Scan Report

November 28, 2024

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 "WEB_www.paritkebumen.desa.id". The scan started at Thu Nov 28 16:05:50 2024 UTC and ended at Thu Nov 28 21:32:52 2024 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
202.74.239.249 www.cloud.paritkebumen.desa.id	0	0	1	170	0
Total: 1	0	0	1	170	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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 "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 results 1 to 171 of the 172 results selected by the filtering described above.
Before filtering there were 172 results.

2 Results per Host

2.1 202.74.239.249

Host scan start	Thu Nov 28 16:06:40 2024 UTC
Host scan end	Thu Nov 28 21:32:51 2024 UTC

Service (Port)	Threat Level
general/tcp	Low
2082/tcp	Log
52230/tcp	Log
general/CPE-T	Log
2083/tcp	Log
general/tcp	Log
52229/tcp	Log

2.1.1 Low general/tcp

Low (CVSS: 2.6) NVT: TCP Timestamps Information Disclosure
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.
. . . continues on next page . . .

... continued from previous page ...

Quality of Detection: 80

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: 880529908
Packet 2: 880531168

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 Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: 2023-12-15T16:10:08Z

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

[return to 202.74.239.249]

2.1.2 Log 2082/tcp

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
```
The Hostname/IP "www.epas.paritkebumen.desa.id" was used to access the remote ho
↪st.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://www.epas.paritkebumen.desa.id:2082/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

. . . continues on next page . . .

... continued from previous page ...

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
The Hostname/IP "www.lapor.paritkebumen.desa.id" was used to access the remote h
↪ost.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://www.lapor.paritkebumen.desa.id:2082/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
```
The Hostname/IP "www.pso.paritkebumen.desa.id" was used to access the remote hos
↪t.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://www.pso.paritkebumen.desa.id:2082/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
```
The Hostname/IP "server101share.extremhost.net" was used to access the remote ho
↪st.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
```

... continues on next page ...

... continued from previous page ...

```
http://server101share.extremhost.net:2082/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "www.paritkebumen.desa.id" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
```

... continues on next page ...

... continued from previous page ...

```
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://www.paritkebumen.desa.id:2082/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "www.cloud.paritkebumen.desa.id" was used to access the remote h
↪ost.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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.
```

... continues on next page ...

... continued from previous page ...

```
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://www.cloud.paritkebumen.desa.id:2082/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪------------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
```

... continues on next page ...

... continued from previous page ...

```
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary

... continues on next page ...

... continued from previous page ...

All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪-----------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
```

... continues on next page ...

... continued from previous page ...

```
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪---------------------------------------------------------------------------------
↪-----------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
```

... continues on next page ...

... continued from previous page ...

```
↪/#referrer-policy
Sec-Fetch-Dest                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options          | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                 | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪-------------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪-------------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
```

... continues on next page ...

... continued from previous page ...

```
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪-----------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
```

... continues on next page ...

... continued from previous page ...

```
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: `HTTP Security Headers Detection`
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `2021-07-14T06:19:43Z`

References
`url: https://owasp.org/www-project-secure-headers/`
`url: https://owasp.org/www-project-secure-headers/#div-headers`

... continues on next page ...

... continued from previous page ...

url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: imunify360-webshield/1.21

Solution:

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: imunify360-webshield/1.21

Solution:

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary

. . . continues on next page . . .

... continued from previous page ...

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
`A web server is running on this port`

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result
`A web server is running on this port`

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

[return to 202.74.239.249]

2.1.3 Log 52230/tcp

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
```
The Hostname/IP "www.epas.paritkebumen.desa.id" was used to access the remote ho
↪st.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://www.epas.paritkebumen.desa.id:52230/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

. . . continues on next page . . .

... continued from previous page ...

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
The Hostname/IP "www.lapor.paritkebumen.desa.id" was used to access the remote h
↪ost.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://www.lapor.paritkebumen.desa.id:52230/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
```
The Hostname/IP "www.pso.paritkebumen.desa.id" was used to access the remote hos
↪t.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://www.pso.paritkebumen.desa.id:52230/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
```
The Hostname/IP "server101share.extremhost.net" was used to access the remote ho
↪st.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
```

... continues on next page ...

... continued from previous page ...

```
http://server101share.extremhost.net:52230/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "www.paritkebumen.desa.id" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
```

... continues on next page ...

... continued from previous page ...

```
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://www.paritkebumen.desa.id:52230/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "www.cloud.paritkebumen.desa.id" was used to access the remote h
↪ost.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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.
```

... continues on next page ...

... continued from previous page ...

```
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
http://www.cloud.paritkebumen.desa.id:52230/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪------------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
```

... continues on next page ...

... continued from previous page ...

```
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary

... continues on next page ...

... continued from previous page ...

All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪-----------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
```

... continues on next page ...

... continued from previous page ...

```
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪-----------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
```

... continues on next page ...

... continued from previous page ...

```
↪/#referrer-policy
Sec-Fetch-Dest                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options          | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                 | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪-------------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

Missing Headers	More Information
Content-Security-Policy	https://owasp.org/www-project-secure-headers/#content-security-policy
Cross-Origin-Embedder-Policy	https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Cross-Origin-Opener-Policy	https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Cross-Origin-Resource-Policy	https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Document-Policy	https://w3c.github.io/webappsec-feature-policy/document-policy#document-policy-http-header
Feature-Policy	https://owasp.org/www-project-secure-headers/#feature-policy, Note: The Feature Policy header has been renamed to Permissions Policy
Permissions-Policy	https://w3c.github.io/webappsec-feature-policy/#permissions-policy-http-header-field
Referrer-Policy	https://owasp.org/www-project-secure-headers/#referrer-policy
Sec-Fetch-Dest	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90

... continues on next page ...

... continued from previous page ...

```
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪-----------------------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
```

... continues on next page ...

