API Vulnerability Scanner Report

✔ http://rest.testinvicti.com/jwt/

Summary

Overall risk level:
Critical

Risk ratings:

Critical:	2
High:	3
Medium:	1
Low:	7
Info:	44

Scan information:

Start time:	Feb 12, 2025 / 09:48:50 UTC+02
Finish time:	Feb 12, 2025 / 09:58:10 UTC+02
Scan duration:	9 min, 20 sec
Tests performed:	57/57
Scan status:	Finished

Findings

SQL Injection

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack
http://rest.testinvicti.com/jwt/api/users/test_username'	GET	Url Path	Injecting the value `'` in the URL path generated the following error(s) in the response: `SQL errorPDOException: SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''test_username''' at line 1 in /var/www/src/routes/users.php:67` Request / Response	

Details

Risk description:
The risk exists that an attacker gains unauthorized access to the information from the database of the application. He could extract and alter information such as: application usernames, passwords, client information and other application specific data.

Recommendation:
We recommend implementing a validation mechanism for all the data received from the users.
The best way to protect against SQL Injection is to use prepared statements for every SQL query performed on the database.
Otherwise, the user input can also be sanitized using dedicated methods such as: mysqli_real_escape_string.

References:
https://owasp.org/www-community/attacks/SQL_Injection
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Classification:
CWE : CWE-89
OWASP Top 10 - 2017 : A1 - Injection
OWASP Top 10 - 2021 : A3 - Injection

OS Command Injection

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack

http://rest.testinvicti.com/jwt/api/users/test_username	PUT	email (Body Parameter)	Injected the `echo ttp1739346686.63417|rev|sed -e 's/^/ptt/' -e 's/\./dot/'|tr a-z A-Z` command in the **email body parameter** and found the expected command output (`PTT71436DOT6866439371PTT`) in the response To validate the vulnerability, we extracted the kernel version and the hostname of the Unix machine. The kernel version is **5.4.0-1092-aws**, and the hostname is **0ac63cf9ce6c**. Request / Response	

Details

Risk description:
The risk is that an attacker can use the application to run OS commands with the privileges of the vulnerable application. This could lead (but not limited) to Remote Code Execution, Denial of Service, Sensitive Information Disclosure, Sensitive Information Deletion.

Recommendation:
There are multiple ways to mitigate this attack:
- avoid calling OS commands directly (use built-in library functions) - escape values added to OS commands specific to each OS
- implement parametrization in conjunction with Input Validation (segregate data by command; implement Positive or whitelist input validation; White list Regular Expression)
In order to provide Defense in Depth, we also recommend to allocate the lowest privileges to web applications.

References:
https://owasp.org/www-community/attacks/Command_Injection
https://cheatsheetseries.owasp.org/cheatsheets/OS_Command_Injection_Defense_Cheat_Sheet.html

Classification:
CWE : CWE-78
OWASP Top 10 - 2017 : A1 - Injection
OWASP Top 10 - 2021 : A3 - Injection

JWT Weak Secret Key

CONFIRMED

URL	Method	Parameters	Evidence
http://rest.testinvicti.com/jwt/	GET	**Headers:** Authorization=Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsImtpZCI6InNlY3JldC50eHQifQ.eyJ1c2VyIjoidGVzdCJ9.jqBFzyBB68KWiOvEJhcaDgMY0Gea-t0KNnf-fR2loyc User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36	The JWT (header `{'typ': 'JWT', 'alg': 'HS256', 'kid': 'secret.txt'}` , payload `{'user': 'test'}`) was signed with a weak secret key. We found its value, `supersecret` , in a dictionary of common secrets.

Details

Risk description:
The risk is that an attacker can forge a valid JWT by guessing or brute-forcing the secret key, gaining unauthorized access to the application. This can lead to impersonating another user, usually resulting in privilege escalation.

Recommendation:
Use strong, random, and unique secret keys for signing JWTs. Avoid using easily guessable, common, or default strings as keys. Implement a robust key management system to securely store and rotate keys. Regularly review and update keys to ensure their security.

References:
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/06-Session_Management_Testing/10-Testing_JSON_Web_Tokens

Classification:
CWE : CWE-347
OWASP Top 10 - 2017 : A5 - Broken Access Control
OWASP Top 10 - 2021 : A2 - Cryptographic Failures

Local File Inclusion

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack

http://rest.testinvicti.com/jwt/api/comments/21	PUT	comment (Body Parameter)	We found a Local File Inclusion vulnerability in the **comment body parameter**.We managed to read the contents of two files.
			First, we tested for the vulnerability by injecting the payload: `/proc/cpuinfo`. We extracted the data:
			`processor : 0`
			`vendor_id : GenuineIntel`
			`cpu family : 6`
			`model : 79`
			`model name : Intel`
			`stepping : 1`
			`microcode : 0x5003801`
			`processor : 1`
			`vendor_id : GenuineIntel`
			`cpu family : 6`
			Additionally, we validated the vulnerability by injecting the payload: `/proc/1/sched`. The extracted data was:
			`se.exec_start : 3365298.605765`
			`se.vruntime : 125673.795813`
			`se.sum_exec_runtime : 696.115095`
			`se.nr_migrations : 1`
			`nr_switches : 4196`
			`nr_voluntary_switches : 3952`
			`nr_involuntary_switches : 244`
			`se.load.weight : 1048576`
			`se.avg.load_sum : 30`
			`se.avg.util_sum : 30720`
			Request / Response	

Details

Risk description:
The risk exists that an attacker can manipulate the affected parameter in order to load and sometimes execute any locally stored file. This could lead to reading arbitrary files, code execution, Cross-Site Scripting, denial of service, sensitive information disclosure.

