

Details

Risk description:
awiki is prone to multiple local file include (LFI) vulnerabilities because it fails to properly sanitize user-supplied input.
An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host.

Recommendation:
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

References:
https://www.exploit-db.com/exploits/36047/
http://www.securityfocus.com/bid/49187

Classification:
CVSS : 5

End-of-Life (EOL) found for Redis key-value store

CONFIRMED

port 6379/tcp

We managed to detect that Redis key-value store has reached the End-of-Life (EOL).

Version detected: 5.0.7
End-of-life date: 2022-04-27 Latest version for the cycle: 5.0.14
This release cycle (5.0) doesn't have long-term-support (LTS). The cycle was released on 2018-10-17 and its latest release date was 2021-10-04. The support ended on 2020-04-30.

Details

Risk description:
Using end-of-life (EOL) software poses significant security risks for organizations. EOL software no longer receives updates, including critical security patches. This creates a vulnerability landscape where known and potentially new security flaws remain unaddressed, making the software an attractive target for malicious actors. Attackers can exploit these vulnerabilities to gain unauthorized access, disrupt services, or steal sensitive data. Moreover, without updates, compatibility issues arise with newer technologies, leading to operational inefficiencies and increased potential for system failures.

Additionally, regulatory and compliance risks accompany the use of EOL software. Many industries have strict data protection regulations that require up-to-date software to ensure the highest security standards. Non-compliance can result in hefty fines and legal consequences. Organizations also risk damaging their reputation if a breach occurs due to outdated software, eroding customer trust and potentially leading to a loss of business. Therefore, continuing to use EOL software undermines both security posture and business integrity, necessitating timely upgrades and proactive risk management strategies.

Recommendation:
To mitigate the risks associated with end-of-life (EOL) software, it's crucial to take proactive steps. Start by identifying any EOL software currently in use within your organization. Once identified, prioritize upgrading or replacing these applications with supported versions that receive regular updates and security patches. This not only helps close security gaps but also ensures better compatibility with newer technologies, enhancing overall system efficiency and reliability.Additionally, develop a comprehensive software lifecycle management plan. This plan should include regular audits to identify upcoming EOL dates and a schedule for timely updates or replacements. Train your IT staff and users about the importance of keeping software up to date and the risks associated with using outdated versions. By maintaining a proactive approach to software management, you can significantly reduce security risks, ensure compliance with industry regulations, and protect your organization's reputation and customer trust.

PHPinfo Page

CONFIRMED

port 4280/tcp

We managed to detect a PHPinfo Page.
We extracted the following information from the target: **8.4.7**
Endpoint: **https://pentest-ground.com:4280/phpinfo.php**

Details

Vulnerability description:

PHPinfo page was detected. The output of the phpinfo() command can reveal sensitive and detailed PHP environment information.

Risk description:
The risk exists that the data is unknowingly exposed to the internet, making it accessible to remote threat actors that can leverage it to attack the target, or the entire company, depending on the sensitivity of the data.

Recommendation:
Remove PHP Info pages from publicly accessible sites, or restrict access to authorized users only.

Weak MAC Algorithm(s) Supported (SSH)

port 4445/tcp

UNCONFIRMED

The remote SSH server supports the following weak client-to-server MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com

The remote SSH server supports the following weak server-to-client MAC algorithm(s):

umac-64-etm@openssh.com
umac-64@openssh.com

Details

Risk description:
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Recommendation:
Disable the reported weak MAC algorithm(s).

References:
https://www.rfc-editor.org/rfc/rfc6668
https://www.rfc-editor.org/rfc/rfc4253#section-6.4

Classification:
CVSS : 2.6

IP Information

CONFIRMED

IP Address	Hostname	Location	Autonomous system (AS) Information	Organization (Name & Type)
178.79.134.182	pentest-ground.com	London, England, United Kingdom	Akamai Technologies Inc (AS63949)	Linode LLC (hosting)

Details

Risk description:
If an attacker knows the physical location of an organization's IP address and its Autonomous System (AS) number, they could launch targeted physical or cyber attacks, exploiting regional vulnerabilities or disrupting critical infrastructure.

Recommendation:
We recommend reviewing physical security measures and monitoring network traffic for unusual activity, indicating potential cyber threats. Additionally, implementing robust network segmentation and adopting encryption protocols for data in transit can help protect sensitive information, even if attackers are aware of the IP addresses and the Autonomous System (AS) number.

DNS Records

port 53/udp

CONFIRMED

Domain Queried	DNS Record Type	Description	Value
pentest-ground.com	A	IPv4 address	178.79.134.182
pentest-ground.com	NS	Name server	ns2.linode.com
pentest-ground.com	NS	Name server	ns3.linode.com

pentest-ground.com	NS	Name server	ns1.linode.com
pentest-ground.com	NS	Name server	ns5.linode.com
pentest-ground.com	NS	Name server	ns4.linode.com
pentest-ground.com	MX	Mail server	10 mail.pentest-ground.com
pentest-ground.com	SOA	Start of Authority	ns1.linode.com. admin2.admin.test. 2021000151 14400 14400 1209600 86400
pentest-ground.com	CAA	Certificate Authority Authorization	0 issue "letsencrypt.org"

Details

Risk description:
An initial step for an attacker aiming to learn about an organization involves conducting searches on its domain names to uncover DNS records associated with the organization. This strategy aims to amass comprehensive insights into the target domain, enabling the attacker to outline the organization's external digital landscape. This gathered intelligence may subsequently serve as a foundation for launching attacks, including those based on social engineering techniques. DNS records pointing to services or servers that are no longer in use can provide an attacker with an easy entry point into the network.

Recommendation:
We recommend reviewing all DNS records associated with the domain and identifying and removing unused or obsolete records.

Open ports discovery

CONFIRMED

Port	State	Service	Product	Product Version
80	open	http	nginx	1.27.5
81	open	https	nginx	1.27.5
443	open	https	nginx	1.27.5
4280	open	https	nginx	1.27.5
4445	open	ssh	OpenSSH	8.4p1 Debian 5+deb11u5
5013	open	https	nginx	1.27.5
6379	open	redis	Redis key-value store	5.0.7
7001	open	https	Oracle WebLogic admin httpd	-
9000	open	https	nginx	1.27.5

Details

Risk description:
This is the list of ports that have been found on the target host. Having unnecessary open ports may expose the target to more risks because those network services and applications may contain vulnerabilities.

Recommendation:
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

Web redirect detected on port 80

CONFIRMED

We managed to detect the redirect using the following Request / Response chain.

Details

Recommendation:
Vulnerability checks are skipped for ports that redirect to another port. We recommend scanning the redirected port directly.

GraphQL Alias-based Batching

port 5013/tcp

CONFIRMED

We managed to detect a GraphQL Alias-based Batching, using the following Request / Response chain.
Endpoint: **https://pentest-ground.com:5013/graphql**

Details

Vulnerability description:
GraphQL supports aliasing of multiple sub-queries into a single queries. This allows users to request multiple objects or multiple instances of objects efficiently. However, an attacker can leverage this feature to evade many security measures, including rate limit.

Risk description:
The risk exists that a remote attacker might leverage the misconfigurations in order to compromise the target.

Recommendation:
Limit queries aliasing in your GraphQL Engine to ensure mitigation of aliasing-based attacks.

References:
https://github.com/dolevf/Damn-Vulnerable-GraphQL-Application
https://cheatsheetseries.owasp.org/cheatsheets/GraphQL_Cheat_Sheet.html
https://graphql.security/
https://stackoverflow.com/questions/62421352/graphql-difference-between-using-alias-versus-multiple-query-objects-when-doin

GraphQL Array-based Batching

port 5013/tcp

CONFIRMED

We managed to detect a GraphQL Array-based Batching, using the following Request / Response chain.
Endpoint: **https://pentest-ground.com:5013/graphql**

Details

Vulnerability description:
Some GraphQL engines support batching of multiple queries into a single request. This allows users to request multiple objects or multiple instances of objects efficiently. However, an attacker can leverage this feature to evade many security measures, including Rate Limit.

Risk description:
The risk exists that a remote attacker might leverage the misconfigurations in order to compromise the target.

Recommendation:
Deactivate or limit Batching in your GraphQL engine.

References:
https://stackoverflow.com/questions/62421352/graphql-difference-between-using-alias-versus-multiple-query-objects-when-doin
https://github.com/dolevf/Damn-Vulnerable-GraphQL-Application
https://graphql.security/

GraphQL Field Suggestion Information Disclosure

port 5013/tcp

CONFIRMED

We managed to detect a GraphQL Field Suggestion Information Disclosure, using the following Request / Response chain.
Endpoint: **https://pentest-ground.com:5013/graphql**

Details

Vulnerability description:
If introspection is disabled on your target, Field Suggestion can allow users to still earn information on the GraphQL schema. By default, GraphQL backends have a feature for fields and operations suggestions. If you try to query a field but you have made a typo, GraphQL will attempt to suggest fields that are similar to the initial attempt.

Risk description:
The risk exists that a remote attacker might leverage the misconfigurations in order to compromise the target.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://github.com/webonyx/graphql-php/issues/454
https://github.com/dolevf/Damn-Vulnerable-GraphQL-Application
https://cheatsheetseries.owasp.org/cheatsheets/GraphQL_Cheat_Sheet.html
https://graphql.security

Missing Subresource Integrity

CONFIRMED

port 443/tcp

We managed to detect a Missing Subresource Integrity.
We extracted the following information from the target: **https://cdn.jsdelivr.net/npm/alpinejs@3.13.0/dist/cdn.min.js, https://cdn.usefathom.com/script.js, https://cdn.tailwindcss.com, https://unpkg.com/@popperjs/core@2, https://unpkg.com/tippy.js@6, https://fonts.googleapis.com/css2?family=Inter:wght@400;600;700;800&display=swap**
Endpoint: **https://pentest-ground.com:443**

Details

Vulnerability description:
Checks if external script and stylesheet tags in the HTML response are missing the Subresource Integrity (SRI) attribute.

Risk description:
The risk exists that a remote attacker might leverage the misconfigurations in order to compromise the target.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Third_Party_Javascript_Management_Cheat_Sheet.html#subresource-integrity
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

Missing Subresource Integrity

CONFIRMED

port 5013/tcp

We managed to detect a Missing Subresource Integrity, using the following Request / Response chain.
We extracted the following information from the target: **https://cdn.usefathom.com/script.js**
Endpoint: **https://pentest-ground.com:5013**

Details

Vulnerability description:
Checks if external script and stylesheet tags in the HTML response are missing the Subresource Integrity (SRI) attribute.