... continued from previous page ...

```
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers

... continues on next page ...

... continued from previous page ...

url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: imunify360-webshield/1.21

Solution:

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: imunify360-webshield/1.21

Solution:

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary

. . . continues on next page . . .

... continued from previous page ...

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
`A web server is running on this port`

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result
`A web server is running on this port`

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

[return to 202.74.239.249]

2.1.4 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.
Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.

Quality of Detection: 80

Vulnerability Detection Result
`202.74.239.249|cpe:/a:ietf:transport_layer_security:1.2`
`202.74.239.249|cpe:/a:ietf:transport_layer_security:1.3`

Solution:

Log Method
Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `2022-07-27T10:11:28Z`

References
`url: https://nvd.nist.gov/products/cpe`

[return to 202.74.239.249]

2.1.5 Log 2083/tcp

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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

... continues on next page ...

... continued from previous page ...

If you think any of this information is wrong please report it to the referenced community forum.

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "server101share.extremhost.net" was used to access the remote ho
↪st.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://server101share.extremhost.net:2083/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method

Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References

`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary

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)

... continues on next page ...

... continued from previous page ...

- 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.

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "www.paritkebumen.desa.id" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://www.paritkebumen.desa.id:2083/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method

Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References

`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary

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)

... continues on next page ...

... continued from previous page ...

- 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.

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "www.cloud.paritkebumen.desa.id" was used to access the remote h
↪ost.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://www.cloud.paritkebumen.desa.id:2083/
https://www.cloud.paritkebumen.desa.id:2083/mynews/includes/tiny_mce
https://www.cloud.paritkebumen.desa.id:2083/mynews/includes/tiny_mce/plugins
https://www.cloud.paritkebumen.desa.id:2083/mynews/includes/tiny_mce/plugins/fil
↪emanager
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method

Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

References

url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
```
The Hostname/IP "www.epas.paritkebumen.desa.id" was used to access the remote ho
↪st.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://www.epas.paritkebumen.desa.id:2083/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

. . . continues on next page . . .

... continued from previous page ...

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
The Hostname/IP "www.lapor.paritkebumen.desa.id" was used to access the remote h
↪ost.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://www.lapor.paritkebumen.desa.id:2083/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
```
The Hostname/IP "www.pso.paritkebumen.desa.id" was used to access the remote hos
↪t.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://www.pso.paritkebumen.desa.id:2083/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪----------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
```

... continues on next page ...

... continued from previous page ...

```
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.

... continues on next page ...

... continued from previous page ...

On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪----------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security         | Please check the output of the VTs including
```

... continues on next page ...

... continued from previous page ...

```
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪----------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
```

... continues on next page ...

... continued from previous page ...

```
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: `HTTP Security Headers Detection`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

Missing Headers	More Information
Content-Security-Policy	https://owasp.org/www-project-secure-headers/#content-security-policy
Cross-Origin-Embedder-Policy	https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Cross-Origin-Opener-Policy	https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Cross-Origin-Resource-Policy	https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Document-Policy	https://w3c.github.io/webappsec-feature-policy/document-policy#document-policy-http-header
Expect-CT	https://owasp.org/www-project-secure-headers/#expect-ct, Note: This is an upcoming header
Feature-Policy	https://owasp.org/www-project-secure-headers/#feature-policy, Note: The Feature Policy header has been renamed to Permissions Policy
Permissions-Policy	https://w3c.github.io/webappsec-feature-policy/#permissions-policy-http-header-field
Public-Key-Pins	Please check the output of the VTs including 'SSL/TLS:' and 'HPKP' in their name for more information and configuration help. Note: Most major browsers have dropped / deprecated support for this header in 2020.
Referrer-Policy	https://owasp.org/www-project-secure-headers/#referrer-policy

... continues on next page ...

... continued from previous page ...

```
Sec-Fetch-Dest                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security       | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options          | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                 | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: `HTTP Security Headers Detection`
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `2021-07-14T06:19:43Z`

References
`url: https://owasp.org/www-project-secure-headers/`
`url: https://owasp.org/www-project-secure-headers/#div-headers`
`url: https://securityheaders.com/`

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪----------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
```

... continues on next page ...

... continued from previous page ...

```
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪----------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
```

... continues on next page ...

... continued from previous page ...

```
↪cy/document-policy#document-policy-http-header
Expect-CT                           | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming header
Feature-Policy                      | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                  | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Public-Key-Pins                     | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                     | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                      | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                      | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                      | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                      | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security           | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options              | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                     | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                    | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

... continues on next page ...

... continued from previous page ...

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration

Summary
This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

Quality of Detection: 80

Vulnerability Detection Result
```
It was possible to enumerate the following HTTP server banner(s):
Server banner                     | Enumeration technique
--------------------------------------------------------------------------------
↪--------------------
Server: imunify360-webshield/1.21 | Invalid HTTP 00.5 GET request (non-existent
↪HTTP version) to '/'
```

Solution:

Log Method
Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2022-06-28T10:11:01Z

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration

Summary
This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

Quality of Detection: 80

Vulnerability Detection Result
```
It was possible to enumerate the following HTTP server banner(s):
Server banner                     | Enumeration technique
--------------------------------------------------------------------------------
↪--------------------
Server: imunify360-webshield/1.21 | Invalid HTTP 00.5 GET request (non-existent
```

... continues on next page ...

... continued from previous page ...

```
↪HTTP version) to '/'
```

Solution:

Log Method
Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2022-06-28T10:11:01Z

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration

Summary
This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

Quality of Detection: 80

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner                     | Enumeration technique
--------------------------------------------------------------------------------
↪--------------------
Server: imunify360-webshield/1.21 | Invalid HTTP 00.5 GET request (non-existent
↪HTTP version) to '/'
```

Solution:

Log Method
Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2022-06-28T10:11:01Z

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
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.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result
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
TLSv1.2:HTTP/2

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
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
TLSv1.2:HTTP/2

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099

... continues on next page ...

... continued from previous page ...

Version used: 2024-09-27T05:05:23Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
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
TLSv1.2:HTTP/2

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
This routine identifies services supporting the following extensions to TLS:
- Application-Layer Protocol Negotiation (ALPN)
- Next Protocol Negotiation (NPN).

... continues on next page ...

... continued from previous page ...

Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.

Quality of Detection: 80

Vulnerability Detection Result