Recommendation:
The most effective solution to eliminating file inclusion vulnerabilities is to avoid passing raw user-submitted input to any filesystem API. If this is not possible, the application can maintain a white list of files that may be included by the page, and then check to see if the user input matches against any of the entries in the white list. Any request containing an invalid identifier has to be rejected. In this way, there is no attack surface for malicious users to manipulate the path.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion

Classification:
CWE : CWE-22
OWASP Top 10 - 2017 : A1 - Injection
OWASP Top 10 - 2021 : A1 - Broken Access Control

Vulnerabilities found for server-side software

UNCONFIRMED

Risk Level	CVSS	CVE	Summary	Affected software

	9.8	CVE-2023-25690	Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.	http_server 2.4.25
	9.8	CVE-2024-38474	Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.	http_server 2.4.25
	9.8	CVE-2024-38476	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue.	http_server 2.4.25
	9	CVE-2022-36760	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.	http_server 2.4.25
	7.8	CVE-2019-9517	Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.	http_server 2.4.25
	7.5	CVE-2017-8923	The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.	php 7.1.26
	7.5	CVE-2019-9641	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.	php 7.1.26
	7.5	CVE-2019-13224	A use-after-free in onig_new_deluxe() in regext.c in Oniguruma 6.9.2 allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression. The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe(). Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust.	php 7.1.26
	7.5	CVE-2019-11043	In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.	php 7.1.26

	6.8	CVE-2019-9675	An issue was discovered in PHP 7.x before 7.1.27 and 7.3.x before 7.3.3. phar_tar_writeheaders_int in ext/phar/tar.c has a buffer overflow via a long link value. NOTE: The vendor indicates that the link value is used only when an archive contains a symlink, which currently cannot happen: "This issue allows theoretical compromise of security, but a practical attack is usually impossible.	php 7.1.26

Details

Risk description:
The risk is that an attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Recommendation:
In order to eliminate the risk of these vulnerabilities, we recommend you check the installed software version and upgrade to the latest version.

Classification:
CWE : CWE-1026
OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities
OWASP Top 10 - 2021 : A6 - Vulnerable and Outdated Components

Communication is not secure

CONFIRMED

URL	Response URL	Evidence
http://rest.testinvicti.com/jwt/	http://rest.testinvicti.com/jwt/	Communication is made over unsecure, unencrypted HTTP.

Details

Risk description:
The risk is that an attacker who manages to intercept the communication at the network level can read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:
We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

Classification:
CWE : CWE-311
OWASP Top 10 - 2017 : A3 - Sensitive Data Exposure
OWASP Top 10 - 2021 : A4 - Insecure Design

Missing security header: X-Content-Type-Options

CONFIRMED

URL	Evidence
http://rest.testinvicti.com/jwt/api/users	Response headers do not include the X-Content-Type-Options HTTP security header Request / Response

Details

Risk description:
The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

Recommendation:
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
http://rest.testinvicti.com/jwt/api/users	Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response

Details

Risk description:
The risk is that if the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
http://rest.testinvicti.com/jwt/api/users	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response. Request / Response

Details

Risk description:
The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

References:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Internal Server Error Found

CONFIRMED

URL	Method	Parameters	Evidence
http://rest.testinvicti.com/jwt/	GET	**Headers:** Authorization=Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsImtpZCI6InNlY3JldC50eHQifQ.eyJ1c2VyIjoidGVzdCJ9.jqBFzyBB68KWiOvEJhcaDgMY0Gea-t0KNnf-fR2Ioyc User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 X-HTTP-Me...	Response has an internal server error status code: 500 Request / Response

Details

Risk description:
The risk exists that attackers could utilize information revealed in Internal Server Error messages to mount more targeted and effective attacks. Detailed error messages could, for example, expose a path traversal weakness (CWE-22) or other exploitable system vulnerabilities.

Recommendation:

Ensure that error messages only contain minimal details that are useful to the intended audience, and nobody else. The messages need to strike the balance between being too cryptic and not being cryptic enough. They should not necessarily reveal the methods that were used to determine the error. Such detailed information can be used to refine the original attack to increase the chances of success. If errors must be tracked in some detail, capture them in log messages - but consider what could occur if the log messages can be viewed by attackers. Avoid recording highly sensitive information such as passwords in any form. Avoid inconsistent messaging that might accidentally tip off an attacker about internal state, such as whether a username is valid or not.