Risk description:
The risk exists that a remote attacker might leverage the misconfigurations in order to compromise the target.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Third_Party_Javascript_Management_Cheat_Sheet.html#subresource-integrity
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

Missing Subresource Integrity

CONFIRMED

port 9000/tcp

We managed to detect a Missing Subresource Integrity, using the following Request / Response chain.
We extracted the following information from the target: **https://cdn.jsdelivr.net/npm/alpinejs@3.13.0/dist/cdn.min.js, https://cdn.usefathom.com/script.js, https://cdn.tailwindcss.com, https://unpkg.com/@popperjs/core@2, https://unpkg.com/tippy.js@6, https://pentest-ground.com/alpine-data.js, https://fonts.googleapis.com/css2?family=Inter:wght@400;600;700;800&display=swap**
Endpoint: **https://pentest-ground.com:9000**

Details

Vulnerability description:
Checks if external script and stylesheet tags in the HTML response are missing the Subresource Integrity (SRI) attribute.

Risk description:
The risk exists that a remote attacker might leverage the misconfigurations in order to compromise the target.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Third_Party_Javascript_Management_Cheat_Sheet.html#subresource-integrity
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

Missing Subresource Integrity

CONFIRMED

port 81/tcp

We managed to detect a Missing Subresource Integrity, using the following Request / Response chain.
We extracted the following information from the target: **https://cdnjs.cloudflare.com/ajax/libs/OwlCarousel2/2.2.1/owl.carousel.min.js, https://cdnjs.cloudflare.com/ajax/libs/OwlCarousel2/2.1.3/assets/owl.carousel.min.css, https://fonts.googleapis.com/css?**

family=Open+Sans:300,400,600,700|Roboto:400,500&display=swap
Endpoint: **https://pentest-ground.com:81**

Details

Vulnerability description:
Checks if external script and stylesheet tags in the HTML response are missing the Subresource Integrity (SRI) attribute.

Risk description:
The risk exists that a remote attacker might leverage the misconfigurations in order to compromise the target.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Third_Party_Javascript_Management_Cheat_Sheet.html#subresource-integrity
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

OpenSSH Service

CONFIRMED

port 4445/tcp

We managed to detect a OpenSSH Service.
We extracted the following information from the target: **SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u5**

Details

Vulnerability description:
OpenSSH service was detected.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
http://www.openwall.com/lists/oss-security/2016/08/01/2
http://www.openwall.com/lists/oss-security/2018/08/15/5
http://seclists.org/fulldisclosure/2016/Jul/51
https://nvd.nist.gov/vuln/detail/CVE-2016-6210
https://nvd.nist.gov/vuln/detail/CVE-2018-15473

Redis Info

CONFIRMED

port 6379/tcp

We managed to detect a Redis Info, using the following Request / Response chain.
We extracted the following information from the target: **connected_slaves:0, used_memory_human:2.10M, role:master, redis_version:5.0.7, process_id:1, used_cpu_sys:0.899621, used_cpu_user:0.476623, connected_clients:59**

Details

Vulnerability description:
Retrieves information (such as version number and architecture) from a Redis key-value store.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://nmap.org/nsedoc/scripts/redis-info.html

Redis Info

CONFIRMED

port 6379/tcp

We managed to detect a Redis Info, using the following Request / Response chain.
We extracted the following information from the target: **role:master, redis_version:5.0.7, process_id:1, used_cpu_sys:0.899621, used_cpu_user:0.476623, connected_clients:59, connected_slaves:0, used_memory_human:2.10M**

Details

Vulnerability description:
Retrieves information (such as version number and architecture) from a Redis key-value store.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://nmap.org/nsedoc/scripts/redis-info.html

SSH Auth Methods

CONFIRMED

port 4445/tcp

We managed to detect a SSH Auth Methods, using the following Request / Response chain.
We extracted the following information from the target: **["publickey","password"]**

⌄ Details

Vulnerability description:
SSH (Secure Shell) authentication modes are methods used to verify the identity of users and ensure secure access to remote systems. Common SSH authentication modes include password-based authentication, which relies on a secret passphrase, and public key authentication, which uses cryptographic keys for a more secure and convenient login process. Additionally, multi-factor authentication (MFA) can be employed to enhance security by requiring users to provide multiple forms of authentication, such as a password and a one-time code.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://nmap.org/nsedoc/scripts/ssh-auth-methods.html

SSH Server Software Enumeration

CONFIRMED

port 4445/tcp

We managed to detect a SSH Server Software Enumeration, using the following Request / Response chain.
We extracted the following information from the target: **SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u5**

⌄ Details

Recommendation:
We recommend you to analyze if this resource should be available or not.

SSH Password-based Authentication

CONFIRMED

port 4445/tcp

We managed to detect a SSH Password-based Authentication, using the following Request / Response chain.

⌄ Details

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://nmap.org/nsedoc/scripts/ssh-auth-methods.html

SSH SHA-1 HMAC Algorithms Enabled

CONFIRMED

port 4445/tcp

We managed to detect a SSH SHA-1 HMAC Algorithms Enabled, using the following Request / Response chain.

⌄ Details

Vulnerability description:
The SSH server at the remote end is set up to allow the use of SHA-1 HMAC algorithms.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://forums.ivanti.com/s/article/How-to-disable-SSH-SHA-1-HMAC-algorithms?language=en_US

TLS Version

CONFIRMED

port 443/tcp

The following TLS Version: **tls12** was detected.
Endpoint: **pentest-ground.com:443**

⌄ Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Recommendation:
We recommend you to analyze if this resource should be available or not.

TLS Version

CONFIRMED

port 9000/tcp

The following TLS Version: **tls12** was detected.
Endpoint: **pentest-ground.com:9000**

Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Recommendation:
We recommend you to analyze if this resource should be available or not.

TLS Version

CONFIRMED

port 5013/tcp

The following TLS Version: **tls12** was detected.
Endpoint: **pentest-ground.com:5013**

Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Recommendation:
We recommend you to analyze if this resource should be available or not.

TLS Version

CONFIRMED

port 7001/tcp

The following TLS Version: **tls12** was detected.
Endpoint: **pentest-ground.com:7001**

Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Recommendation:
We recommend you to analyze if this resource should be available or not.

TLS Version

CONFIRMED

port 81/tcp

The following TLS Version: **tls12** was detected.
Endpoint: **pentest-ground.com:81**

Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Recommendation:
We recommend you to analyze if this resource should be available or not.

TLS Version

CONFIRMED

port 4280/tcp

The following TLS Version: **tls12** was detected.
Endpoint: **pentest-ground.com:4280**

Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a

computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Recommendation:
We recommend you to analyze if this resource should be available or not.

TLS Version

port 443/tcp

CONFIRMED

The following TLS Version: **tls13** was detected.
Endpoint: **pentest-ground.com:443**

Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Recommendation:
We recommend you to analyze if this resource should be available or not.

TLS Version

port 9000/tcp

CONFIRMED

The following TLS Version: **tls13** was detected.
Endpoint: **pentest-ground.com:9000**

Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Recommendation:
We recommend you to analyze if this resource should be available or not.

TLS Version

port 5013/tcp

CONFIRMED

The following TLS Version: **tls13** was detected.
Endpoint: **pentest-ground.com:5013**

Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Recommendation:
We recommend you to analyze if this resource should be available or not.

TLS Version

port 81/tcp

CONFIRMED

The following TLS Version: **tls13** was detected.
Endpoint: **pentest-ground.com:81**

Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Recommendation:
We recommend you to analyze if this resource should be available or not.

TLS Version

port 7001/tcp

CONFIRMED

The following TLS Version: **tls13** was detected.
Endpoint: **pentest-ground.com:7001**

Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Recommendation:
We recommend you to analyze if this resource should be available or not.

TLS Version

port 4280/tcp

CONFIRMED

The following TLS Version: **tls13** was detected.
Endpoint: **pentest-ground.com:4280**

Details

Vulnerability description:
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Recommendation:
We recommend you to analyze if this resource should be available or not.

WAF

port 81/tcp

CONFIRMED

We managed to detect the following Web Application Firewall: **nginxgeneric**, using the following Request / Response chain.

Details

Vulnerability description:
A web application firewall was detected.

References:
https://github.com/Ekultek/WhatWaf

WAF

port 5013/tcp

CONFIRMED

We managed to detect the following Web Application Firewall: **nginxgeneric**, using the following Request / Response chain.

Details

Vulnerability description:
A web application firewall was detected.

References:
https://github.com/Ekultek/WhatWaf

WAF

port 443/tcp

CONFIRMED

We managed to detect the following Web Application Firewall: **nginxgeneric**, using the following Request / Response chain.

Details

Vulnerability description:
A web application firewall was detected.

References:
https://github.com/Ekultek/WhatWaf

WAF

port 9000/tcp

CONFIRMED

We managed to detect the following Web Application Firewall: **nginxgeneric**, using the following Request / Response chain.

Details

Vulnerability description:
A web application firewall was detected.

References:

https://github.com/Ekultek/WhatWaf

WAF

port 4280/tcp

CONFIRMED

We managed to detect the following Web Application Firewall: **apachegeneric**, using the following Request / Response chain.

Details

Vulnerability description:
A web application firewall was detected.

References:
https://github.com/Ekultek/WhatWaf

OpenAPI

port 9000/tcp

CONFIRMED

We managed to detect a OpenAPI, using the following Request / Response chain.
Endpoint: **https://pentest-ground.com:9000/openapi.json**

Details

Vulnerability description:
OpenAPI was detected.

Risk description:
The risk exists that the data is unknowingly exposed to the internet, making it accessible to remote threat actors that can leverage it to attack the target, or the entire company, depending on the sensitivity of the data.

Recommendation:
We suggest restricting access to the exposed resource.

References:
https://www.openapis.org/

RDAP WHOIS

port 6379/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **client renew prohibited, client transfer prohibited, client update prohibited, client delete prohibited**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 6379/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2019-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:

This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 6379/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2023-11-05T20:45:44Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 6379/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2025-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 6379/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **NS1.LINODE.COM, NS2.LINODE.COM**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 6379/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **false**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:

The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:

This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:

We recommend you to analyze if this data should be available or not.

References:

https://about.rdap.org/

RDAP WHOIS

port 4280/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2019-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:

The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:

This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:

We recommend you to analyze if this data should be available or not.

References:

https://about.rdap.org/

RDAP WHOIS

port 4280/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2023-11-05T20:45:44Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:

The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:

This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:

We recommend you to analyze if this data should be available or not.