```
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
TLSv1.2:HTTP/2
```

Solution:

Log Method

Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References

```
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04
```

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary

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.

Quality of Detection: 80

Vulnerability Detection Result

```
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
TLSv1.2:HTTP/2
```

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
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
TLSv1.2:HTTP/2

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

Product detection result
cpe:/a:ietf:transport_layer_security

... continues on next page ...

... continued from previous page ...

Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

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

Quality of Detection: 98

Vulnerability Detection Result
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

Solution:

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2024-09-30T08:38:05Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Quality of Detection: 98

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_ARIA_128_GCM_SHA256
TLS_RSA_WITH_ARIA_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256

Solution:

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: Report Medium Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: 2024-09-27T05:05:23Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

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

Quality of Detection: 98

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_ARIA_128_GCM_SHA256
TLS_RSA_WITH_ARIA_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_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

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2024-09-27T05:05:23Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

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

Quality of Detection: 98

Vulnerability Detection Result
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_ARIA_128_GCM_SHA256
TLS_RSA_WITH_ARIA_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
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.
```

Solution:

Vulnerability Insight
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.

Log Method
Details: `SSL/TLS: Report Supported Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: `2024-09-27T05:05:23Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

Summary

... continues on next page ...

... continued from previous page ...

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.

Quality of Detection: 80

Vulnerability Detection Result

```
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 403 Forbidden
Date: ***replaced***
Content-Type: text/html
Content-Length: ***replaced***
Connection: close
Server: imunify360-webshield/1.21
```

Solution:
Solution type: Workaround
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.

Log Method
Details: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
OID:1.3.6.1.4.1.25623.1.0.108247
Version used: 2024-02-08T05:05:59Z

References

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

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

Summary

... continues on next page ...

... continued from previous page ...

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

Quality of Detection: 80

Vulnerability Detection Result

```
The remote web server is not enforcing HSTS.
HTTP-Banner:
HTTP/1.1 403 Forbidden
Date: ***replaced***
Content-Type: text/html
Content-Length: ***replaced***
Connection: close
Server: imunify360-webshield/1.21
```

Solution:
Solution type: Workaround
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.

Log Method
Details: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
OID:1.3.6.1.4.1.25623.1.0.105879
Version used: 2024-02-08T05:05:59Z

References

```
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-cheat-sheets/cheatsheets/HTTP_Strict_Transpor
↪t_Security_Cheat_Sheet.html
url: https://owasp.org/www-project-secure-headers/#http-strict-transport-securit
↪y-hsts
url: https://tools.ietf.org/html/rfc6797
url: https://securityheaders.io/
url: https://httpd.apache.org/docs/current/mod/mod_headers.html#header
url: https://nginx.org/en/docs/http/ngx_http_headers_module.html#add_header
```

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

... continues on next page ...

... continued from previous page ...

cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.pso.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

... continues on next page ...

... continued from previous page ...

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.pso.paritkebumen.desa.id".
Certificate details:
fingerprint (SHA-1)             | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)           | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A
issued by                       | CN=R10,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 030996EF9572D98AE1689504F343AC7352B9
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=server101share.extremhost.net
subject alternative names (SAN) | server101share.extremhost.net
valid from                      | 2024-11-13 01:31:40 UTC
valid until                     | 2025-02-11 01:31:39 UTC
```

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

... continues on next page ...

... continued from previous page ...

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.pso.paritkebumen.desa.id".
Certificate details:
fingerprint (SHA-1)             | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)           | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A
issued by                       | CN=R10,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 030996EF9572D98AE1689504F343AC7352B9
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=server101share.extremhost.net
subject alternative names (SAN) | server101share.extremhost.net
valid from                      | 2024-11-13 01:31:40 UTC
valid until                     | 2025-02-11 01:31:39 UTC
```

Solution:

Log Method

Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.lapor.paritkebumen.desa.id".
Certificate details:
fingerprint (SHA-1)             | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)           | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A
issued by                       | CN=R10,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 030996EF9572D98AE1689504F343AC7352B9
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=server101share.extremhost.net
subject alternative names (SAN) | server101share.extremhost.net
valid from                      | 2024-11-13 01:31:40 UTC
valid until                     | 2025-02-11 01:31:39 UTC
```

Solution:

Log Method

Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.lapor.paritkebumen.desa.id".
```

... continues on next page ...

... continued from previous page ...

Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not match the hostname "www.pso.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8E19057D81273EEB29A

... continues on next page ...

... continued from previous page ...

issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.epas.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A	
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption

... continues on next page ...

... continued from previous page ...

subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.lapor.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC

... continues on next page ...

... continued from previous page ...

valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.lapor.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.epas.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.epas.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.epas.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.cloud.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.cloud.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

. . . continues on next page . . .

... continued from previous page ...

cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.cloud.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

... continues on next page ...

... continued from previous page ...

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.cloud.paritkebumen.desa.id".
Certificate details:
fingerprint (SHA-1)             | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)           | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A
issued by                       | CN=R10,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 030996EF9572D98AE1689504F343AC7352B9
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=server101share.extremhost.net
subject alternative names (SAN) | server101share.extremhost.net
valid from                      | 2024-11-13 01:31:40 UTC
valid until                     | 2025-02-11 01:31:39 UTC
```

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

... continues on next page ...

... continued from previous page ...

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.paritkebumen.desa.id".
Certificate details:
fingerprint (SHA-1)             | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)           | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A
issued by                       | CN=R10,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 030996EF9572D98AE1689504F343AC7352B9
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=server101share.extremhost.net
subject alternative names (SAN) | server101share.extremhost.net
valid from                      | 2024-11-13 01:31:40 UTC
valid until                     | 2025-02-11 01:31:39 UTC
```

Solution:

Log Method

Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.paritkebumen.desa.id".
Certificate details:
fingerprint (SHA-1)             | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)           | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A
issued by                       | CN=R10,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 030996EF9572D98AE1689504F343AC7352B9
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=server101share.extremhost.net
subject alternative names (SAN) | server101share.extremhost.net
valid from                      | 2024-11-13 01:31:40 UTC
valid until                     | 2025-02-11 01:31:39 UTC
```

Solution:

Log Method

Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.paritkebumen.desa.id".
```

... continues on next page ...