Classification:

CWE : CWE-209
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Screenshot:

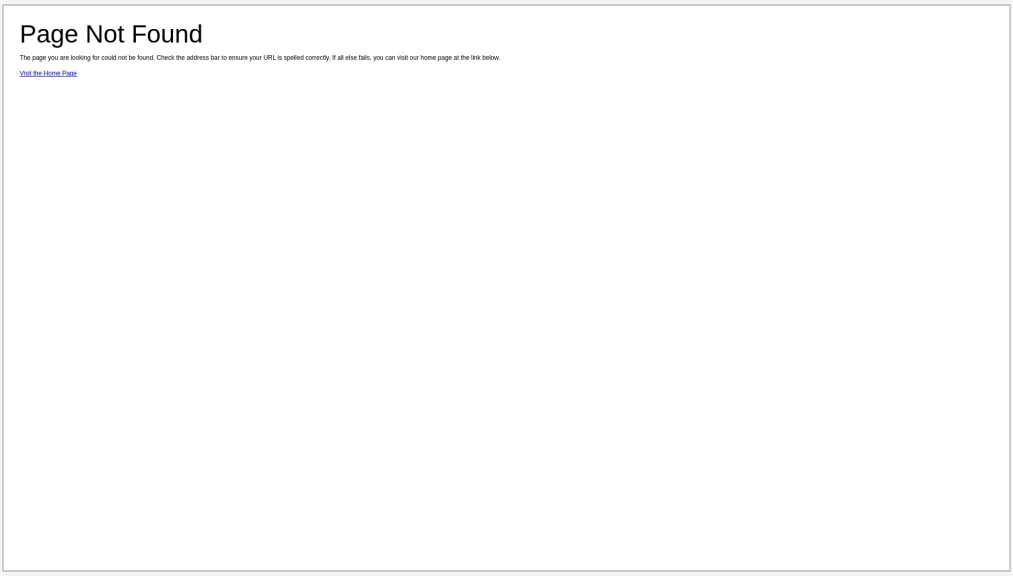

Figure 2. Internal Error

Server software and technology found

UNCONFIRMED

Software / Version	Category
Debian	Operating systems
Apache HTTP Server 2.4.25	Web servers
PHP 7.1.26	Programming languages

Details

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.

References:

https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:

OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Screenshot:

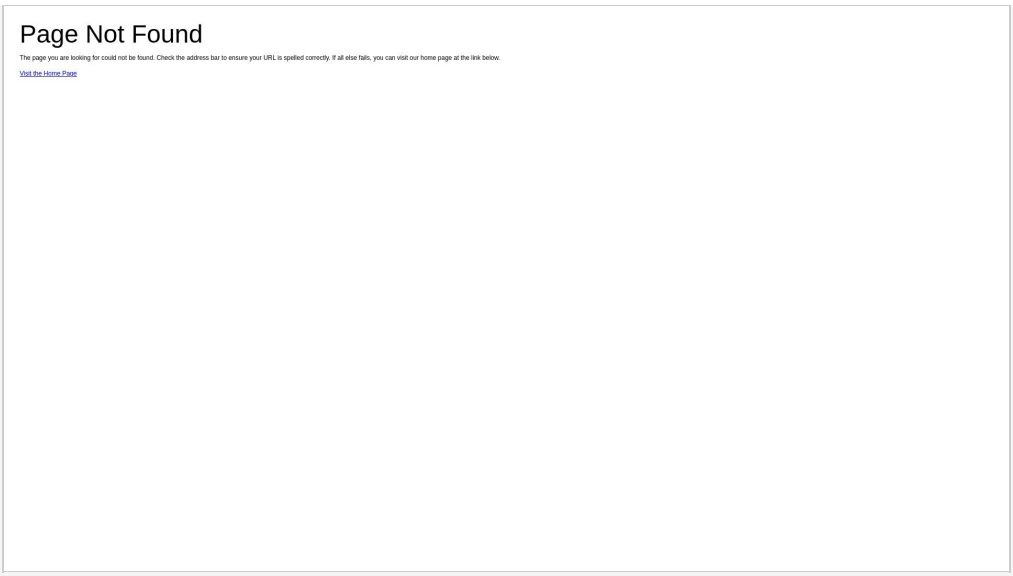

Figure 3. Website Screenshot

Error message containing sensitive information

UNCONFIRMED

URL	Method	Parameters	Evidence
http://rest.testinvicti.com/jwt/api/users/test_username'	GET	**Headers:** User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36	Error message **You have an error in your SQL syntax** found in: `TE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL` Request / Response

Details

Risk description:
The risk is that an attacker may use the contents of error messages to help launch another, more focused attack. For example, an attempt to exploit a path traversal weakness (CWE-22) might yield the full pathname of the installed application.

Recommendation:
It is recommended treating all exceptions of the application flow. Ensure that error messages only contain minimal details.