References:

https://about.rdap.org/

RDAP WHOIS

port 4280/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2025-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 4280/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **NS1.LINODE.COM, NS2.LINODE.COM**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 4280/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **false**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 4280/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **client delete prohibited, client renew prohibited, client transfer prohibited, client update prohibited**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:

This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 4445/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2019-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 4445/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2023-11-05T20:45:44Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 4445/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2025-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 4445/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **NS1.LINODE.COM, NS2.LINODE.COM**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 4445/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **false**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 4445/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **client delete prohibited, client renew prohibited, client transfer prohibited, client update prohibited**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 443/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2019-11-04T15:22:35Z**

We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 443/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2023-11-05T20:45:44Z**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 443/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2025-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 443/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **NS1.LINODE.COM, NS2.LINODE.COM**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:

This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

CONFIRMED

port 443/tcp

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **false**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

CONFIRMED

port 443/tcp

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **client transfer prohibited, client update prohibited, client delete prohibited, client renew prohibited**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

CONFIRMED

port 81/tcp

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2025-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:

https://about.rdap.org/

RDAP WHOIS

port 5013/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **client delete prohibited, client renew prohibited, client transfer prohibited, client update prohibited**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 81/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **NS1.LINODE.COM, NS2.LINODE.COM**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 5013/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2019-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 5013/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2023-11-05T20:45:44Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:

The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:

This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:

We recommend you to analyze if this data should be available or not.

References:

https://about.rdap.org/

RDAP WHOIS

port 5013/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2025-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:

The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:

This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:

We recommend you to analyze if this data should be available or not.

References:

https://about.rdap.org/

RDAP WHOIS

port 5013/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **NS1.LINODE.COM, NS2.LINODE.COM**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:

The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:

This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:

We recommend you to analyze if this data should be available or not.

References:

https://about.rdap.org/

RDAP WHOIS

port 5013/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **false**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:

The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 81/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **false**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 81/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **client delete prohibited, client renew prohibited, client transfer prohibited, client update prohibited**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 81/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2019-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 81/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2023-11-05T20:45:44Z**
We managed to produce this finding using the following Request / Response chain.
⌄ Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 7001/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **NS1.LINODE.COM, NS2.LINODE.COM**
We managed to produce this finding using the following Request / Response chain.
⌄ Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 7001/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **false**
We managed to produce this finding using the following Request / Response chain.
⌄ Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 7001/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **client delete prohibited, client renew prohibited, client transfer prohibited, client update prohibited**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:

The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:

This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:

We recommend you to analyze if this data should be available or not.

References:

https://about.rdap.org/

RDAP WHOIS

port 9000/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2019-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:

The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:

This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:

We recommend you to analyze if this data should be available or not.

References:

https://about.rdap.org/

RDAP WHOIS

port 7001/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2019-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:

The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:

This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:

We recommend you to analyze if this data should be available or not.

References:

https://about.rdap.org/

RDAP WHOIS

port 9000/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2023-11-05T20:45:44Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:

The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about

Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 9000/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2025-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 7001/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2023-11-05T20:45:44Z**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 9000/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **NS1.LINODE.COM, NS2.LINODE.COM**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 7001/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **2025-11-04T15:22:35Z**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 9000/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **false**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

RDAP WHOIS

port 9000/tcp

CONFIRMED

Endpoint: **https://rdap.verisign.com/com/v1/domain/pentest-ground.com**
We extracted the following information from the target: **client update prohibited, client delete prohibited, client renew prohibited, client transfer prohibited**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
The Registration Data Access Protocol (RDAP) is the successor to WHOIS. Like WHOIS, RDAP provides access to information about Internet resources (domain names, autonomous system numbers, and IP addresses).

Risk description:
This is not a vulnerability, but the data queried from RDAP can leak information about the target.

Recommendation:
We recommend you to analyze if this data should be available or not.

References:
https://about.rdap.org/

Oracle WebLogic Login Panel

port 7001/tcp

CONFIRMED

We managed to detect a Oracle WebLogic Login Panel, using the following Request / Response chain.
We extracted the following information from the target: **12.2.1.3.0**.
Endpoint: **https://pentest-ground.com:7001/console/login/LoginForm.jsp**.

Details

Vulnerability description:
Oracle WebLogic login panel was detected.

Risk description:
The risk exists that a remote unauthenticated attacker could brute-force the login panel to gain access to the service as an authenticated user. If an authenticated vulnerability is present on the machine, it could also be leveraged to exploit the target, compromising the underlying system.

Recommendation:
We suggest restricting access in the configs, or placing the panel behind a firewall if it was left out by an oversight in configuration.

GraphQL CSRF / GET method

port 5013/tcp

CONFIRMED

We managed to detect a GraphQL CSRF / GET method, using the following Request / Response chain.
Endpoint: **https://pentest-ground.com:5013/graphql?query={__typename}**

Details

Vulnerability description:
Cross Site Request Forgery happens when an external website gains ability to make API calls impersonating an user if he visits the website while being authenticated to your API. Allowing API calls through GET requests can lead to CSRF attacks, because cookies are added automatically to GET requests by the browser.

Risk description:
The risk exists that a remote attacker might leverage the misconfigurations in order to compromise the target.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://graphql.org/learn/serving-over-http/#get-request
https://github.com/dolevf/Damn-Vulnerable-GraphQL-Application
https://cheatsheetseries.owasp.org/cheatsheets/GraphQL_Cheat_Sheet.html
https://graphql.security/

HTML form

port 81/tcp

CONFIRMED

Endpoint: **https://pentest-ground.com:81**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
A form is a collection of HTML elements that allow users to submit data to a web application.

Risk description:
This is not a vulnerability, but often forms can hide vulnerabilities. Further inspection is advised.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://github.com/dirtycoder0124/formcrawler

Email Extractor

port 5013/tcp

CONFIRMED

Endpoint: **https://pentest-ground.com:5013**
We extracted the following information from the target: **nick@blackhatgraphql.com, dolev@blackhatgraphql.com**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:
Email addresses are listed on the website. The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

Risk description:
The risks exists that an attacker can use this to launch phishing attacks and learn more about the internal structure of the organization.

Recommendation:
We recommend you to analyze if email addresses should be listed on the website or not.

References:
https://portswigger.net/web-security/information-disclosure
https://portswigger.net/kb/issues/00600200_email-addresses-disclosed

Nginx version

port 5013/tcp

CONFIRMED

Extracted results: **nginx/1.27.5**.
Endpoint: **https://pentest-ground.com:5013**.
Details

Vulnerability description:
Some nginx servers have the version on the response header. Useful when you need to find specific CVEs on your targets.

Recommendation:
We recommend you to analyze if this resource should be available or not.

Nginx version

port 4280/tcp

CONFIRMED

Extracted results: **nginx/1.27.5**.
Endpoint: **https://pentest-ground.com:4280**.
Details

Vulnerability description:
Some nginx servers have the version on the response header. Useful when you need to find specific CVEs on your targets.

Recommendation:
We recommend you to analyze if this resource should be available or not.

PHP

port 4280/tcp

CONFIRMED

Extracted results: **8.4.7**.
Endpoint: **https://pentest-ground.com:4280**.
Details

Recommendation:
We recommend you to analyze if this resource should be available or not.

Nginx version

port 9000/tcp

CONFIRMED

Extracted results: **nginx/1.27.5**.
Endpoint: **https://pentest-ground.com:9000**.
Details

Vulnerability description:
Some nginx servers have the version on the response header. Useful when you need to find specific CVEs on your targets.

Recommendation:
We recommend you to analyze if this resource should be available or not.

Email Extractor

port 81/tcp

CONFIRMED

Endpoint: **https://pentest-ground.com:81**
We extracted the following information from the target: **demo@gmail.com**
We managed to produce this finding using the following Request / Response chain.
Details

Vulnerability description:

Email addresses are listed on the website. The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

Risk description:

The risks exists that an attacker can use this to launch phishing attacks and learn more about the internal structure of the organization.

Recommendation:

We recommend you to analyze if email addresses should be listed on the website or not.

References:

https://portswigger.net/web-security/information-disclosure
https://portswigger.net/kb/issues/00600200_email-addresses-disclosed

Nginx version

port 81/tcp

CONFIRMED

Extracted results: **nginx/1.27.5**.
Endpoint: **https://pentest-ground.com:81**.

Details

Vulnerability description:

Some nginx servers have the version on the response header. Useful when you need to find specific CVEs on your targets.

Recommendation:

We recommend you to analyze if this resource should be available or not.

Nginx version

port 443/tcp

CONFIRMED

Extracted results: **nginx/1.27.5**.
Endpoint: **https://pentest-ground.com:443**.

Details

Vulnerability description:

Some nginx servers have the version on the response header. Useful when you need to find specific CVEs on your targets.

Recommendation:

We recommend you to analyze if this resource should be available or not.

FingerprintHub Technology Fingerprint

port 7001/tcp

CONFIRMED

We extracted the following information from the target: **weblogic**.
Endpoint: **https://pentest-ground.com:7001**.

Details

Vulnerability description:

FingerprintHub Technology Fingerprint tests run in nuclei.

Recommendation:

We recommend you to analyze if this resource should be available or not.

References:

https://github.com/0x727/FingerprintHub

Wappalyzer Technology

port 4280/tcp

CONFIRMED

We extracted the following information from the target: **php**.
Endpoint: **https://pentest-ground.com:4280**.

Details

Recommendation:

We recommend you to analyze if this resource should be available or not.

Wappalyzer Technology

port 9000/tcp

CONFIRMED

We extracted the following information from the target: **jsdelivr**.
Endpoint: **https://pentest-ground.com:9000**.

Details

Recommendation:
We recommend you to analyze if this resource should be available or not.

Wappalyzer Technology

port 5013/tcp

CONFIRMED

We extracted the following information from the target: **nginx**.
Endpoint: **https://pentest-ground.com:5013**.

Details

Recommendation:
We recommend you to analyze if this resource should be available or not.

FingerprintHub Technology Fingerprint

port 443/tcp

CONFIRMED

We extracted the following information from the target: **weblogic**.
Endpoint: **https://pentest-ground.com:443**.

Details

Vulnerability description:
FingerprintHub Technology Fingerprint tests run in nuclei.

Recommendation:
We recommend you to analyze if this resource should be available or not.

References:
https://github.com/0x727/FingerprintHub

Wappalyzer Technology

port 443/tcp

CONFIRMED

We extracted the following information from the target: **jsdelivr**.
Endpoint: **https://pentest-ground.com:443**.

Details

Recommendation:
We recommend you to analyze if this resource should be available or not.

Wappalyzer Technology

port 81/tcp

CONFIRMED

We extracted the following information from the target: **google-font-api**.
Endpoint: **https://pentest-ground.com:81**.