... continued from previous page ...

Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not match the hostname "www.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8E19057D81273EEB29A

... continues on next page ...

... continued from previous page ...

issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: imunify360-webshield/1.21

Solution:

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2023-08-01T13:29:10Z

... continues on next page ...

. . . continued from previous page . . .

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary

. . . continues on next page . . .

... continued from previous page ...

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result

```
The remote HTTP Server banner is:
Server: imunify360-webshield/1.21
```

Solution:

Log Method

Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary

This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Quality of Detection: 98

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)              | C378EC72F0C28748350B96DE419748546CE65318
fingerprint (SHA-256)            | C07652AD9A2734A17115EAB083D8843B7DCF4D1339ED23
↪EFC359B12E890CDEB8
issued by                        | CN=R11,O=Let's Encrypt,C=US
public key size (bits)           | 2048
serial                           | 049EF750C9E350875AFB060C8CE15DD76B50
signature algorithm              | sha256WithRSAEncryption
subject                          | CN=www.lapor.paritkebumen.desa.id
subject alternative names (SAN)  | *.paritkebumen.desa.id, paritkebumen.desa.id,
↪www.cloud.paritkebumen.desa.id, www.epas.paritkebumen.desa.id, www.lapor.parit
↪kebumen.desa.id, www.pso.paritkebumen.desa.id
valid from                       | 2024-11-04 21:09:23 UTC
valid until                      | 2025-02-02 21:09:22 UTC
```

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Quality of Detection: 98

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | C378EC72F0C28748350B96DE419748546CE65318
fingerprint (SHA-256)           | C07652AD9A2734A17115EAB083D8843B7DCF4D1339ED23
↪EFC359B12E890CDEB8
issued by                       | CN=R11,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 049EF750C9E350875AFB060C8CE15DD76B50
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=www.lapor.paritkebumen.desa.id
subject alternative names (SAN) | *.paritkebumen.desa.id, paritkebumen.desa.id,
↪www.cloud.paritkebumen.desa.id, www.epas.paritkebumen.desa.id, www.lapor.parit
↪kebumen.desa.id, www.pso.paritkebumen.desa.id
valid from                      | 2024-11-04 21:09:23 UTC
valid until                     | 2025-02-02 21:09:22 UTC
```

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 98

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | C378EC72F0C28748350B96DE419748546CE65318
fingerprint (SHA-256)           | C07652AD9A2734A17115EAB083D8843B7DCF4D1339ED23
↪EFC359B12E890CDEB8
issued by                       | CN=R11,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 049EF750C9E350875AFB060C8CE15DD76B50
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=www.lapor.paritkebumen.desa.id
subject alternative names (SAN) | *.paritkebumen.desa.id, paritkebumen.desa.id,
↪www.cloud.paritkebumen.desa.id, www.epas.paritkebumen.desa.id, www.lapor.parit
↪kebumen.desa.id, www.pso.paritkebumen.desa.id
valid from                      | 2024-11-04 21:09:23 UTC
valid until                     | 2025-02-02 21:09:22 UTC
```

Solution:

Log Method

Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary

This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Quality of Detection: 98

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | C378EC72F0C28748350B96DE419748546CE65318
fingerprint (SHA-256)           | C07652AD9A2734A17115EAB083D8843B7DCF4D1339ED23
↪EFC359B12E890CDEB8
issued by                       | CN=R11,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 049EF750C9E350875AFB060C8CE15DD76B50
signature algorithm             | sha256WithRSAEncryption
```

... continues on next page ...

... continued from previous page ...

subject	CN=www.lapor.paritkebumen.desa.id
subject alternative names (SAN)	*.paritkebumen.desa.id, paritkebumen.desa.id, ↪www.cloud.paritkebumen.desa.id, www.epas.paritkebumen.desa.id, www.lapor.parit ↪kebumen.desa.id, www.pso.paritkebumen.desa.id
valid from	2024-11-04 21:09:23 UTC
valid until	2025-02-02 21:09:22 UTC

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Quality of Detection: 98

Vulnerability Detection Result
The following certificate details of the remote service were collected.
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection: 80

Vulnerability Detection Result
`The remote SSL/TLS service supports the following SSL/TLS protocol version(s):`
`TLSv1.2`
`TLSv1.3`

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`
OID:1.3.6.1.4.1.25623.1.0.105782
Version used: `2024-09-27T05:05:23Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection: 80

Vulnerability Detection Result
`The remote SSL/TLS service supports the following SSL/TLS protocol version(s):`
`TLSv1.2`
`TLSv1.3`

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.105782
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result
A web server is running on this port through SSL

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2023-06-14T05:05:19Z

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result
A TLScustom server answered on this port

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

... continues on next page ...

. . . continued from previous page . . .

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result
`A web server is running on this port through SSL`

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result
`A TLScustom server answered on this port`

Solution:

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2023-06-14T05:05:19Z

[return to 202.74.239.249]

2.1.6 Log general/tcp

Log (CVSS: 0.0)
NVT: Hostname Determination Reporting

Summary
The script reports information on how the hostname of the target was determined.

Quality of Detection: 80

Vulnerability Detection Result
Hostname determination for IP 202.74.239.249:
Hostname|Source
server101share.extremhost.net|Reverse-DNS
www.cloud.paritkebumen.desa.id|SSL/TLS server certificate
www.epas.paritkebumen.desa.id|SSL/TLS server certificate
www.lapor.paritkebumen.desa.id|SSL/TLS server certificate
www.paritkebumen.desa.id|Forward-DNS
www.pso.paritkebumen.desa.id|SSL/TLS server certificate

Solution:

Log Method
Details: Hostname Determination Reporting
OID:1.3.6.1.4.1.25623.1.0.108449
Version used: 2022-07-27T10:11:28Z

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This VT consolidates and reports the information collected by the following VTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)

... continues on next page ...

... continued from previous page ...

- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

If you know any of the information reported here, please send the full output to the referenced community forum.

Quality of Detection: 80

Vulnerability Detection Result

```
Unknown banners have been collected which might help to identify the OS running
↪on this host. If these banners containing information about the host OS please
↪ report the following information to https://forum.greenbone.net/c/vulnerabili
↪ty-tests/7:
Banner: Server: imunify360-webshield/1.21
Identified from: HTTP Server banner on port 2082/tcp
Banner: Server: imunify360-webshield/1.21
Identified from: HTTP Server banner on port 2083/tcp
Banner: Server: imunify360-webshield/1.21
Identified from: HTTP Server banner on port 52229/tcp
Banner: Server: imunify360-webshield/1.21
Identified from: HTTP Server banner on port 52230/tcp
```

Solution:

Log Method

Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `2023-06-22T10:34:15Z`

References

`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Traceroute

Summary

Collect information about the network route and network distance between the scanner host and the target host.

Quality of Detection: 80

Vulnerability Detection Result

```
Network route from scanner (10.81.20.14) to target (202.74.239.249):
10.81.20.14
10.12.10.254
```

... continues on next page ...

... continued from previous page ...

202.74.239.249
Network distance between scanner and target: 3

Solution:

Vulnerability Insight
For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Log Method
A combination of the protocols ICMP and TCP is used to determine the route. This method is applicable for IPv4 only and it is also known as 'traceroute'.
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: 2022-10-17T11:13:19Z

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several VTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community forum.

Quality of Detection: 80

Vulnerability Detection Result
No Best matching OS identified. Please see the VT 'Unknown OS and Service Banner Reporting' (OID: 1.3.6.1.4.1.25623.1.0.108441) for possible ways to identify this OS.

Solution:

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2024-11-27T05:05:40Z

References
url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: SSL/TLS: Hostname discovery from server certificate

Summary
It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.

Quality of Detection: 98

Vulnerability Detection Result
```
The following additional and resolvable hostnames were detected:
www.cloud.paritkebumen.desa.id
www.epas.paritkebumen.desa.id
www.lapor.paritkebumen.desa.id
www.pso.paritkebumen.desa.id
The following additional and resolvable hostnames pointing to a different host i
↪p were detected:
paritkebumen.desa.id
```

Solution:

Log Method
Details: SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: 2021-11-22T15:32:39Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Hostname discovery from server certificate

Summary
It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.

Quality of Detection: 98

Vulnerability Detection Result
```
The following additional and resolvable hostnames were detected:
server101share.extremhost.net
www.cloud.paritkebumen.desa.id
www.epas.paritkebumen.desa.id
www.lapor.paritkebumen.desa.id
www.pso.paritkebumen.desa.id
The following additional and resolvable hostnames pointing to a different host i
↪p were detected:
paritkebumen.desa.id
```

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: 2021-11-22T15:32:39Z

[return to 202.74.239.249]

2.1.7 Log 52229/tcp

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
```
The Hostname/IP "www.epas.paritkebumen.desa.id" was used to access the remote ho
↪st.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
```

... continues on next page ...

... continued from previous page ...

```
The following directories were used for web application scanning:
https://www.epas.paritkebumen.desa.id:52229/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "www.lapor.paritkebumen.desa.id" was used to access the remote h
↪ost.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
```

... continues on next page ...

... continued from previous page ...

```
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://www.lapor.paritkebumen.desa.id:52229/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "www.pso.paritkebumen.desa.id" was used to access the remote hos
↪t.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
```

... continues on next page ...

... continued from previous page ...

```
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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://www.pso.paritkebumen.desa.id:52229/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "server101share.extremhost.net" was used to access the remote ho
↪st.
```

... continues on next page ...

... continued from previous page ...

```
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://server101share.extremhost.net:52229/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method
Details: `Web Application Scanning Consolidation / Info Reporting`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `2024-09-19T05:05:57Z`

References
`url: https://forum.greenbone.net/c/vulnerability-tests/7`

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary
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.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "www.paritkebumen.desa.id" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://www.paritkebumen.desa.id:52229/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method

Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

References

url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: Web Application Scanning Consolidation / Info Reporting

Summary

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

... continues on next page ...

... continued from previous page ...

- 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.

Quality of Detection: 80

Vulnerability Detection Result

```
The Hostname/IP "www.cloud.paritkebumen.desa.id" was used to access the remote h
↪ost.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he 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 20.8.2)" was used to access
↪ the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for web app
↪lication scanning. You can enable this again with the "Add historic /scripts a
↪nd /cgi-bin to directories for CGI scanning" option within the "Global variabl
↪e settings" of the scan config in use.
The following directories were used for web application scanning:
https://www.cloud.paritkebumen.desa.id:52229/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Solution:

Log Method

Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2024-09-19T05:05:57Z

References

url: https://forum.greenbone.net/c/vulnerability-tests/7

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary

All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪----------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
```

... continues on next page ...

... continued from previous page ...

```
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪----------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
```

... continues on next page ...

... continued from previous page ...

```
Document-Policy                  | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Expect-CT                        | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming header
Feature-Policy                   | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy               | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Public-Key-Pins                  | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                  | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                   | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                   | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                   | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                   | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security        | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options           | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                  | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                 | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

... continues on next page ...

... continued from previous page ...

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

Missing Headers	More Information
Content-Security-Policy	https://owasp.org/www-project-secure-headers/#content-security-policy
Cross-Origin-Embedder-Policy	https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Cross-Origin-Opener-Policy	https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Cross-Origin-Resource-Policy	https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header
Document-Policy	https://w3c.github.io/webappsec-feature-policy/document-policy#document-policy-http-header
Expect-CT	https://owasp.org/www-project-secure-headers/#expect-ct, Note: This is an upcoming header
Feature-Policy	https://owasp.org/www-project-secure-headers/#feature-policy, Note: The Feature Policy header has been renamed to Permissions Policy
Permissions-Policy	https://w3c.github.io/webappsec-feature-policy/#permissions-policy-http-header-field
Public-Key-Pins	Please check the output of the VTs including 'SSL/TLS:' and 'HPKP' in their name for more information and configuration help. Note: Most major browsers have dropped / deprecated support for this header in 2020.
Referrer-Policy	https://owasp.org/www-project-secure-headers/#referrer-policy
Sec-Fetch-Dest	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo

... continues on next page ...