Classification:
CWE : CWE-209
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A4 - Insecure Design

Enumerable Parameter

UNCONFIRMED

URL	Method	Vulnerable Parameter	Evidence
http://rest.testinvicti.com/jwt/api/comments/20	GET	Url Path	The **URL path** appears to contain an enumerable numeric part. We modified its initial value **21** to **20** and the two responses were **11%** similar. The parameter may introduce an Insecure Direct Object Reference (IDOR) vulnerability. Request / Response
http://rest.testinvicti.com/jwt/api/posts/20	GET	Url Path	The **URL path** appears to contain an enumerable numeric part. We modified its initial value **21** to **20** and the two responses were **45%** similar. The parameter may introduce an Insecure Direct Object Reference (IDOR) vulnerability. Request / Response
http://rest.testinvicti.com/jwt/api/posts/4/comments	GET	Url Path	The **URL path** appears to contain an enumerable numeric part. We modified its initial value **5** to **4** and the two responses were **1%** similar. The parameter may introduce an Insecure Direct Object Reference (IDOR) vulnerability. Request / Response

http://rest.testinvicti.com/jwt/api/users/ena6/posts	GET	Url Path	The **URL path** appears to contain an enumerable numeric part. We modified its initial value **ena07** to **ena6** and the two responses were **10%** similar. The parameter may introduce an Insecure Direct Object Reference (IDOR) vulnerability. Request / Response

Details

Risk description:
The vulnerability allows attackers to brute-force parameter values to uncover and access unauthorized resources and functionalities.

Recommendation:
Ensure that parameter values would not reveal sensitive information and that the application properly checks the user's authorization to access the resource. Also, the resource IDs should not be predictable.

References:
Testing for Insecure Direct Object References

Classification:
CWE : CWE-284
OWASP Top 10 - 2017 : A5 - Broken Access Control
OWASP Top 10 - 2021 : A1 - Broken Access Control

Security.txt file is missing

CONFIRMED

URL
Missing: http://rest.testinvicti.com/.well-known/security.txt

Details

Risk description:
There is no particular risk in not having a security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Authentication scanning: Cookies/Headers method.

URL
http://rest.testinvicti.com/jwt/

Details

Screenshot:

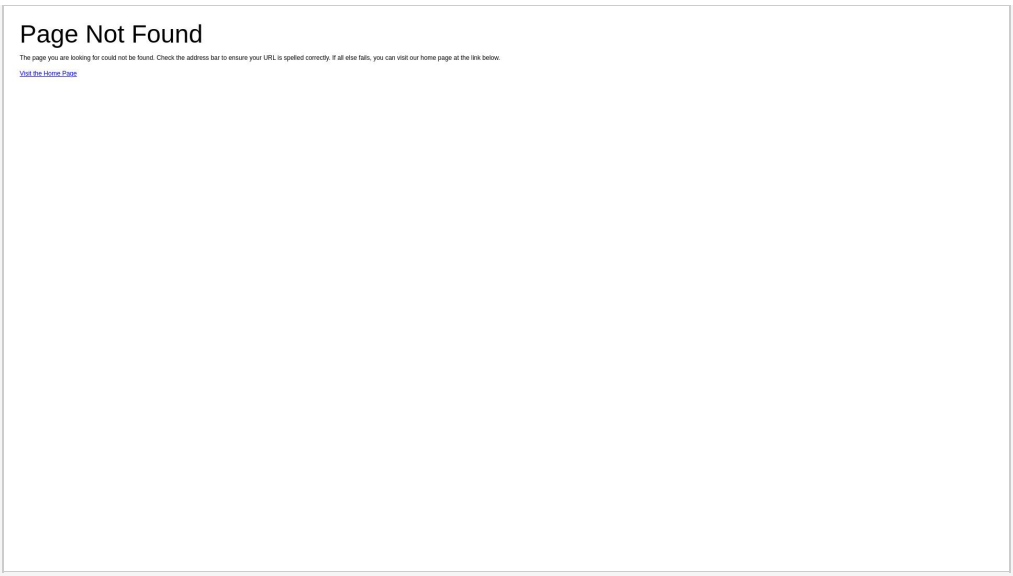

Figure 4. Authentication sequence result

Path Disclosure

UNCONFIRMED

URL	Method	Parameters	Evidence
http://rest.testinvicti.com/jwt/	GET	**Headers:** Authorization=Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsImtpZCI6InNIY3JldC50eHQifQ.eyJ1c2VyIjoidGVzdCJ9.jqBFzyBB68KWiOvEJhcaDgMY0Gea-t0KNnf-fR2loyc User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 X-HTTP-Me...	Operating system paths found in the HTTP response: `/var/www/vendor/slim/slim/Slim/Http/Request.php(267` `/var/www/vendor/slim/slim/Slim/App.php(578` `/var/www/vendor/slim/slim/Slim/App.php(497` `/var/www/src/middlewares/oauth2.php(23` `/var/www/vendor/slim/slim/Slim/MiddlewareAwareTrait.php(117` `/var/www/src/middlewares/jwt.php(25` `/var/www/public/index.php(36` `/var/www/src/middlewares/check_auth_type.php(19` `/var/www/vendor/slim/slim/Slim/MiddlewareAwareTrait.php(70` `/var/www/vendor/slim/slim/Slim/App.php(392` `/var/www/vendor/slim/slim/Slim/Router.php(194` `/var/www/vendor/slim/slim/Slim/Http/Request.php` `/var/www/vendor/slim/slim/Slim/App.php(297` `/var/www/vendor/tuupola/slim-basic-auth/src/HttpBasicAuthentication.php(87` `/var/www/vendor/slim/slim/Slim/DeferredCallable.php(57` Request / Response