Details

Recommendation:
We recommend you to analyze if this resource should be available or not.

README.md file disclosure

port 4280/tcp

CONFIRMED

We managed to detect a README.md file disclosure.
Endpoint: **https://pentest-ground.com:4280/README.md**

Details

Vulnerability description:
Internal documentation file often used in projects which can contain sensitive information.

Risk description:

The risk exists that the data is unknowingly exposed to the internet, making it accessible to remote threat actors that can leverage it to attack the target, or the entire company, depending on the sensitivity of the data.

Recommendation:

We suggest restricting access to the exposed resource.

Find Pages with Old Copyright Dates

port 81/tcp

CONFIRMED

Endpoint: **https://pentest-ground.com:81**
We extracted the following information from the target: **© 2022**
We managed to produce this finding using the following Request / Response chain.

Details

Vulnerability description:

Copyright dates are used to indicate the year of the content's creation or last modification.

Risk description:

This is not a vulnerability, but the presence of old copyright dates can leak information about the target.

Recommendation:

We recommend you to analyze if this copyright information should be updated or not.

References:

https://www.nolo.com/legal-encyclopedia/when-do-you-need-copyright-notice-websites-and-where-do-you-place-it.html

SSL DNS Names

port 9000/tcp

CONFIRMED

The following SSL DNS Names: **pentest-ground.com** was detected.
Endpoint: **pentest-ground.com:9000**

Details

Vulnerability description:

Extract the Subject Alternative Name (SAN) from the target's certificate. SAN facilitates the usage of additional hostnames with the same certificate.

Recommendation:

We recommend you to analyze if this resource should be available or not.

SSL Certificate Issuer

port 9000/tcp

CONFIRMED

The following SSL Certificate Issuer: **Let's Encrypt** was detected.
Endpoint: **pentest-ground.com:9000**

Details

Vulnerability description:

Extract the issuer's organization from the target's certificate. Issuers are entities which sign and distribute certificates.

Recommendation:

We recommend you to analyze if this resource should be available or not.

SSL DNS Names

port 4280/tcp

CONFIRMED

The following SSL DNS Names: **pentest-ground.com** was detected.
Endpoint: **pentest-ground.com:4280**

Details

Vulnerability description:

Extract the Subject Alternative Name (SAN) from the target's certificate. SAN facilitates the usage of additional hostnames with the same certificate.

Recommendation:

We recommend you to analyze if this resource should be available or not.

SSL Certificate Issuer

port 4280/tcp

CONFIRMED

The following SSL Certificate Issuer: **Let's Encrypt** was detected.
Endpoint: **pentest-ground.com:4280**

Details

Vulnerability description:
Extract the issuer's organization from the target's certificate. Issuers are entities which sign and distribute certificates.

Recommendation:
We recommend you to analyze if this resource should be available or not.

SSL DNS Names

port 5013/tcp

CONFIRMED

The following SSL DNS Names: **pentest-ground.com** was detected.
Endpoint: **pentest-ground.com:5013**

Details

Vulnerability description:
Extract the Subject Alternative Name (SAN) from the target's certificate. SAN facilitates the usage of additional hostnames with the same certificate.

Recommendation:
We recommend you to analyze if this resource should be available or not.

SSL DNS Names

port 443/tcp

CONFIRMED

The following SSL DNS Names: **pentest-ground.com** was detected.
Endpoint: **pentest-ground.com:443**

Details

Vulnerability description:
Extract the Subject Alternative Name (SAN) from the target's certificate. SAN facilitates the usage of additional hostnames with the same certificate.

Recommendation:
We recommend you to analyze if this resource should be available or not.

SSL Certificate Issuer

port 5013/tcp

CONFIRMED

The following SSL Certificate Issuer: **Let's Encrypt** was detected.
Endpoint: **pentest-ground.com:5013**

Details

Vulnerability description:
Extract the issuer's organization from the target's certificate. Issuers are entities which sign and distribute certificates.

Recommendation:
We recommend you to analyze if this resource should be available or not.

SSL Certificate Issuer

port 443/tcp

CONFIRMED

The following SSL Certificate Issuer: **Let's Encrypt** was detected.
Endpoint: **pentest-ground.com:443**

Details

Vulnerability description:
Extract the issuer's organization from the target's certificate. Issuers are entities which sign and distribute certificates.

Recommendation:
We recommend you to analyze if this resource should be available or not.

SSL DNS Names

port 81/tcp

CONFIRMED

The following SSL DNS Names: **pentest-ground.com** was detected.
Endpoint: **pentest-ground.com:81**

Details

Vulnerability description:
Extract the Subject Alternative Name (SAN) from the target's certificate. SAN facilitates the usage of additional hostnames with the same certificate.

Recommendation:
We recommend you to analyze if this resource should be available or not.

SSL Certificate Issuer

port 81/tcp

CONFIRMED

The following SSL Certificate Issuer: **Let's Encrypt** was detected.
Endpoint: **pentest-ground.com:81**

Details

Vulnerability description:
Extract the issuer's organization from the target's certificate. Issuers are entities which sign and distribute certificates.

Recommendation:
We recommend you to analyze if this resource should be available or not.

SSL DNS Names

port 7001/tcp

CONFIRMED

The following SSL DNS Names: **pentest-ground.com** was detected.
Endpoint: **pentest-ground.com:7001**

Details

Vulnerability description:
Extract the Subject Alternative Name (SAN) from the target's certificate. SAN facilitates the usage of additional hostnames with the same certificate.

Recommendation:
We recommend you to analyze if this resource should be available or not.

SSL Certificate Issuer

port 7001/tcp

CONFIRMED

The following SSL Certificate Issuer: **Let's Encrypt** was detected.
Endpoint: **pentest-ground.com:7001**

Details

Vulnerability description:
Extract the issuer's organization from the target's certificate. Issuers are entities which sign and distribute certificates.

Recommendation:
We recommend you to analyze if this resource should be available or not.

OS Detection

UNCONFIRMED

Operating System	Accuracy
Linux 4.15 - 5.6	100%

Details

Vulnerability description:
OS Detection

Server software and technologies

port 81/tcp

UNCONFIRMED

Software / Version	Category
Bootstrap	UI frameworks
Nginx 1.27.5	Web servers, Reverse proxies
Cloudflare	CDN
OWL Carousel	JavaScript libraries
jQuery 3.4.1	JavaScript libraries
cdnjs	CDN

Details

Vulnerability description:
We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Server software and technologies

port 443/tcp

UNCONFIRMED

Software / Version	Category
Nginx 1.27.5	Web servers, Reverse proxies

Details

Vulnerability description:
We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Server software and technologies

port 4280/tcp

UNCONFIRMED

Software / Version	Category
PHP 8.4.7	Programming languages
Nginx 1.27.5	Web servers, Reverse proxies

Details

Vulnerability description:
We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Server software and technologies

port 5013/tcp

UNCONFIRMED

Software / Version	Category
Bootstrap	UI frameworks
Nginx 1.27.5	Web servers, Reverse proxies
jQuery	JavaScript libraries
Fathom	Analytics

Details

Vulnerability description:
We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Server software and technologies

port 7001/tcp

UNCONFIRMED

Software / Version	Category
Java	Programming languages
JavaServer Pages	Web frameworks
Weblogic Server	Web servers

Details

Vulnerability description:
We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Server software and technologies

port 9000/tcp

UNCONFIRMED

Software / Version	Category
Tailwind CSS	UI frameworks
Nginx 1.27.5	Web servers, Reverse proxies
Unpkg	CDN
Tippy.js 6	JavaScript libraries

jsDelivr	CDN
Fathom	Analytics
Popper 2	Miscellaneous

Details

Vulnerability description:
We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Service Detection with 'GET' Request

port 6379/tcp

UNCONFIRMED

A Redis server seems to be running on this port.

Details

Risk description:
This plugin performs service detection.
This plugin is a complement of the plugin 'Services' (OID: 1.3.6.1.4.1.25623.1.0.10330). It sends a HTTP 'GET' request to the remaining unknown services and tries to identify them.

Recommendation:
No recommendations to display.

SSH Protocol Algorithms Supported

port 4445/tcp

UNCONFIRMED

The following options are supported by the remote SSH service:

kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,kex-strict-s-v00@openssh.com

server_host_key_algorithms:
rsa-sha2-512,rsa-sha2-256,ssh-rsa,ecdsa-sha2-nistp256,ssh-ed25519

encryption_algorithms_client_to_server:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

mac_algorithms_server_to_client:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

compression_algorithms_client_to_server:
none,zlib@openssh.com

compression_algorithms_server_to_client:
none,zlib@openssh.com

Details

Risk description:
This script detects which algorithms are supported by the remote SSH service.

Recommendation:
No recommendations to display.

SSH Server type and version

UNCONFIRMED

port 4445/tcp

Remote SSH server banner: SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u5
Remote SSH supported authentication: password,publickey
Remote SSH text/login banner: (not available)

This is probably:

- OpenSSH

Concluded from remote connection attempt with credentials:

Login: OpenVASVT
Password: OpenVASVT

Details

Risk description:

This detects the SSH Server's type and version by connecting to the server and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Recommendation:

No recommendations to display.

OpenSSH Detection Consolidation

UNCONFIRMED

Detected OpenSSH Server

Version: 8.4p1
Location: 4445/tcp
CPE: cpe:/a:openbsd:openssh:8.4p1

Concluded from version/product identification result:
SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u5

Details

Risk description:

Consolidation of OpenSSH detections.

Recommendation:

No recommendations to display.

References:

https://www.openssh.com/

Redis Server Detection (TCP)

UNCONFIRMED

port 6379/tcp

Detected Redis Server

Version: 5.0.7
Location: /
CPE: cpe:/a:redis:redis:5.0.7

Concluded from version/product identification result:
redis_version:5.0.7

Extra information:
Redis Server is not protected with a password.

Details

Risk description:

TCP based detection of Redis server.

Recommendation:

No recommendations to display.

References:

https://redis.io/

SSH Protocol Versions Supported

UNCONFIRMED

port 4445/tcp

The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0

SSHv2 Fingerprint(s):
ecdsa-sha2-nistp256: 24:26:04:22:1b:67:fd:12:bb:ed:f4:91:d7:e8:03:5c
ssh-ed25519: d0:75:67:4e:53:14:6f:8a:28:c0:43:b2:13:7e:4f:4a
ssh-rsa: 14:20:68:34:e9:b9:96:ae:d5:f1:96:8f:d7:c4:e9:99

⌄ Details

Risk description:
Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.

Recommendation:
No recommendations to display.