... continued from previous page ...

```
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                  | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security       | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options          | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                 | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Missing Headers                   | More Information
----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪----------------------------------------------------------------------------
↪----------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
```

... continues on next page ...

... continued from previous page ...

```
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪----------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming header
```

... continues on next page ...

... continued from previous page ...

```
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers

... continues on next page ...

... continued from previous page ...

url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the remote web server.
On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Quality of Detection: 80

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪----------------------------------------------------------------------------------
↪----------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Cross-Origin-Embedder-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Opener-Policy        | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Cross-Origin-Resource-Policy      | https://scotthelme.co.uk/coop-and-coep/, Not
↪e: This is an upcoming header
Document-Policy                   | https://w3c.github.io/webappsec-feature-poli
↪cy/document-policy#document-policy-http-header
Expect-CT                         | https://owasp.org/www-project-secure-headers
↪/#expect-ct, Note: This is an upcoming header
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissi
↪ons Policy
Permissions-Policy                | https://w3c.github.io/webappsec-feature-poli
↪cy/#permissions-policy-http-header-field
Public-Key-Pins                   | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HPKP' in their name for more information and configuration he
↪lp. Note: Most major browsers have dropped / deprecated support for this heade
↪r in 2020.
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
Sec-Fetch-Dest                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-Mode                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
```

... continues on next page ...

... continued from previous page ...

```
Sec-Fetch-Site                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Sec-Fetch-User                    | https://developer.mozilla.org/en-US/docs/Web
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header suppo
↪rted only in newer browsers like e.g. Firefox 90
Strict-Transport-Security         | Please check the output of the VTs including
↪ 'SSL/TLS:' and 'HSTS' in their name for more information and configuration he
↪lp.
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated suppor
↪t for this header in 2020.
```

Solution:

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2021-07-14T06:19:43Z

References
url: https://owasp.org/www-project-secure-headers/
url: https://owasp.org/www-project-secure-headers/#div-headers
url: https://securityheaders.com/

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result

```
The remote service advertises support for the following Network Protocol(s) via
↪the ALPN extension:
```

... continues on next page ...

... continued from previous page ...

SSL/TLS Protocol:Network Protocol
TLSv1.2:HTTP/1.1
TLSv1.2:HTTP/2

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
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
TLSv1.2:HTTP/2

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
```
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
TLSv1.2:HTTP/2
```

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
```
The remote service advertises support for the following Network Protocol(s) via
↪the ALPN extension:
SSL/TLS Protocol:Network Protocol
```

... continues on next page ...

... continued from previous page ...

TLSv1.2:HTTP/1.1
TLSv1.2:HTTP/2

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
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
TLSv1.2:HTTP/2

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

Log (CVSS: 0.0)
NVT: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result
```
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
TLSv1.2:HTTP/2
```

Solution:

Log Method
Details: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
OID:1.3.6.1.4.1.25623.1.0.108099
Version used: 2024-09-27T05:05:23Z

References
```
url: https://tools.ietf.org/html/rfc7301
url: https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04
```

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

Product detection result
```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

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

Quality of Detection: 98

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
```

Solution:

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2024-09-30T08:38:05Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Quality of Detection: 98

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_ARIA_128_GCM_SHA256
TLS_RSA_WITH_ARIA_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.3 protocol:
TLS_AES_128_GCM_SHA256

Solution:

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Log Method
Details: SSL/TLS: Report Medium Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: 2024-09-27T05:05:23Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

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

Quality of Detection: 98

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_ARIA_128_GCM_SHA256
TLS_RSA_WITH_ARIA_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_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

... continues on next page ...

... continued from previous page ...

Solution:

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2024-09-27T05:05:23Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

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

Quality of Detection: 98

Vulnerability Detection Result
'Strong' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_ARIA_128_GCM_SHA256
TLS_RSA_WITH_ARIA_256_GCM_SHA384

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
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.
```

Solution:

Vulnerability Insight
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.

Log Method
Details: `SSL/TLS: Report Supported Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: `2024-09-27T05:05:23Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing

Summary
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.

Quality of Detection: 80

Vulnerability Detection Result

```
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 403 Forbidden
Date: ***replaced***
Content-Type: text/html
```

... continues on next page ...

... continued from previous page ...

```
Content-Length: ***replaced***
Connection: close
Server: imunify360-webshield/1.21
```

Solution:
Solution type: Workaround
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.

Log Method
Details: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
OID:1.3.6.1.4.1.25623.1.0.108247
Version used: 2024-02-08T05:05:59Z

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

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

Summary
The remote web server is not enforcing HTTP Strict Transport Security (HSTS).

Quality of Detection: 80

Vulnerability Detection Result
The remote web server is not enforcing HSTS.
HTTP-Banner:
HTTP/1.1 403 Forbidden
Date: ***replaced***
Content-Type: text/html
Content-Length: ***replaced***
Connection: close

... continues on next page ...

... continued from previous page ...

Server: imunify360-webshield/1.21

Solution:
Solution type: Workaround
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.

Log Method
Details: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
OID:1.3.6.1.4.1.25623.1.0.105879
Version used: 2024-02-08T05:05:59Z

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

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not

... continues on next page ...

... continued from previous page ...

```
↪match the hostname "www.pso.paritkebumen.desa.id".
Certificate details:
fingerprint (SHA-1)             | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)           | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A
issued by                       | CN=R10,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 030996EF9572D98AE1689504F343AC7352B9
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=server101share.extremhost.net
subject alternative names (SAN) | server101share.extremhost.net
valid from                      | 2024-11-13 01:31:40 UTC
valid until                     | 2025-02-11 01:31:39 UTC
```

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.pso.paritkebumen.desa.id".
Certificate details:
fingerprint (SHA-1)             | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)           | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
```

... continues on next page ...

