Pentest Tools

SharePoint Security Scanner Report

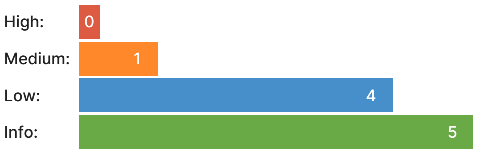
✓ **http://95.179.253.46**

Summary

Overall risk level:

Medium

Risk ratings:



Scan information:

Start time:	2023-04-25 15:42:17 UTC+03
Finish time:	2023-04-25 15:42:24 UTC+03
Scan duration:	7 sec
Tests performed:	10/10
Scan status:	Finished

Findings

Found SharePoint web services

http://95.179.253.46/_layouts/15//_vti_bin/spdisco.aspx

Details

Risk description:
An attacker could use this information to mount specific attacks against the SharePoint installation.

Recommendation:
We recommend you to disable anonymous access to SharePoint web services.

More information about this issue:
http://www.sharepointdiary.com/2012/06/sharepoint-web-services-exposed-to-anonymous-users.html
https://technet.microsoft.com/en-us/library/ee191479(v=office.12).aspx

Server software and technology found

Technology	ASP.NET 4.0.30319
Server	Microsoft-IIS 8.5
Operating system	Windows

Details

Risk description:
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 may allow an attacker to identify the software platform, technology, server and operating system (ex. HTTP server headers, meta information, etc).

More information about this issue:
https://www.owasp.org/index.php/Fingerprint_Web_Server_(OTG-INFO-002)

SharePoint installation found from fingerprint

Microsoft SharePoint 2013 - version(s) 15.0.0.4420

Details

Risk description:
An attacker could use this information to mount specific attacks against the identified SharePoint installation.

Recommendation:
We recommend you to remove the MicrosoftSharePointTeamServices header from the HTTP response.

More information about this issue:
https://blogs.msdn.microsoft.com/gajendra/2015/08/24/removing-http-response-headers-for-publicinternet-facing-sharepoint-sites/

SharePoint configuration information

Configuration Type	HTTP Header	Value
Request duration	SPRequestDuration	15 milliseconds
Server health score	X-SharePointHealthScore	Not found
Web front-end server latency	SPIislatency	1 milliseconds
Log Correlation Id	SPRequestGuid	c7a9aca0-11d2-80c1-ea16-5efd396756b8

Details

Risk description:
An attacker could use this vulnerability to obtain information about the server load status. This could be used to monitor the effectiveness of a Denial of Service attack against this server.

Recommendation:
We recommend you to eliminate the HTTP headers mentioned above, in order to mitigate this vulnerability.

More information about this issue:
https://support.office.com/en-gb/article/Diagnosing-performance-issues-with-SharePoint-Online-3c364f9e-b9f6-4da4-a792-c8e8c8cd2e86
https://msdn.microsoft.com/en-us/library/jj162162(v=office.12).aspx
http://technicalinternetwideworld.blogspot.com/search/label/SPIisLatency
http://blog.michelbarneveld.nl/michel/archive/2009/11/08/x-sharepointhealthscore-a-new-sharepoint-2010-http-header.aspx

Search engine exposure

site:95.179.253.46 inurl:"/_catalogs"

site:95.179.253.46 inurl:"/Forms"

site:95.179.253.46 inurl:"/_layouts"

Details

Risk description:
You should manually access the above URLs in order to see if there are any sensitive SharePoint pages indexed by Google.

Recommendation:
We recommend you to restrict public access to sensitive pages, if such access is not needed for business purposes.

More information about this issue:
https://www.slideshare.net/AntonioMaio2/best-practices-for-security-in-microsoft-sharepoint-2013

FrontPage Server Extensions not found

User enumeration failed

Permissions on default _catalogs are secure

Permissions on default forms are secure

Permissions on default _layouts are secure

Scan coverage information

List of tests performed (10/10)

- ✓ Fingerprinting the server software and technology...
- ✓ Fingerprinting the SharePoint installation...
- ✓ Analyzing SharePoint configuration...
- ✓ Checking FrontPage Server Extensions...
- ✓ Checking SharePoint web services...
- ✓ Attempting SharePoint user enumeration (max 20 users)...
- ✓ Checking permissions on default _catalogs...
- ✓ Checking permissions on default forms...
- ✓ Checking permissions on default _layouts...
- ✓ Checking search engine exposure...

Scan parameters

Target:	http://95.179.253.46