http://rest.testinvicti.com/jwt/api/comments	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
			Operating system paths found in the HTTP response:
			`/../../../../../../../../../../etc/httpd/logs/error_log`
			`/../../../../../../../../../../var/log/apache/error.log`
			`/../../../../../../../../../../etc/httpd/logs/access.log`
			`/etc/passwd`
			`/../../../../../../../../../../var/log/lighttpd/access.log`
			`/../../../../../../../../../../var/log/nginx/access.log`
			`/../../../../../../../../../../etc/httpd/logs/error.log`
			`/../../../../../../../../../../opt/lampp/logs/access_log`
			`/../../../../../../../../../../var/log/apache2/error.log`
			`/../../../../../../../../../../etc/passwd`
			`/../../../../../../../../../../var/log/apache2/access.log`
			`/../../../../../../../../../../var/log/apache/access.log`
			Request / Response

http://rest.testinvicti.com/jwt/api/comments	GET	**Query:**
		__proto__.aacB92A=aacB92A
		__proto__=&0[aef4F28]=aef4F28
		__proto__[a2c7bD4]=a2c7bD4
		x.__proto__.aBFaA5F=aBFaA5F
		x[__proto__][adb3BBF]=adb3BBF
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
			Operating system paths found in the HTTP response:
			`/../../../../../../../../../../etc/httpd/logs/error_log`
			`/../../../../../../../../../../var/log/apache/error.log`
			`/../../../../../../../../../../etc/httpd/logs/access.log`
			`/etc/passwd`
			`/../../../../../../../../../../var/log/lighttpd/access.log`
			`/../../../../../../../../../../var/log/nginx/access.log`
			`/../../../../../../../../../../etc/httpd/logs/error.log`
			`/../../../../../../../../../../opt/lampp/logs/access_log`
			`/../../../../../../../../../../var/log/apache2/error.log`
			`/../../../../../../../../../../etc/passwd`
			`/../../../../../../../../../../var/log/apache2/access.log`
			`/../../../../../../../../../../var/log/apache/access.log`
			Request / Response

http://rest.testinvicti.com/jwt/api/posts	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
			Operating system paths found in the HTTP response:
			`/../../../../../../../../../../etc/httpd/logs/error_log`
			`/../../../../../../../../../../var/log/apache/error.log`
			`/../../../../../../../../../../etc/httpd/logs/access.log`
			`/etc/passwd`
			`/../../../../../../../../../../var/log/lighttpd/access.log`
			`/../../../../../../../../../../var/log/nginx/access.log`
			`/../../../../../../../../../../etc/httpd/logs/error.log`
			`/../../../../../../../../../../opt/lampp/logs/access_log`
			`/../../../../../../../../../../var/log/apache2/error.log`
			`/../../../../../../../../../../etc/passwd`
			`/../../../../../../../../../../var/log/apache2/access.log`
			`/../../../../../../../../../../var/log/apache/access.log`
			Request / Response

http://rest.testinvicti.com/jwt/api/posts	GET	**Query:**
		__proto__.a85b978=a85b978
		__proto__=&0[aa2E9b8]=aa2E9b8
		__proto__[aEdbc0A]=aEdbc0A
		x.__proto__.aD4Ca91=aD4Ca91
		x[__proto__][a5bEbEB]=a5bEbEB
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
			Operating system paths found in the HTTP response:
			`/../../../../../../../../../../etc/httpd/logs/error_log`
			`/../../../../../../../../../../var/log/apache/error.log`
			`/../../../../../../../../../../etc/httpd/logs/access.log`
			`/etc/passwd`
			`/../../../../../../../../../../var/log/lighttpd/access.log`
			`/../../../../../../../../../../var/log/nginx/access.log`
			`/../../../../../../../../../../etc/httpd/logs/error.log`
			`/../../../../../../../../../../opt/lampp/logs/access_log`
			`/../../../../../../../../../../var/log/apache2/error.log`
			`/../../../../../../../../../../etc/passwd`
			`/../../../../../../../../../../var/log/apache2/access.log`
			`/../../../../../../../../../../var/log/apache/access.log`
			Request / Response

http://rest.testinvicti.com/jwt/api/posts/5/comments	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
			Operating system paths found in the HTTP response:
			`/../../../../../../../../../../etc/httpd/logs/error_log`
			`/../../../../../../../../../../var/log/apache/error.log`
			`/../../../../../../../../../../etc/httpd/logs/access.log`
			`/etc/passwd`
			`/../../../../../../../../../../var/log/lighttpd/access.log`
			`/../../../../../../../../../../var/log/nginx/access.log`
			`/../../../../../../../../../../etc/httpd/logs/error.log`
			`/../../../../../../../../../../opt/lampp/logs/access_log`
			`/../../../../../../../../../../var/log/apache2/error.log`
			`/../../../../../../../../../../etc/passwd`
			`/../../../../../../../../../../var/log/apache2/access.log`
			`/../../../../../../../../../../var/log/apache/access.log`
			Request / Response