TCP Timestamps Information Disclosure

UNCONFIRMED

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1052158290
Packet 2: 1052159434

⌄ Details

Risk description:
The remote host implements TCP timestamps and therefore allows to compute the uptime.
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Recommendation:
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps

References:
https://datatracker.ietf.org/doc/html/rfc1323
https://datatracker.ietf.org/doc/html/rfc7323
https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152
https://www.fortiguard.com/psirt/FG-IR-16-090

Classification:
CVSS : 2.6

Apache HTTP Server Detection Consolidation

UNCONFIRMED

Detected Apache HTTP Server

Version: 2.4.62
Location: 4280/tcp
CPE: cpe:/a:apache:http_server:2.4.62

Concluded from version/product identification result:
Server: Apache/2.4.62 (Debian)

Concluded from version/product identification location:
https://pentest-ground.com:4280/vt-test-non-existent.html

⌄ Details

Risk description:
Consolidation of Apache HTTP Server detections.

Recommendation:
No recommendations to display.

References:
https://httpd.apache.org

SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

port 443/tcp

UNCONFIRMED

The remote web server is not enforcing HPKP.

HTTP-Banner:

HTTP/1.1 200 OK

```
Server: nginx/1.27.5
Date: ***replaced***
Content-Type: text/html
Content-Length: ***replaced***
Last-Modified: ***replaced***
Connection: close
ETag: "***replaced***"
Accept-Ranges: bytes
```

Details

Risk description:

The remote web server is not enforcing HTTP Public Key Pinning (HPKP). Note: Most major browsers have dropped / deprecated support for this header in 2020.

Recommendation:

Enable HPKP or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility.

References:

https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp
https://tools.ietf.org/html/rfc7469
https://securityheaders.io/
https://httpd.apache.org/docs/current/mod/mod_headers.html#header
https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

UNCONFIRMED

port 9000/tcp

The remote web server is not enforcing HPKP.

HTTP-Banner:

```
HTTP/1.1 200 OK
Server: nginx/1.27.5
Date: ***replaced***
Content-Type: text/html; charset=utf-8
Content-Length: ***replaced***
Connection: close
Content-Disposition: inline; filename=index.html
Last-Modified: ***replaced***
Cache-Control: no-cache
ETag: "***replaced***"
```

Details

Risk description:

The remote web server is not enforcing HTTP Public Key Pinning (HPKP). Note: Most major browsers have dropped / deprecated support for this header in 2020.

Recommendation:

Enable HPKP or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility.

References:

https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp
https://tools.ietf.org/html/rfc7469
https://securityheaders.io/
https://httpd.apache.org/docs/current/mod/mod_headers.html#header
https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

UNCONFIRMED

port 81/tcp

The remote web server is not enforcing HPKP.

HTTP-Banner:

```
HTTP/1.1 200 OK
Server: nginx/1.27.5
Date: ***replaced***
Content-Type: text/html; charset=utf-8
```

```
Content-Length: ***replaced***
Connection: close
Access-Control-Allow-Origin: *
Set-Cookie: ***replaced***
```

Details

Risk description:
The remote web server is not enforcing HTTP Public Key Pinning (HPKP). Note: Most major browsers have dropped / deprecated support for this header in 2020.

Recommendation:
Enable HPKP or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility.

References:
https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp
https://tools.ietf.org/html/rfc7469
https://securityheaders.io/
https://httpd.apache.org/docs/current/mod/mod_headers.html#header
https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

port 7001/tcp

UNCONFIRMED

The remote web server is not enforcing HPKP.

HTTP-Banner:

```
HTTP/1.1 404 Not Found
Connection: close
Date: ***replaced***
Content-Length: ***replaced***
Content-Type: text/html; charset=UTF-8
```

Details

Risk description:
The remote web server is not enforcing HTTP Public Key Pinning (HPKP). Note: Most major browsers have dropped / deprecated support for this header in 2020.

Recommendation:
Enable HPKP or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility.

References:
https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp
https://tools.ietf.org/html/rfc7469
https://securityheaders.io/
https://httpd.apache.org/docs/current/mod/mod_headers.html#header
https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

port 5013/tcp

UNCONFIRMED

The remote web server is not enforcing HPKP.

HTTP-Banner:

```
HTTP/1.1 200 OK
Server: nginx/1.27.5
Date: ***replaced***
Content-Type: text/html; charset=utf-8
Content-Length: ***replaced***
Connection: close
Set-Cookie: ***replaced***
```

Details

Risk description:
The remote web server is not enforcing HTTP Public Key Pinning (HPKP). Note: Most major browsers have dropped / deprecated support for this header in 2020.

Recommendation:
Enable HPKP or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility.

References:
https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-secure-headers/#public-key-pinning-extension-for-http-hpkp
https://tools.ietf.org/html/rfc7469
https://securityheaders.io/
https://httpd.apache.org/docs/current/mod/mod_headers.html#header
https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

UNCONFIRMED

port 7001/tcp

The remote web server is not enforcing HSTS.

HTTP-Banner:

```
HTTP/1.1 404 Not Found
Connection: close
Date: ***replaced***
Content-Length: ***replaced***
Content-Type: text/html; charset=UTF-8
```

Details

Risk description:
The remote web server is not enforcing HTTP Strict Transport Security (HSTS).

Recommendation:
Enable HSTS or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility.

References:
https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
https://tools.ietf.org/html/rfc6797
https://securityheaders.io/
https://httpd.apache.org/docs/current/mod/mod_headers.html#header
https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

UNCONFIRMED

port 5013/tcp

The remote web server is not enforcing HSTS.

HTTP-Banner:

```
HTTP/1.1 200 OK
Server: nginx/1.27.5
Date: ***replaced***
Content-Type: text/html; charset=utf-8
Content-Length: ***replaced***
Connection: close
Set-Cookie: ***replaced***
```

Details

Risk description:
The remote web server is not enforcing HTTP Strict Transport Security (HSTS).

Recommendation:
Enable HSTS or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility.

References:
https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
https://tools.ietf.org/html/rfc6797
https://securityheaders.io/
https://httpd.apache.org/docs/current/mod/mod_headers.html#header
https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

UNCONFIRMED

port 443/tcp

The remote web server is not enforcing HSTS.

HTTP-Banner:

```
HTTP/1.1 200 OK
Server: nginx/1.27.5
Date: ***replaced***
Content-Type: text/html
Content-Length: ***replaced***
Last-Modified: ***replaced***
Connection: close
ETag: "***replaced***"
Accept-Ranges: bytes
```

Details

Risk description:
The remote web server is not enforcing HTTP Strict Transport Security (HSTS).

Recommendation:
Enable HSTS or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility.

References:
https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
https://tools.ietf.org/html/rfc6797
https://securityheaders.io/
https://httpd.apache.org/docs/current/mod/mod_headers.html#header
https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

UNCONFIRMED

port 9000/tcp

The remote web server is not enforcing HSTS.

HTTP-Banner:

```
HTTP/1.1 200 OK
Server: nginx/1.27.5
Date: ***replaced***
Content-Type: text/html; charset=utf-8
Content-Length: ***replaced***
Connection: close
Content-Disposition: inline; filename=index.html
Last-Modified: ***replaced***
Cache-Control: no-cache
ETag: "***replaced***"
```

Details

Risk description:
The remote web server is not enforcing HTTP Strict Transport Security (HSTS).

Recommendation:
Enable HSTS or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility.

References:
https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
https://tools.ietf.org/html/rfc6797
https://securityheaders.io/

https://httpd.apache.org/docs/current/mod/mod_headers.html#header
https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

UNCONFIRMED

port 81/tcp

The remote web server is not enforcing HSTS.

HTTP-Banner:

```
HTTP/1.1 200 OK
Server: nginx/1.27.5
Date: ***replaced***
Content-Type: text/html; charset=utf-8
Content-Length: ***replaced***
Connection: close
Access-Control-Allow-Origin: *
Set-Cookie: ***replaced***
```

Details

Risk description:
The remote web server is not enforcing HTTP Strict Transport Security (HSTS).

Recommendation:
Enable HSTS or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility.

References:
https://owasp.org/www-project-secure-headers/
https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
https://owasp.org/www-project-secure-headers/#http-strict-transport-security-hsts
https://tools.ietf.org/html/rfc6797
https://securityheaders.io/
https://httpd.apache.org/docs/current/mod/mod_headers.html#header
https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header

SSL/TLS: Report Medium Cipher Suites

UNCONFIRMED

port 4280/tcp

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_128_GCM_SHA256
```

Details

Risk description:
This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Recommendation:
No recommendations to display.

SSL/TLS: Report Medium Cipher Suites

UNCONFIRMED

port 9000/tcp

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_128_GCM_SHA256
```

Details

Risk description:
This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Recommendation:
No recommendations to display.

SSL/TLS: Report Medium Cipher Suites

port 81/tcp

UNCONFIRMED

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_128_GCM_SHA256
```

Details

Risk description:
This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Recommendation:
No recommendations to display.

SSL/TLS: Report Medium Cipher Suites

port 7001/tcp

UNCONFIRMED

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_128_GCM_SHA256
```

Details

Risk description:
This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Recommendation:
No recommendations to display.

SSL/TLS: Report Medium Cipher Suites

port 5013/tcp

UNCONFIRMED

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_128_GCM_SHA256
```

Details

Risk description:

This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Recommendation:

No recommendations to display.

SSL/TLS: Report Medium Cipher Suites

UNCONFIRMED

port 443/tcp

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_128_GCM_SHA256
```

Details

Risk description:

This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Recommendation:

No recommendations to display.

SSL/TLS: Report Non Weak Cipher Suites

UNCONFIRMED

port 81/tcp

'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
```

'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

Details

Risk description:

This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Recommendation:

No recommendations to display.

SSL/TLS: Report Non Weak Cipher Suites

UNCONFIRMED

port 9000/tcp

'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
```

'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

Details

Risk description:
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Recommendation:
No recommendations to display.

SSL/TLS: Report Non Weak Cipher Suites

UNCONFIRMED

port 4280/tcp

'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
```

'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

Details

Risk description:
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Recommendation:
No recommendations to display.

SSL/TLS: Report Non Weak Cipher Suites

UNCONFIRMED

port 443/tcp

'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
```

'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

Details

Risk description:
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Recommendation:
No recommendations to display.

SSL/TLS: Report Non Weak Cipher Suites

UNCONFIRMED

port 5013/tcp

'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
```

'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
```

TLS_CHACHA20_POLY1305_SHA256

Details

Risk description:
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Recommendation:
No recommendations to display.