... continued from previous page ...

```
↪E19057D81273EEB29A
issued by                       | CN=R10,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 030996EF9572D98AE1689504F343AC7352B9
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=server101share.extremhost.net
subject alternative names (SAN) | server101share.extremhost.net
valid from                      | 2024-11-13 01:31:40 UTC
valid until                     | 2025-02-11 01:31:39 UTC
```

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.pso.paritkebumen.desa.id".
Certificate details:
fingerprint (SHA-1)             | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)           | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A
issued by                       | CN=R10,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 030996EF9572D98AE1689504F343AC7352B9
```

... continues on next page ...

... continued from previous page ...

signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.lapor.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC

... continues on next page ...

... continued from previous page ...

valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.epas.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A	
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.lapor.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method

... continues on next page ...

... continued from previous page ...

Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.lapor.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.epas.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.epas.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.cloud.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

. . . continues on next page . . .

... continued from previous page ...

cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.cloud.paritkebumen.desa.id".
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

... continues on next page ...

... continued from previous page ...

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.cloud.paritkebumen.desa.id".
Certificate details:
fingerprint (SHA-1)             | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)           | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A
issued by                       | CN=R10,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 030996EF9572D98AE1689504F343AC7352B9
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=server101share.extremhost.net
subject alternative names (SAN) | server101share.extremhost.net
valid from                      | 2024-11-13 01:31:40 UTC
valid until                     | 2025-02-11 01:31:39 UTC
```

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

... continues on next page ...

... continued from previous page ...

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "server101share.extremhost.net".
Certificate details:
fingerprint (SHA-1)                | C378EC72F0C28748350B96DE419748546CE65318
fingerprint (SHA-256)              | C07652AD9A2734A17115EAB083D8843B7DCF4D1339ED23
↪EFC359B12E890CDEB8
issued by                          | CN=R11,O=Let's Encrypt,C=US
public key size (bits)             | 2048
serial                             | 049EF750C9E350875AFB060C8CE15DD76B50
signature algorithm                | sha256WithRSAEncryption
subject                            | CN=www.lapor.paritkebumen.desa.id
subject alternative names (SAN) | *.paritkebumen.desa.id, paritkebumen.desa.id,
↪www.cloud.paritkebumen.desa.id, www.epas.paritkebumen.desa.id, www.lapor.parit
↪kebumen.desa.id, www.pso.paritkebumen.desa.id
valid from                         | 2024-11-04 21:09:23 UTC
valid until                        | 2025-02-02 21:09:22 UTC
```

Solution:

Log Method

Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "server101share.extremhost.net".
Certificate details:
fingerprint (SHA-1)                | C378EC72F0C28748350B96DE419748546CE65318
fingerprint (SHA-256)              | C07652AD9A2734A17115EAB083D8843B7DCF4D1339ED23
↪EFC359B12E890CDEB8
issued by                          | CN=R11,O=Let's Encrypt,C=US
public key size (bits)             | 2048
serial                             | 049EF750C9E350875AFB060C8CE15DD76B50
signature algorithm                | sha256WithRSAEncryption
subject                            | CN=www.lapor.paritkebumen.desa.id
subject alternative names (SAN) | *.paritkebumen.desa.id, paritkebumen.desa.id,
↪www.cloud.paritkebumen.desa.id, www.epas.paritkebumen.desa.id, www.lapor.parit
↪kebumen.desa.id, www.pso.paritkebumen.desa.id
valid from                         | 2024-11-04 21:09:23 UTC
valid until                        | 2025-02-02 21:09:22 UTC
```

Solution:

Log Method

Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "server101share.extremhost.net".
Certificate details:
fingerprint (SHA-1)             | C378EC72F0C28748350B96DE419748546CE65318
fingerprint (SHA-256)           | C07652AD9A2734A17115EAB083D8843B7DCF4D1339ED23
↪EFC359B12E890CDEB8
issued by                       | CN=R11,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 049EF750C9E350875AFB060C8CE15DD76B50
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=www.lapor.paritkebumen.desa.id
subject alternative names (SAN) | *.paritkebumen.desa.id, paritkebumen.desa.id,
↪www.cloud.paritkebumen.desa.id, www.epas.paritkebumen.desa.id, www.lapor.parit
↪kebumen.desa.id, www.pso.paritkebumen.desa.id
valid from                      | 2024-11-04 21:09:23 UTC
valid until                     | 2025-02-02 21:09:22 UTC
```

Solution:

Log Method

Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.paritkebumen.desa.id".
Certificate details:
fingerprint (SHA-1)             | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)           | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A
issued by                       | CN=R10,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 030996EF9572D98AE1689504F343AC7352B9
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=server101share.extremhost.net
subject alternative names (SAN) | server101share.extremhost.net
valid from                      | 2024-11-13 01:31:40 UTC
valid until                     | 2025-02-11 01:31:39 UTC
```

Solution:

Log Method

Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result

Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result

```
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.paritkebumen.desa.id".
```

... continues on next page ...

... continued from previous page ...

```
Certificate details:
fingerprint (SHA-1)             | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)           | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A
issued by                       | CN=R10,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 030996EF9572D98AE1689504F343AC7352B9
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=server101share.extremhost.net
subject alternative names (SAN) | server101share.extremhost.net
valid from                      | 2024-11-13 01:31:40 UTC
valid until                     | 2025-02-11 01:31:39 UTC
```

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Quality of Detection: 98

Vulnerability Detection Result
The certificate of the remote service contains a common name (CN) that does not
↪match the hostname "www.paritkebumen.desa.id".
Certificate details:
fingerprint (SHA-1) | 5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256) | 532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8
↪E19057D81273EEB29A

... continues on next page ...

... continued from previous page ...

issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN
OID:1.3.6.1.4.1.25623.1.0.103141
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: imunify360-webshield/1.21

Solution:

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2023-08-01T13:29:10Z

... continues on next page ...

. . . continued from previous page . . .

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result
`The remote HTTP Server banner is:`
`Server: imunify360-webshield/1.21`

Solution:

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `2023-08-01T13:29:10Z`

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary

. . . continues on next page . . .