http://rest.testinvicti.com/jwt/api/posts/5/comments	GET	**Query:**
		__proto__.a25C27F=a25C27F
		__proto__=&0[ad57ffd]=ad57ffd
		__proto__[a3BEFA7]=a3BEFA7
		x.__proto__.a9A82bc=a9A82bc
		x[__proto__][a8dcd7d]=a8dcd7d
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
			Operating system paths found in the HTTP response:
			`/../../../../../../../../../../etc/httpd/logs/error_log`
			`/../../../../../../../../../../var/log/apache/error.log`
			`/../../../../../../../../../../etc/httpd/logs/access.log`
			`/etc/passwd`
			`/../../../../../../../../../../var/log/lighttpd/access.log`
			`/../../../../../../../../../../var/log/nginx/access.log`
			`/../../../../../../../../../../etc/httpd/logs/error.log`
			`/../../../../../../../../../../opt/lampp/logs/access_log`
			`/../../../../../../../../../../var/log/apache2/error.log`
			`/../../../../../../../../../../etc/passwd`
			`/../../../../../../../../../../var/log/apache2/access.log`
			`/../../../../../../../../../../var/log/apache/access.log`
			Request / Response

http://rest.testinvicti.com/jwt/api/posts/5/comments	PUT	**Body:**
		content=content
		title=title
		user_id=1123123
		Headers:
		Accept=application/json
		Content-Type=application/json
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
			Operating system paths found in the HTTP response:
			`/../../../../../../../../../../etc/httpd/logs/error_log`
			`/../../../../../../../../../../var/log/apache/error.log`
			`/../../../../../../../../../../etc/httpd/logs/access.log`
			`/etc/passwd`
			`/../../../../../../../../../../var/log/lighttpd/access.log`
			`/../../../../../../../../../../var/log/nginx/access.log`
			`/../../../../../../../../../../etc/httpd/logs/error.log`
			`/../../../../../../../../../../opt/lampp/logs/access_log`
			`/../../../../../../../../../../var/log/apache2/error.log`
			`/../../../../../../../../../../etc/passwd`
			`/../../../../../../../../../../var/log/apache2/access.log`
			`/../../../../../../../../../../var/log/apache/access.log`
			Request / Response

http://rest.testinvicti.com/jwt/api/posts/5/comments	PUT	**Query:**
		__proto__.aaC5b9a=aaC5b9a
		__proto__=&0[a4f8AF5]=a4f8AF5
		__proto__[aC15a4D]=aC15a4D
		x.__proto__.a2fa29B=a2fa29B
		x[__proto__][aD5B5f9]=aD5B5f9
		Body:
		content=content
		title=title
		user_id=1123123
		Headers:
		Accept=application/json
		Content-Type=application/json
		User-Agent=Mozi...
			Operating system paths found in the HTTP response:
			`/../../../../../../../../../../etc/httpd/logs/error_log`
			`/../../../../../../../../../../var/log/apache/error.log`
			`/../../../../../../../../../../etc/httpd/logs/access.log`
			`/etc/passwd`
			`/../../../../../../../../../../var/log/lighttpd/access.log`
			`/../../../../../../../../../../var/log/nginx/access.log`
			`/../../../../../../../../../../etc/httpd/logs/error.log`
			`/../../../../../../../../../../opt/lampp/logs/access_log`
			`/../../../../../../../../../../var/log/apache2/error.log`
			`/../../../../../../../../../../etc/passwd`
			`/../../../../../../../../../../var/log/apache2/access.log`
			`/../../../../../../../../../../var/log/apache/access.log`
			Request / Response

http://rest.testinvicti.com/jwt/api/users	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
			Operating system paths found in the HTTP response:
			`/../../../../../../../../../../etc/httpd/logs/error_log`
			`/../../../../../../../../../../var/log/apache/error.log`
			`/etc/passwd`
			`/../../../../../../../../../../etc/httpd/logs/access.log`
			`/../../../../../../../../../../var/log/lighttpd/access.log`
			`/../../../../../../../../../../var/log/nginx/access.log`
			`/../../../../../../../../../../etc/httpd/logs/error.log`
			`/../../../../../../../../../../opt/lampp/logs/access_log`
			`/../../../../../../../../../../var/log/apache2/error.log`
			`/etc/issue`
			`/../../../../../../../../../../etc/passwd`
			`/../../../../../../../../../../var/log/apache2/access.log`
			`/../../../../../../../../../../var/log/apache/access.log`
			Request / Response