SSL/TLS: Report Non Weak Cipher Suites

UNCONFIRMED

port 7001/tcp

'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

'Non Weak' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Details

Risk description:
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Recommendation:
No recommendations to display.

SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

UNCONFIRMED

port 81/tcp

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Recommendation:
No recommendations to display.

SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

UNCONFIRMED

port 9000/tcp

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Recommendation:
No recommendations to display.

SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

UNCONFIRMED

port 4280/tcp

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Recommendation:
No recommendations to display.

SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

UNCONFIRMED

port 443/tcp

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Recommendation:
No recommendations to display.

SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

UNCONFIRMED

port 5013/tcp

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Recommendation:
No recommendations to display.

SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

UNCONFIRMED

port 7001/tcp

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Recommendation:
No recommendations to display.

SSL/TLS: Report Supported Cipher Suites

UNCONFIRMED

port 7001/tcp

'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

'Strong' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256

No 'Weak' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.3 protocol.

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service.

Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Recommendation:

No recommendations to display.

SSL/TLS: Report Supported Cipher Suites

port 4280/tcp

UNCONFIRMED

'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
```

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

'Strong' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_128_GCM_SHA256
```

No 'Weak' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.3 protocol.

Details

Risk description:

This routine reports all SSL/TLS cipher suites accepted by a service.
Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Recommendation:

No recommendations to display.

SSL/TLS: Report Supported Cipher Suites

port 443/tcp

UNCONFIRMED

'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
```

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

'Strong' cipher suites accepted by this service via the TLSv1.3 protocol:

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256

No 'Weak' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.3 protocol.

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service.
Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Recommendation:
No recommendations to display.

SSL/TLS: Report Supported Cipher Suites

port 9000/tcp

UNCONFIRMED

'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

'Strong' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256

No 'Weak' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.3 protocol.

Details

Risk description:
This routine reports all SSL/TLS cipher suites accepted by a service.
Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Recommendation:
No recommendations to display.

SSL/TLS: Report Supported Cipher Suites

port 81/tcp

UNCONFIRMED

'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

'Strong' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256

No 'Weak' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.3 protocol.

⌄ Details

Risk description:

This routine reports all SSL/TLS cipher suites accepted by a service.
Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Recommendation:

No recommendations to display.

SSL/TLS: Report Supported Cipher Suites

port 5013/tcp

UNCONFIRMED

'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

'Strong' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:

TLS_AES_128_GCM_SHA256

No 'Weak' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Null' cipher suites accepted by this service via the TLSv1.3 protocol.

No 'Anonymous' cipher suites accepted by this service via the TLSv1.3 protocol.

⌄ Details

Risk description:

This routine reports all SSL/TLS cipher suites accepted by a service.
Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Recommendation:

No recommendations to display.

Oracle WebLogic Server Detection Consolidation

UNCONFIRMED

Detected Oracle WebLogic Server

Version: 12.2.1.3.0
Location: /
CPE: cpe:/a:oracle:weblogic_server:12.2.1.3.0

Detection methods:

HTTP(s) on port 7001/tcp
Concluded from version/product identification result: WebLogic Server Version: 12.2.1.3.0
Concluded from version/product identification location: https://pentest-ground.com:7001/console/login/LoginForm.jsp

Details

Risk description:
Consolidation of Oracle WebLogic detections.

Recommendation:
No recommendations to display.

References:
https://www.oracle.com/middleware/weblogic/

SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

port 9000/tcp

UNCONFIRMED

The remote service advertises support for the following Network Protocol(s) via the ALPN extension:

SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1

Details

Risk description:
This routine identifies services supporting the following extensions to TLS: - Application-Layer Protocol Negotiation (ALPN) - Next Protocol Negotiation (NPN). Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.

Recommendation:
No recommendations to display.

References:
https://tools.ietf.org/html/rfc7301
https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

port 81/tcp

UNCONFIRMED

The remote service advertises support for the following Network Protocol(s) via the ALPN extension:

SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1

Details

Risk description:
This routine identifies services supporting the following extensions to TLS: - Application-Layer Protocol Negotiation (ALPN) - Next Protocol Negotiation (NPN). Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.

Recommendation:
No recommendations to display.

References:
https://tools.ietf.org/html/rfc7301
https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

port 5013/tcp

UNCONFIRMED

The remote service advertises support for the following Network Protocol(s) via the ALPN extension:

SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1

Details

Risk description:
This routine identifies services supporting the following extensions to TLS: - Application-Layer Protocol Negotiation (ALPN) - Next Protocol Negotiation (NPN). Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.

Recommendation:
No recommendations to display.

References:
https://tools.ietf.org/html/rfc7301
https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

UNCONFIRMED

port 443/tcp

The remote service advertises support for the following Network Protocol(s) via the ALPN extension:

SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1

Details

Risk description:
This routine identifies services supporting the following extensions to TLS: - Application-Layer Protocol Negotiation (ALPN) - Next Protocol Negotiation (NPN). Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.

Recommendation:
No recommendations to display.

References:
https://tools.ietf.org/html/rfc7301
https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

UNCONFIRMED

port 4280/tcp

The remote service advertises support for the following Network Protocol(s) via the ALPN extension:

SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1

Details

Risk description:
This routine identifies services supporting the following extensions to TLS: - Application-Layer Protocol Negotiation (ALPN) - Next Protocol Negotiation (NPN). Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.

Recommendation:
No recommendations to display.

References:
https://tools.ietf.org/html/rfc7301
https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

PHP Detection (HTTP)

UNCONFIRMED

port 4280/tcp

Detected PHP

Version: 8.4.7
Location: 4280/tcp
CPE: cpe:/a:php:php:8.4.7

Concluded from version/product identification result:
X-Powered-By: PHP/8.4.7

Details

Risk description:
HTTP based detection of PHP.

Recommendation:
No recommendations to display.

Web Application Scanning Consolidation / Info Reporting

UNCONFIRMED

port 4280/tcp

The Hostname/IP "pentest-ground.com" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

Requests to this service are done via HTTP/1.1.

This service seems to be able to host PHP scripts.

This service seems to be able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for web application scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

A possible recursion was detected during web application scanning:

The service is using a relative URL in one or more HTML references where e.g. /file1.html contains <a href="subdir/file2.html"> and a subsequent request for subdir/file2.html is linking to subdir/file2.html. This would resolves to subdir/subdir/file2.html causing a recursion. To work around this counter-measures have been enabled but the service should be fixed as well to not use such problematic links. Below an excerpt of URLs is shown to help identify those issues.

Syntax : URL (HTML link)

```
https://pentest-ground.com:4280/. (dvwa/css/main.css)
https://pentest-ground.com:4280/. (dvwa/images/logo.png)
https://pentest-ground.com:4280/. (dvwa/js/add_event_listeners.js)
https://pentest-ground.com:4280/. (dvwa/js/dvwaPage.js)
https://pentest-ground.com:4280/. (vulnerabilities/brute/)
```

The following directories were used for web application scanning:

```
https://pentest-ground.com:4280/
https://pentest-ground.com:4280/config
https://pentest-ground.com:4280/database
https://pentest-ground.com:4280/docs
https://pentest-ground.com:4280/external
https://pentest-ground.com:4280/vulnerabilities/brute
https://pentest-ground.com:4280/vulnerabilities/captcha
https://pentest-ground.com:4280/vulnerabilities/csp
https://pentest-ground.com:4280/vulnerabilities/csrf
https://pentest-ground.com:4280/vulnerabilities/exec
https://pentest-ground.com:4280/vulnerabilities/fi
https://pentest-ground.com:4280/vulnerabilities/open_redirect
https://pentest-ground.com:4280/vulnerabilities/open_redirect/source
https://pentest-ground.com:4280/vulnerabilities/sqli
https://pentest-ground.com:4280/vulnerabilities/sqli_blind
https://pentest-ground.com:4280/vulnerabilities/upload
https://pentest-ground.com:4280/vulnerabilities/weak_id
https://pentest-ground.com:4280/vulnerabilities/xss_d
https://pentest-ground.com:4280/vulnerabilities/xss_r
https://pentest-ground.com:4280/vulnerabilities/xss_s
```

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

The following directories were excluded from web application scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the VT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)"

```
https://pentest-ground.com:4280/docs/graphics/docker
https://pentest-ground.com:4280/dvwa/css
https://pentest-ground.com:4280/dvwa/images
https://pentest-ground.com:4280/dvwa/js
https://pentest-ground.com:4280/icons
https://pentest-ground.com:4280/vulnerabilities/javascript
```

Extraneous phpinfo() output found at:

```
https://pentest-ground.com:4280/phpinfo.php
Concluded from:
<title>PHP 8.4.7 - phpinfo()</title>
<tr><td class="e">Configuration File (php.ini) Path </td>
<h2>PHP Variables</h2>
https://pentest-ground.com:4280/phpinfo.php
Concluded from:
<title>PHP 8.4.7 - phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></head>
<tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/local/etc/php </td></tr>
<h2>PHP Variables</h2>
```

PHP script discloses physical path at:

```
https://pentest-ground.com:4280/instructions.php (/var/www/html/dvwa/includes/dvwaPage.inc.php)
```

https://pentest-ground.com:4280/vulnerabilities/fi/ (/var/www/html/vulnerabilities/fi/source/low.php)
https://pentest-ground.com:4280/vulnerabilities/fi/. (/var/www/html/vulnerabilities/fi/source/low.php)

The following CGIs were discovered:

Syntax : cginame (arguments [default value])

https://pentest-ground.com:4280/ (doc [readme])
https://pentest-ground.com:4280/login.php (username [] password [] Login [Login] user_token [***replaced***])
https://pentest-ground.com:4280/security.php (security [] seclev_submit [Submit] user_token [***replaced***])
https://pentest-ground.com:4280/setup.php (create_db [Create / Reset Database] user_token [***replaced***])
https://pentest-ground.com:4280/vulnerabilities/brute/ (username [] password [] Login [Login])
https://pentest-ground.com:4280/vulnerabilities/captcha/ (step [1] password_new [] password_conf [] Change [Change])
https://pentest-ground.com:4280/vulnerabilities/csrf/ (password_new [] password_conf [] Change [Change])
https://pentest-ground.com:4280/vulnerabilities/exec/ (ip [] Submit [Submit])
https://pentest-ground.com:4280/vulnerabilities/fi/. (page [include.php])
https://pentest-ground.com:4280/vulnerabilities/open_redirect/source/low.php (redirect=info.php?id [1])
https://pentest-ground.com:4280/vulnerabilities/sqli/ (id [] Submit [Submit])
https://pentest-ground.com:4280/vulnerabilities/sqli_blind/ (id [] Submit [Submit])
https://pentest-ground.com:4280/vulnerabilities/upload/ (MAX_FILE_SIZE [100000] uploaded [] Upload [Upload])
https://pentest-ground.com:4280/vulnerabilities/xss_r/ (name [])

Details

Risk description:
The script consolidates and reports various information for web application (formerly called 'CGI') scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community forum.

Recommendation:
No recommendations to display.

References:
https://forum.greenbone.net/c/vulnerability-tests/7

Web Application Scanning Consolidation / Info Reporting

UNCONFIRMED

port 5013/tcp

The Hostname/IP "pentest-ground.com" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

Requests to this service are done via HTTP/1.1.

This service seems to be able to host PHP scripts.

This service seems to be able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for web application scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

The following directories were used for web application scanning:

https://pentest-ground.com:5013/
https://pentest-ground.com:5013/#
https://pentest-ground.com:5013/static

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

The following directories were excluded from web application scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the VT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)"

https://pentest-ground.com:5013/static/bootstrap/css
https://pentest-ground.com:5013/static/bootstrap/js
https://pentest-ground.com:5013/static/images
https://pentest-ground.com:5013/static/jquery

Details

Risk description:
The script consolidates and reports various information for web application (formerly called 'CGI') scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to

directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community forum.

Recommendation:

No recommendations to display.

References:

https://forum.greenbone.net/c/vulnerability-tests/7

Web Application Scanning Consolidation / Info Reporting

UNCONFIRMED

port 7001/tcp

The Hostname/IP "pentest-ground.com" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

Requests to this service are done via HTTP/1.1.

This service seems to be able to host PHP scripts.

This service seems to be able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for web application scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

The following files/directories require authentication and are tested (if enabled) by the script "HTTP Brute Force Logins with default Credentials (OID: 1.3.6.1.4.1.25623.1.0.108041)":

https://pentest-ground.com:7001/management

The following directories were used for web application scanning:

https://pentest-ground.com:7001/

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

The following directories were excluded from web application scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the VT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)"

https://pentest-ground.com:7001/console/css
https://pentest-ground.com:7001/console/framework/skins/wlsconsole/css
https://pentest-ground.com:7001/console/framework/skins/wlsconsole/images

The following CGIs were discovered:

Syntax : cginame (arguments [default value])

https://pentest-ground.com:7001/console/j_security_check (j_username [] j_password [] j_character_encoding [UTF-8])

Details

Risk description:

The script consolidates and reports various information for web application (formerly called 'CGI') scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community forum.

Recommendation:

No recommendations to display.

References:

https://forum.greenbone.net/c/vulnerability-tests/7

Web Application Scanning Consolidation / Info Reporting

UNCONFIRMED

port 81/tcp

The Hostname/IP "pentest-ground.com" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

Requests to this service are done via HTTP/1.1.

This service seems to be able to host PHP scripts.

This service seems to be able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for web application scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

A possible recursion was detected during web application scanning:

The service is using a relative URL in one or more HTML references where e.g. /file1.html contains <a href="subdir/file2.html"> and a subsequent request for subdir/file2.html is linking to subdir/file2.html. This would resolves to subdir/subdir/file2.html causing a recursion. To work around this counter-measures have been enabled but the service should be fixed as well to not use such problematic links. Below an excerpt of URLs is shown to help identify those issues.

Syntax : URL (HTML link)

https://pentest-ground.com:81/services (images/arrow-black.png)

The following directories were used for web application scanning:

https://pentest-ground.com:81/
https://pentest-ground.com:81/#
https://pentest-ground.com:81/1
https://pentest-ground.com:81/2

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

The following directories were excluded from web application scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the VT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was:
"/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)"

https://pentest-ground.com:81/images
https://pentest-ground.com:81/static/css
https://pentest-ground.com:81/static/images
https://pentest-ground.com:81/static/js

The following CGIs were discovered:

Syntax : cginame (arguments [default value])

https://pentest-ground.com:81/ ()
https://pentest-ground.com:81/# ()
https://pentest-ground.com:81/1/edit ()
https://pentest-ground.com:81/2/edit ()
https://pentest-ground.com:81/about ()
https://pentest-ground.com:81/blog ()
https://pentest-ground.com:81/contact ()
https://pentest-ground.com:81/login (remember_me [true] password [] username [])
https://pentest-ground.com:81/post/1 ()
https://pentest-ground.com:81/post/2 ()
https://pentest-ground.com:81/services ()

Details

Risk description:
The script consolidates and reports various information for web application (formerly called 'CGI') scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community forum.

Recommendation:
No recommendations to display.

References:
https://forum.greenbone.net/c/vulnerability-tests/7

Web Application Scanning Consolidation / Info Reporting

port 9000/tcp

UNCONFIRMED

The Hostname/IP "pentest-ground.com" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

Requests to this service are done via HTTP/1.1.

This service seems to be able to host PHP scripts.

This service seems to be able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for web application scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

The following directories were used for web application scanning:

https://pentest-ground.com:9000/
https://pentest-ground.com:9000/#

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

The following directories were excluded from web application scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the VT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)"

https://pentest-ground.com:9000/img

Details

Risk description:
The script consolidates and reports various information for web application (formerly called 'CGI') scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community forum.

Recommendation:
No recommendations to display.

References:
https://forum.greenbone.net/c/vulnerability-tests/7

Web Application Scanning Consolidation / Info Reporting

UNCONFIRMED

port 443/tcp

The Hostname/IP "pentest-ground.com" was used to access the remote host.

Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.

Requests to this service are done via HTTP/1.1.

This service seems to be able to host PHP scripts.

This service seems to be able to host ASP scripts.

The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.1)" was used to access the remote host.

Historic /scripts and /cgi-bin are not added to the directories used for web application scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.

A possible recursion was detected during web application scanning:

The service is using a relative URL in one or more HTML references where e.g. /file1.html contains <a href="subdir/file2.html"> and a subsequent request for subdir/file2.html is linking to subdir/file2.html. This would resolves to subdir/subdir/file2.html causing a recursion. To work around this counter-measures have been enabled but the service should be fixed as well to not use such problematic links. Below an excerpt of URLs is shown to help identify those issues.

Syntax : URL (HTML link)

https://pentest-ground.com/ (img/CopyIcon.svg)
https://pentest-ground.com/# (img/CopyIcon.svg)

The following directories were used for web application scanning:

https://pentest-ground.com/
https://pentest-ground.com/#

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

The following directories were excluded from web application scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the VT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)"

https://pentest-ground.com/img

Details

Risk description:

The script consolidates and reports various information for web application (formerly called 'CGI') scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community forum.

Recommendation:

No recommendations to display.

References:

https://forum.greenbone.net/c/vulnerability-tests/7

Domain name servers are not vulnerable to DNS Server Zone Transfer Information Disclosure (AXFR) vulnerability

Version-based detection found no vulnerabilities for nginx 1.27.5

port 443/tcp

Version-based detection found no vulnerabilities for nginx 1.27.5

port 4280/tcp

Version-based detection found no vulnerabilities for OpenSSH 8.4p1 Debian 5+deb11u5

port 4445/tcp

Version-based detection found no vulnerabilities for nginx 1.27.5

port 5013/tcp

Version-based detection found no vulnerabilities on port 7001

port 7001/tcp

Version-based detection found no vulnerabilities for nginx 1.27.5

port 9000/tcp

Scan coverage information

List of tests performed (204/204)

- ✓ Running IP information lookup phase
- ✓ Performing DNS enumeration
