Scan Report

May 13, 2021

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "PTSP". The scan started at Thu May 13 05:50:18 2021 UTC and ended at Thu May 13 06:32:33 2021 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
43.249.142.70 ptsp.sumedangkab.go.id	2	2	1	0	0
Total: 1	2	2	1	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 5 results selected by the filtering described above. Before filtering there were 229 results.

2 Results per Host

2.1 43.249.142.70

Host scan start	Thu May 13 05:50:24 2021 UTC
Host scan end	Thu May 13 06:31:00 2021 UTC

Service (Port)	Threat Level
443/tcp	High
80/tcp	High
443/tcp	Medium
80/tcp	Medium
general/tcp	Low

2.1.1 High 443/tcp

High (CVSS: 7.5)
NVT: phpinfo() output Reporting

Summary
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.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
https://ptsp.sumedangkab.go.id/info.php

Impact
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.

Solution
Solution type: Workaround
Delete the listed files or restrict access to them.

Vulnerability Detection Method
Details: phpinfo() output Reporting
OID:1.3.6.1.4.1.25623.1.0.11229

[return to 43.249.142.70]

2.1.2 High 80/tcp

High (CVSS: 7.5)
NVT: phpinfo() output Reporting

Summary
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.

Vulnerability Detection Result
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://ptsp.sumedangkab.go.id/info.php

Impact
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.

Solution
Solution type: Workaround
Delete the listed files or restrict access to them.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details: `phpinfo() output Reporting`
OID:1.3.6.1.4.1.25623.1.0.11229

[return to 43.249.142.70]

2.1.3 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: MacOS X Finder '.DS_Store' Information Disclosure

Summary
MacOS X creates a hidden file '.DS_Store', in each directory that has been viewed with the 'Finder'. This file contains a list of the contents of the directory, giving an attacker information on the structure and contents of your website.

Vulnerability Detection Result
```
The following files were identified:
https://ptsp.sumedangkab.go.id/app/asset/pixel/plugins/bower_components/ion-rang
↪eslider/.DS_Store
```

Solution
Solution type: Workaround
Block access to hidden files (starting with a dot) within your webservers configuration

Vulnerability Detection Method
Details: `MacOS X Finder '.DS_Store' Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.10756

References
```
cve: CVE-2016-1776
cve: CVE-2018-6470
bid: 3316
bid: 3324
bid: 85054
url: https://www.securityfocus.com/bid/3316
url: https://www.securityfocus.com/bid/3324
url: https://www.securityfocus.com/bid/85054
url: https://helpx.adobe.com/dreamweaver/kb/remove-ds-store-files-mac.html
url: https://support.apple.com/en-us/HT1629
cert-bund: CB-K16/0450
dfn-cert: DFN-CERT-2016-0489
```

[return to 43.249.142.70]

2.1.4 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result
The following input fields where identified (URL:input name):
http://ptsp.sumedangkab.go.id/db/:pma_password
http://ptsp.sumedangkab.go.id/ptsp/:login_password
http://ptsp.sumedangkab.go.id/ptsp/agenda/read_agenda/123:login_password
http://ptsp.sumedangkab.go.id/ptsp/agenda/read_agenda/lauching-sistem-informasi-ptsp:login_password
http://ptsp.sumedangkab.go.id/ptsp/agenda:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/category/berita-izin-lingkungan:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/category/umum:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/index/:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/read/berita-izin-lingklungan-22-oktober-2018:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/read/berita-izin-lingkungan-10-oktober-2018:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/read/berita-izin-lingkungan-2-nopember-2018:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/read/berita-izin-lingkungan-26-nopember-2018:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/read/berita-izin-lingkungan-3-desember-2018:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/read/bersyarat-pemprov-jabar-keluarkan-18-iup-dan-wiup:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/read/informasi-izin-lingkungan-12-nopember-2018:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/read/kpk-dorong-17-provinsi-manfaakan-aplikasi-e-government-pemprov-jabar-sebagai-daerah-percontohan:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/read/pemberutahuan-yang-telah-mengajukan-dan-mendapatkan-izin-lingkungan-dari-kepala-dpmptsp-kabupaten-su:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/read/tiga-inovasi-jabar-akan-diadopsi-oleh-16-provinsi:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/tag/android:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita/tag/php:login_password
http://ptsp.sumedangkab.go.id/ptsp/berita:login_password
http://ptsp.sumedangkab.go.id/ptsp/download:login_password
http://ptsp.sumedangkab.go.id/ptsp/eloker:login_password
http://ptsp.sumedangkab.go.id/ptsp/epromotion:login_password

... continues on next page ...

... continued from previous page ...

http://ptsp.sumedangkab.go.id/ptsp/grafikizin:login_password
http://ptsp.sumedangkab.go.id/ptsp/home:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/101:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/102:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/103:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/105:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/109:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/11:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/120:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/121:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/122:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/124:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/125:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/127:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/128:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/129:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/12:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/131:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/135:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/141:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/143:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/145:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/146:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/147:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/149:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/14:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/150:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/151:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/154:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/156:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/158:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/15:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/162:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/167:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/169:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/172:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/173:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/19:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/26:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/28:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/29:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/33:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/36:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/40:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/43:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/46:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/47:login_password

... continues on next page ...

... continued from previous page ...

http://ptsp.sumedangkab.go.id/ptsp/izin/detail/49:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/63:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/66:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/68:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/84:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/85:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/86:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/87:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin/detail/91:login_password
http://ptsp.sumedangkab.go.id/ptsp/izin:login_password
http://ptsp.sumedangkab.go.id/ptsp/maklumat:login_password
http://ptsp.sumedangkab.go.id/ptsp/mobil_pelayanan:login_password
http://ptsp.sumedangkab.go.id/ptsp/onestopservices:login_password
http://ptsp.sumedangkab.go.id/ptsp/oss:login_password
http://ptsp.sumedangkab.go.id/ptsp/panduan:login_password
http://ptsp.sumedangkab.go.id/ptsp/pengaduan:login_password
http://ptsp.sumedangkab.go.id/ptsp/persyaratan:login_password
http://ptsp.sumedangkab.go.id/ptsp/profil:login_password
http://ptsp.sumedangkab.go.id/ptsp/siice:login_password

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440

References
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management

... continues on next page ...

... continued from previous page ...

```
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html
```

[return to 43.249.142.70]

2.1.5 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1660075926
Packet 2: 1660077025
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091

References

... continues on next page ...

... continued from previous page ...

```
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 43.249.142.70]
