Pentest-Tools.com

SharePoint Security Scanner Report

http://sharepointtarget.com

Summary

Overall risk level:

High

Risk ratings:

Scan information:

Start time:	2017-06-29 17:02:54
Finish time:	2017-06-29 17:04:42
Scan duration:	108.0 seconds
Tests performed:	10/10
Scan status:	Finished

Findings

Found SharePoint user information

http://sharepointtarget.com//_layouts/userdisp.aspx?Force=True&id=1	
Account	i:0#.w|sharepointtarget\administrator
Name	Administrator
Work e-mail	Administrator@sharepointtarget.com
http://sharepointtarget.com//_layouts/userdisp.aspx?Force=True&id=14	
Account	i:0#.f|ldapmember|anonym
Name	anonym
http://sharepointtarget.com//_layouts/userdisp.aspx?Force=True&id=15	
Account	i:0#.f|ldapmember|max.jonesie
Name	maxjonesie
Work e-mail	max.jonesie@gmail.com
Title	Doctor of Engineering
http://sharepointtarget.com//_layouts/userdisp.aspx?Force=True&id=16	
Account	i:0#.f|ldapmember|roswella.damm
Name	RoswellaDamm-sharepointtarget
Work e-mail	roswella.damm@sharepointtarget.com
Title	Doctor of Management

Details

Risk description:
An attacker could utilize user information to mount phishing attacks against SharePoint users. Because the amount of user information is significant, the phishing attack can be more effective, containing details such as victim's full name, title and work e-mail.
Furthermore, the gathered usernames can be used in brute force attacks, in order to find the associated passwords. This way, the attacker would gain unauthorized access to the SharePoint application.

Recommendation:
We recommend you to disable anonymous access to the userdisp.aspx page.

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

Found SharePoint web services

http://sharepointtarget.com//_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

Found 2 of 3 searched _catalogs

http://sharepointtarget.com//_catalogs/masterpage/Forms/AllItems.aspx

http://sharepointtarget.com//_catalogs/wp/Forms/AllItems.aspx

Details

Risk description:
The default _catalogs pages could contain confidential information which can be useful for attackers.

Recommendation:
We recommend you to restrict anonymous access to default _catalogs 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

Found 12 of 128 searched _layouts

http://sharepointtarget.com//_layouts/viewlsts.aspx

http://sharepointtarget.com//_layouts/userdisp.aspx

http://sharepointtarget.com//_layouts/userdisp.aspx?ID=1

http://sharepointtarget.com//_layouts/aclinv.aspx

http://sharepointtarget.com//_layouts/bpcf.aspx

http://sharepointtarget.com//_layouts/groups.aspx

http://sharepointtarget.com//_layouts/help.aspx

http://sharepointtarget.com//_layouts/mcontent.aspx

http://sharepointtarget.com//_layouts/mobile/mbllists.aspx

http://sharepointtarget.com//_layouts/people.aspx?MembershipGroupId=0

http://sharepointtarget.com//_layouts/recyclebin.aspx

http://sharepointtarget.com//_layouts/spcf.aspx

Details

Risk description:
The default _layouts pages could contain confidential information which can be useful for attackers.

Recommendation:
We recommend you to restrict anonymous access to default _layouts 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

Server software and technology found

Technology	ASP.NET 2.0.50727
Server	Microsoft-IIS 7.5
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 2010 - version(s) 14.0.0.6108

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	Not found
Server health score	X-SharePointHealthScore	0 (small load)
Web front-end server latency	SPIisLatency	Not found
Log Correlation Id	SPRequestGuid	6690f134-2acd-48af-91c2-fd30ba142149

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

FrontPage Server Extensions found

FrontPage Server Extensions version 14.00.0.000
View source: http://sharepointtarget.com//_vti_inf.html

Details

Risk description:
An attacker could use this information to mount specific attacks against FrontPage Server Extensions.

Recommendation:
We recommend you to remove FrontPage Server Extensions if it is not needed for business purposes.

More information about this issue:
https://support.microsoft.com/en-us/help/951039/error-message-when-you-try-to-upgrade-windows-server-2003-to-windows-s

Search engine exposure

site:sharepointtarget.com inurl:"/_catalogs"
site:sharepointtarget.com inurl:"/Forms"
site:sharepointtarget.com 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

Permissions on default forms 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://sharepointtarget.com