- ✓ Performing OS detection
- ✓ Running port discovery
- ✓ Scanning for publicly exposed SSH service
- ✓ Scanning for publicly exposed Redis service
- ✓ Checking for web redirect on port 80
- ✓ Attempting zone transfer against name servers...
- ✓ Scanning for Redis key-value store technology if it reached End-of-Life (EOL) on port 6379
- ✓ Fingerprinting website for technologies on port 81
- ✓ Scanning for vulnerabilities of jQuery on port 81
- ✓ Fingerprinting website for technologies on port 443
- ✓ Searching for version-based vulnerabilities on port 443
- ✓ Fingerprinting website for technologies on port 4280
- ✓ Searching for version-based vulnerabilities on port 4280
- ✓ Searching for version-based vulnerabilities on port 4445
- ✓ Fingerprinting website for technologies on port 5013
- ✓ Searching for version-based vulnerabilities on port 5013

- ✓ Scanning for vulnerabilities of Redis Key-Value Store on port 6379
- ✓ Fingerprinting website for technologies on port 7001
- ✓ Searching for version-based vulnerabilities on port 7001
- ✓ Fingerprinting website for technologies on port 9000
- ✓ Searching for version-based vulnerabilities on port 9000
- ✓ Checking for Redis - Remote Code Execution (CVE-2022-0543) (Sniper Module) on port 6379
- ✓ Checking for Oracle Weblogic - Remote Code Execution (CVE-2018-2894) (Sniper Module) on port 7001
- ✓ Checking for Oracle WebLogic - Remote Code Execution (CVE-2023-21839) (Sniper Module) on port 7001
- ✓ Checking for Oracle Fusion Middleware WebLogic Server Administration Console - Remote Code Execution (CVE-2020-14883) on port 7001
- ✓ Checking for DVWA Default Login on port 4280
- ✓ Checking for Redis - Default Logins on port 6379
- ✓ Checking for PHPinfo Page on port 4280
- ✓ Checking for GraphQL Alias-based Batching on port 5013
- ✓ Checking for GraphQL Array-based Batching on port 5013
- ✓ Checking for GraphQL Field Suggestion Information Disclosure on port 5013
- ✓ Checking for Missing Subresource Integrity on port 443
- ✓ Checking for Missing Subresource Integrity on port 5013
- ✓ Checking for Missing Subresource Integrity on port 9000
- ✓ Checking for Missing Subresource Integrity on port 81
- ✓ Checking for Redis Server - Unauthenticated Access on port 6379
- ✓ Checking for OpenSSH Service on port 4445
- ✓ Checking for Redis Info on port 6379
- ✓ Checking for Redis Info on port 6379
- ✓ Checking for SSH Auth Methods on port 4445
- ✓ Checking for SSH Server Software Enumeration on port 4445
- ✓ Checking for SSH Password-based Authentication on port 4445
- ✓ Checking for SSH SHA-1 HMAC Algorithms Enabled on port 4445
- ✓ Checking for TLS Version on port 443
- ✓ Checking for TLS Version on port 9000
- ✓ Checking for TLS Version on port 5013
- ✓ Checking for TLS Version on port 7001
- ✓ Checking for TLS Version on port 81
- ✓ Checking for TLS Version on port 4280
- ✓ Checking for TLS Version on port 443
- ✓ Checking for TLS Version on port 9000
- ✓ Checking for TLS Version on port 5013
- ✓ Checking for TLS Version on port 81
- ✓ Checking for TLS Version on port 7001
- ✓ Checking for TLS Version on port 4280
- ✓ Checking for WAF on port 81
- ✓ Checking for WAF on port 5013
- ✓ Checking for WAF on port 443
- ✓ Checking for WAF on port 9000
- ✓ Checking for WAF on port 4280
- ✓ Checking for OpenAPI on port 9000
- ✓ Checking for RDAP WHOIS on port 6379
- ✓ Checking for RDAP WHOIS on port 6379
- ✓ Checking for RDAP WHOIS on port 6379
- ✓ Checking for RDAP WHOIS on port 6379
- ✓ Checking for RDAP WHOIS on port 6379
- ✓ Checking for RDAP WHOIS on port 6379
- ✓ Checking for RDAP WHOIS on port 4280
- ✓ Checking for RDAP WHOIS on port 4280
- ✓ Checking for RDAP WHOIS on port 4280
- ✓ Checking for RDAP WHOIS on port 4280
- ✓ Checking for RDAP WHOIS on port 4280
- ✓ Checking for RDAP WHOIS on port 4280
- ✓ Checking for RDAP WHOIS on port 4445
- ✓ Checking for RDAP WHOIS on port 4445
- ✓ Checking for RDAP WHOIS on port 4445
- ✓ Checking for RDAP WHOIS on port 4445
- ✓ Checking for RDAP WHOIS on port 4445
- ✓ Checking for RDAP WHOIS on port 4445
- ✓ Checking for RDAP WHOIS on port 443
- ✓ Checking for RDAP WHOIS on port 443
- ✓ Checking for RDAP WHOIS on port 443
- ✓ Checking for RDAP WHOIS on port 443
- ✓ Checking for RDAP WHOIS on port 443
- ✓ Checking for RDAP WHOIS on port 443
- ✓ Checking for RDAP WHOIS on port 81
- ✓ Checking for RDAP WHOIS on port 5013
- ✓ Checking for RDAP WHOIS on port 81
- ✓ Checking for RDAP WHOIS on port 5013
- ✓ Checking for RDAP WHOIS on port 5013
- ✓ Checking for RDAP WHOIS on port 5013
- ✓ Checking for RDAP WHOIS on port 5013

- ✓ Checking for RDAP WHOIS on port 5013
- ✓ Checking for RDAP WHOIS on port 81
- ✓ Checking for RDAP WHOIS on port 81
- ✓ Checking for RDAP WHOIS on port 81
- ✓ Checking for RDAP WHOIS on port 81
- ✓ Checking for RDAP WHOIS on port 7001
- ✓ Checking for RDAP WHOIS on port 7001
- ✓ Checking for RDAP WHOIS on port 7001
- ✓ Checking for RDAP WHOIS on port 9000
- ✓ Checking for RDAP WHOIS on port 7001
- ✓ Checking for RDAP WHOIS on port 9000
- ✓ Checking for RDAP WHOIS on port 9000
- ✓ Checking for RDAP WHOIS on port 7001
- ✓ Checking for RDAP WHOIS on port 9000
- ✓ Checking for RDAP WHOIS on port 7001
- ✓ Checking for RDAP WHOIS on port 9000
- ✓ Checking for RDAP WHOIS on port 9000
- ✓ Checking for Oracle WebLogic Server - Remote Code Execution (CVE-2020-2551) on port 7001
- ✓ Checking for Oracle WebLogic Login Panel on port 7001
- ✓ Checking for GraphQL CSRF / GET method on port 5013
- ✓ Checking for HTML form on port 81
- ✓ Checking for Email Extractor on port 5013
- ✓ Checking for Nginx version on port 5013
- ✓ Checking for Nginx version on port 4280
- ✓ Checking for PHP on port 4280
- ✓ Checking for Nginx version on port 9000
- ✓ Checking for Email Extractor on port 81
- ✓ Checking for Nginx version on port 81
- ✓ Checking for Nginx version on port 443
- ✓ Checking for FingerprintHub Technology Fingerprint on port 7001
- ✓ Checking for Wappalyzer Technology on port 4280
- ✓ Checking for Wappalyzer Technology on port 9000
- ✓ Checking for Wappalyzer Technology on port 5013
- ✓ Checking for FingerprintHub Technology Fingerprint on port 443
- ✓ Checking for Wappalyzer Technology on port 443
- ✓ Checking for Wappalyzer Technology on port 81
- ✓ Checking for README.md file disclosure on port 4280
- ✓ Checking for Find Pages with Old Copyright Dates on port 81
- ✓ Checking for SSL DNS Names on port 9000
- ✓ Checking for SSL Certificate Issuer on port 9000
- ✓ Checking for SSL DNS Names on port 4280
- ✓ Checking for SSL Certificate Issuer on port 4280
- ✓ Checking for SSL DNS Names on port 5013
- ✓ Checking for SSL DNS Names on port 443
- ✓ Checking for SSL Certificate Issuer on port 5013
- ✓ Checking for SSL Certificate Issuer on port 443
- ✓ Checking for SSL DNS Names on port 81
- ✓ Checking for SSL Certificate Issuer on port 81
- ✓ Checking for SSL DNS Names on port 7001
- ✓ Checking for SSL Certificate Issuer on port 7001
- ✓ Checking for Service Detection with 'GET' Request on port 6379
- ✓ Checking for SSH Protocol Algorithms Supported on port 4445
- ✓ Checking for SSH Server type and version on port 4445
- ✓ Checking for OpenSSH Detection Consolidation
- ✓ Checking for Redis Server Detection (TCP) on port 6379
- ✓ Checking for Redis Server No Password on port 6379
- ✓ Checking for SSH Protocol Versions Supported on port 4445
- ✓ Checking for TCP Timestamps Information Disclosure
- ✓ Checking for Apache HTTP Server Detection Consolidation
- ✓ Checking for SSL/TLS: HTTP Public Key Pinning (HPKP) Missing on port 443
- ✓ Checking for SSL/TLS: HTTP Public Key Pinning (HPKP) Missing on port 9000
- ✓ Checking for SSL/TLS: HTTP Public Key Pinning (HPKP) Missing on port 81
- ✓ Checking for SSL/TLS: HTTP Public Key Pinning (HPKP) Missing on port 7001
- ✓ Checking for SSL/TLS: HTTP Public Key Pinning (HPKP) Missing on port 5013
- ✓ Checking for SSL/TLS: HTTP Strict Transport Security (HSTS) Missing on port 7001
- ✓ Checking for SSL/TLS: HTTP Strict Transport Security (HSTS) Missing on port 5013
- ✓ Checking for SSL/TLS: HTTP Strict Transport Security (HSTS) Missing on port 443
- ✓ Checking for SSL/TLS: HTTP Strict Transport Security (HSTS) Missing on port 9000
- ✓ Checking for SSL/TLS: HTTP Strict Transport Security (HSTS) Missing on port 81
- ✓ Checking for SSL/TLS: Report Medium Cipher Suites on port 4280
- ✓ Checking for SSL/TLS: Report Medium Cipher Suites on port 9000
- ✓ Checking for SSL/TLS: Report Medium Cipher Suites on port 81
- ✓ Checking for SSL/TLS: Report Medium Cipher Suites on port 7001
- ✓ Checking for SSL/TLS: Report Medium Cipher Suites on port 5013
- ✓ Checking for SSL/TLS: Report Medium Cipher Suites on port 443
- ✓ Checking for SSL/TLS: Report Non Weak Cipher Suites on port 81
- ✓ Checking for SSL/TLS: Report Non Weak Cipher Suites on port 9000

- ✓ Checking for SSL/TLS: Report Non Weak Cipher Suites on port 4280
- ✓ Checking for SSL/TLS: Report Non Weak Cipher Suites on port 443
- ✓ Checking for SSL/TLS: Report Non Weak Cipher Suites on port 5013
- ✓ Checking for SSL/TLS: Report Non Weak Cipher Suites on port 7001
- ✓ Checking for SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites on port 81
- ✓ Checking for SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites on port 9000
- ✓ Checking for SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites on port 4280
- ✓ Checking for SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites on port 443
- ✓ Checking for SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites on port 5013
- ✓ Checking for SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites on port 7001
- ✓ Checking for SSL/TLS: Report Supported Cipher Suites on port 7001
- ✓ Checking for SSL/TLS: Report Supported Cipher Suites on port 4280
- ✓ Checking for SSL/TLS: Report Supported Cipher Suites on port 443
- ✓ Checking for SSL/TLS: Report Supported Cipher Suites on port 9000
- ✓ Checking for SSL/TLS: Report Supported Cipher Suites on port 81
- ✓ Checking for SSL/TLS: Report Supported Cipher Suites on port 5013
- ✓ Checking for Weak MAC Algorithm(s) Supported (SSH) on port 4445
- ✓ Checking for Oracle WebLogic Server Detection Consolidation
- ✓ Checking for SSL/TLS: NPN / ALPN Extension and Protocol Support Detection on port 9000
- ✓ Checking for SSL/TLS: NPN / ALPN Extension and Protocol Support Detection on port 81
- ✓ Checking for SSL/TLS: NPN / ALPN Extension and Protocol Support Detection on port 5013
- ✓ Checking for SSL/TLS: NPN / ALPN Extension and Protocol Support Detection on port 443
- ✓ Checking for SSL/TLS: NPN / ALPN Extension and Protocol Support Detection on port 4280
- ✓ Checking for PHP Detection (HTTP) on port 4280
- ✓ Checking for Web Application Scanning Consolidation / Info Reporting on port 4280
- ✓ Checking for Web Application Scanning Consolidation / Info Reporting on port 5013
- ✓ Checking for Web Application Scanning Consolidation / Info Reporting on port 7001
- ✓ Checking for Web Application Scanning Consolidation / Info Reporting on port 81
- ✓ Checking for Web Application Scanning Consolidation / Info Reporting on port 9000
- ✓ Checking for Web Application Scanning Consolidation / Info Reporting on port 443
- ✓ Checking for phpinfo() Output Reporting (HTTP) on port 4280
- ✓ Checking for Free Articles Directory RFI Vulnerability on port 4280
- ✓ Checking for awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check on port 4280

Scan parameters

Target:	pentest-ground.com
Preset:	Custom
Scanning engines:	Version_based, Sniper, Nuclei, Openvas
Check alive:	True
Extensive modules:	False
Protocol type:	TCP
Ports to scan:	Full port range