http://rest.testinvicti.com/jwt/api/users	GET	**Query:**
		__proto__.acfDBda=acfDBda
		__proto__=&0[af149Ea]=af149Ea
		__proto__[a1C99AE]=a1C99AE
		x.__proto__.acAF483=acAF483
		x[__proto__][aBeedfa]=aBeedfa
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
			Operating system paths found in the HTTP response:
			`/../../../../../../../../../../etc/httpd/logs/error_log`
			`/../../../../../../../../../../var/log/apache/error.log`
			`/../../../../../../../../../../etc/httpd/logs/access.log`
			`/etc/passwd`
			`/../../../../../../../../../../var/log/lighttpd/access.log`
			`/../../../../../../../../../../var/log/nginx/access.log`
			`/../../../../../../../../../../etc/httpd/logs/error.log`
			`/../../../../../../../../../../opt/lampp/logs/access_log`
			`/../../../../../../../../../../var/log/apache2/error.log`
			`/etc/issue`
			`/../../../../../../../../../../etc/passwd`
			`/../../../../../../../../../../var/log/apache2/access.log`
			`/../../../../../../../../../../var/log/apache/access.log`
			Request / Response

http://rest.testinvicti.com/jwt/api/users/test_username'	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
			Operating system paths found in the HTTP response:
			`/var/www/vendor/slim/slim/Slim/MiddlewareAwareTrait.php(117`
			`/var/www/src/middlewares/oauth2.php(23`
			`/var/www/public/index.php(36`
			`/var/www/src/middlewares/jwt.php(25`
			`/var/www/vendor/slim/slim/Slim/Handlers/Strategies/RequestResponse.php(40`
			`/var/www/vendor/slim/slim/Slim/App.php(297`
			`/var/www/vendor/slim/slim/Slim/DeferredCallable.php(57`
			`/var/www/src/middlewares/check_auth_type.php(19`
			`/var/www/vendor/slim/slim/Slim/MiddlewareAwareTrait.php(70`
			`/var/www/src/routes/users.php`
			`/var/www/vendor/slim/slim/Slim/App.php(392`
			`/var/www/src/routes/users.php(67`
			`/var/www/vendor/slim/slim/Slim/Route.php(281`
			`/var/www/vendor/slim/slim/Slim/Route.php(268`
			`/var/www/vendor/tuupola/slim-basic-auth/src/HttpBasicAuthentication.php(87`
			`/var/www/vendor/slim/slim/Slim/App.php(503`
			Request / Response

http://rest.testinvicti.com/jwt/api/users/test_username	GET	**Headers:** User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36	Operating system paths found in the HTTP response: `/var/www/src/helpers.php` Request / Response

Details

Risk description:
The risk is that path disclosure may help an attacker learn more about the remote server's file system, thus increasing the effectiveness and precision of any future attacks.

Recommendation:
Configure the web server to avoid leaking path information by using generic error messages that do not reveal any internal file paths. Make sure no server file is referred with its absolute path in the website code.

References:
https://cwe.mitre.org/data/definitions/200.html

Classification:
CWE : CWE-200

Spider results

URL	Method	Parameters	Page Title	Page Size	Status Code
http://rest.testinvicti.com/jwt/api	GET		Page Not Found	885 B	404
http://rest.testinvicti.com/jwt/api/comments	GET			46.5 KB	200
http://rest.testinvicti.com/jwt/api/comments/21	GET			323 B	200
http://rest.testinvicti.com/jwt/api/comments/21	PUT	**Body:** comment=comment post_id=1123123 user_id=1123123		108 B	200
http://rest.testinvicti.com/jwt/api/comments/21	DELETE	**Query:** callback=callback **Body:** comment=comment post_id=1123123 user_id=1123123		58 B	200
http://rest.testinvicti.com/jwt/api/comments	POST	**Body:** comment=comment post_id=1123123 user_id=1123123		115 B	200
http://rest.testinvicti.com/jwt/api/posts	GET			64.29 KB	200
http://rest.testinvicti.com/jwt/api/posts/1/comments	DELETE	**Query:** callback=callback **Body:** content=content title=title user_id=1123123	Method not allowed	555 B	405
http://rest.testinvicti.com/jwt/api/posts/21	GET			323 B	200
http://rest.testinvicti.com/jwt/api/posts/5/comments	GET			19.02 KB	200
http://rest.testinvicti.com/jwt/api/posts/5/comments	PUT	**Body:** content=content title=title user_id=1123123		53 B	405
http://rest.testinvicti.com/jwt/api/posts	POST	**Body:** content=content title=title user_id=1123123		106 B	200
http://rest.testinvicti.com/jwt/api/users	GET			109.77 KB	200
http://rest.testinvicti.com/jwt/api/users/ena07/posts	GET			304 B	200
http://rest.testinvicti.com/jwt/api/users/test_username	GET			5 B	200
http://rest.testinvicti.com/jwt/api/users/test_username	PUT	**Body:** email=example_email@example.com first_name=first_name last_name=last_name password=Secure123456$ username=us3rn4me2bed373rm1n3d		151 B	200

http://rest.testinvicti.com/jwt/api/users/test_username	DELETE	**Query:** callback=callback **Body:** email=example_email@example.com first_name=first_name last_name=last_name password=Secure123456$ username=us3rn4me2bed373rm1n3d		64 B	200
http://rest.testinvicti.com/jwt/api/users	POST	**Body:** email=example_email@example.com first_name=first_name last_name=last_name password=Secure123456$ username=us3rn4me2bed373rm1n3d		200 B	200
http://rest.testinvicti.com/jwt/	GET		Page Not Found	885 B	404

Details

Risk description:
The table contains all the unique pages the scanner found. The duplicated URLs are not available here as scanning those is considered unnecessary

Recommendation:
We recommend to advanced users to make sure the scan properly detected most of the URLs in the application.

References:
All the URLs the scanner found, including duplicates (available for 90 days after the scan date)

Api is accessible.

Nothing was found for CORS misconfiguration.

Nothing was found for use of untrusted certificates.

Nothing was found for enabled HTTP debug methods.

Nothing was found for enabled HTTP OPTIONS method.

Nothing was found for GraphQL endpoints.

Nothing was found for directory listing.

Nothing was found for passwords submitted unencrypted.

Nothing was found for debug messages.

Nothing was found for code comments.

- Nothing was found for missing HTTP header - Strict-Transport-Security.
- Nothing was found for XML External Entity Injection.
- Nothing was found for passwords submitted in URLs.
- Nothing was found for JWT weaknesses.
- Nothing was found for domain too loose set for cookies.
- Nothing was found for mixed content between HTTP and HTTPS.
- Nothing was found for cross domain file inclusion.
- Nothing was found for HttpOnly flag of cookie.
- Nothing was found for Secure flag of cookie.
- Nothing was found for login interfaces.
- Nothing was found for secure password submission.
- Nothing was found for sensitive data.
- Nothing was found for Server Side Request Forgery.
- Nothing was found for Open Redirect.
- Nothing was found for PHP Code Injection.
- Nothing was found for JavaScript Code Injection.
- Nothing was found for Broken Authentication.
- Nothing was found for Ruby Code Injection.
- Nothing was found for Python Code Injection.

Nothing was found for Perl Code Injection.

Nothing was found for Remote Code Execution through Log4j.

Nothing was found for Server Side Template Injection.

Nothing was found for Remote Code Execution through VIEWSTATE.

Nothing was found for Request URL Override.

Nothing was found for HTTP/1.1 Request Smuggling.

Nothing was found for NoSQL Injection.

Nothing was found for Insecure Deserialization.

Nothing was found for unsafe HTTP header Content Security Policy.

Nothing was found for OpenAPI files.

Nothing was found for Session Token in URL.

Scan coverage information

List of tests performed (57/57)

- Starting the scan...
- Trying to authenticate...
- Checking for secure communication...
- Checking for missing HTTP header - X-Content-Type-Options...
- Checking for missing HTTP header - Content Security Policy...
- Checking for missing HTTP header - Referrer...
- Checking for Path Disclosure...
- Spidering target...
- Checking for JWT Weak Secret Key...
- Checking for internal error code...
- Checking for website technologies...
- Checking for vulnerabilities of server-side software...
- Checking for absence of the security.txt file...
- Checking for CORS misconfiguration...
- Checking for use of untrusted certificates...
- Checking for enabled HTTP debug methods...
- Checking for enabled HTTP OPTIONS method...
- Checking for GraphQL endpoints...
- Checking for error messages...
- Checking for SQL Injection...
- Checking for OS Command Injection...
- Checking for Insecure Direct Object Reference...
- Checking for Local File Inclusion...
- Checking for directory listing...
- Checking for passwords submitted unencrypted...
- Checking for debug messages...

- Checking for code comments...
- Checking for missing HTTP header - Strict-Transport-Security...
- Checking for XML External Entity Injection...
- Checking for passwords submitted in URLs...
- Checking for JWT weaknesses...
- Checking for domain too loose set for cookies...
- Checking for mixed content between HTTP and HTTPS...
- Checking for cross domain file inclusion...
- Checking for HttpOnly flag of cookie...
- Checking for Secure flag of cookie...
- Checking for login interfaces...
- Checking for secure password submission...
- Checking for sensitive data...
- Checking for Server Side Request Forgery...
- Checking for Open Redirect...
- Checking for PHP Code Injection...
- Checking for JavaScript Code Injection...
- Checking for Broken Authentication...
- Checking for Ruby Code Injection...
- Checking for Python Code Injection...
- Checking for Perl Code Injection...
- Checking for Remote Code Execution through Log4j...
- Checking for Server Side Template Injection...
- Checking for Remote Code Execution through VIEWSTATE...
- Checking for Request URL Override...
- Checking for HTTP/1.1 Request Smuggling...
- Checking for NoSQL Injection...
- Checking for Insecure Deserialization...
- Checking for unsafe HTTP header Content Security Policy...
- Checking for OpenAPI files...
- Checking for Session Token in URL...

Scan parameters

Target:	http://rest.testinvicti.com/jwt/
API Type:	REST
Spec URL:	http://rest.testsparker.com/files/openapi-swagger_jwt.yaml
Authentication:	True
Scan Type:	Deep

Scan stats

Unique Injection Points Detected:	19
URLs spidered:	1
Total number of HTTP requests:	9612
Average time until a response was received:	170ms
Total number of HTTP request errors:	6