... continued from previous page ...

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Quality of Detection: 80

Vulnerability Detection Result

```
The remote HTTP Server banner is:
Server: imunify360-webshield/1.21
```

Solution:

Log Method

Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2023-08-01T13:29:10Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary

This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Quality of Detection: 98

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)              | C378EC72F0C28748350B96DE419748546CE65318
fingerprint (SHA-256)            | C07652AD9A2734A17115EAB083D8843B7DCF4D1339ED23
↪EFC359B12E890CDEB8
issued by                        | CN=R11,O=Let's Encrypt,C=US
public key size (bits)           | 2048
serial                           | 049EF750C9E350875AFB060C8CE15DD76B50
signature algorithm              | sha256WithRSAEncryption
subject                          | CN=www.lapor.paritkebumen.desa.id
subject alternative names (SAN)  | *.paritkebumen.desa.id, paritkebumen.desa.id,
↪www.cloud.paritkebumen.desa.id, www.epas.paritkebumen.desa.id, www.lapor.parit
↪kebumen.desa.id, www.pso.paritkebumen.desa.id
valid from                       | 2024-11-04 21:09:23 UTC
valid until                      | 2025-02-02 21:09:22 UTC
```

Solution:

... continues on next page ...

... continued from previous page ...

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Quality of Detection: 98

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | C378EC72F0C28748350B96DE419748546CE65318
fingerprint (SHA-256)           | C07652AD9A2734A17115EAB083D8843B7DCF4D1339ED23
↪EFC359B12E890CDEB8
issued by                       | CN=R11,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 049EF750C9E350875AFB060C8CE15DD76B50
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=www.lapor.paritkebumen.desa.id
subject alternative names (SAN) | *.paritkebumen.desa.id, paritkebumen.desa.id,
↪www.cloud.paritkebumen.desa.id, www.epas.paritkebumen.desa.id, www.lapor.parit
↪kebumen.desa.id, www.pso.paritkebumen.desa.id
valid from                      | 2024-11-04 21:09:23 UTC
valid until                     | 2025-02-02 21:09:22 UTC
```

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 98

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | C378EC72F0C28748350B96DE419748546CE65318
fingerprint (SHA-256)           | C07652AD9A2734A17115EAB083D8843B7DCF4D1339ED23
↪EFC359B12E890CDEB8
issued by                       | CN=R11,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 049EF750C9E350875AFB060C8CE15DD76B50
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=www.lapor.paritkebumen.desa.id
subject alternative names (SAN) | *.paritkebumen.desa.id, paritkebumen.desa.id,
↪www.cloud.paritkebumen.desa.id, www.epas.paritkebumen.desa.id, www.lapor.parit
↪kebumen.desa.id, www.pso.paritkebumen.desa.id
valid from                      | 2024-11-04 21:09:23 UTC
valid until                     | 2025-02-02 21:09:22 UTC
```

Solution:

Log Method

Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary

This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Quality of Detection: 98

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
fingerprint (SHA-1)             | C378EC72F0C28748350B96DE419748546CE65318
fingerprint (SHA-256)           | C07652AD9A2734A17115EAB083D8843B7DCF4D1339ED23
↪EFC359B12E890CDEB8
issued by                       | CN=R11,O=Let's Encrypt,C=US
public key size (bits)          | 2048
serial                          | 049EF750C9E350875AFB060C8CE15DD76B50
signature algorithm             | sha256WithRSAEncryption
```

... continues on next page ...

... continued from previous page ...

subject	CN=www.lapor.paritkebumen.desa.id
subject alternative names (SAN)	*.paritkebumen.desa.id, paritkebumen.desa.id, ↪www.cloud.paritkebumen.desa.id, www.epas.paritkebumen.desa.id, www.lapor.parit ↪kebumen.desa.id, www.pso.paritkebumen.desa.id
valid from	2024-11-04 21:09:23 UTC
valid until	2025-02-02 21:09:22 UTC

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Quality of Detection: 98

Vulnerability Detection Result
The following certificate details of the remote service were collected.
Certificate details:

fingerprint (SHA-1)	5AA9DFB7934F2ACD2476143313474149045632F2
fingerprint (SHA-256)	532FBD1B92321DBCF4653FF359DD6268529F887D3F54C8 ↪E19057D81273EEB29A
issued by	CN=R10,O=Let's Encrypt,C=US
public key size (bits)	2048
serial	030996EF9572D98AE1689504F343AC7352B9
signature algorithm	sha256WithRSAEncryption
subject	CN=server101share.extremhost.net
subject alternative names (SAN)	server101share.extremhost.net
valid from	2024-11-13 01:31:40 UTC
valid until	2025-02-11 01:31:39 UTC

Solution:

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection: 80

Vulnerability Detection Result
`The remote SSL/TLS service supports the following SSL/TLS protocol version(s):`
`TLSv1.2`
`TLSv1.3`

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`
OID:1.3.6.1.4.1.25623.1.0.105782
Version used: `2024-09-27T05:05:23Z`

Log (CVSS: 0.0)
NVT: SSL/TLS: Version Detection

Summary
Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Quality of Detection: 80

Vulnerability Detection Result
`The remote SSL/TLS service supports the following SSL/TLS protocol version(s):`
`TLSv1.2`
`TLSv1.3`

Solution:

Log Method
Sends multiple connection requests to the remote service and attempts to determine the SSL/TLS protocol versions supported by the service from the replies.
Note: The supported SSL/TLS protocol versions included in the report of this VT are reported independently from the allowed / supported SSL/TLS ciphers.
Details: `SSL/TLS: Version Detection`

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.105782
Version used: 2024-09-27T05:05:23Z

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result
A web server is running on this port through SSL

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2023-06-14T05:05:19Z

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result
A TLScustom server answered on this port

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

... continues on next page ...

. . . continued from previous page . . .

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2023-06-14T05:05:19Z

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result
A web server is running on this port through SSL

Solution:

Vulnerability Insight
This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2023-06-14T05:05:19Z

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection: 80

Vulnerability Detection Result
A TLScustom server answered on this port

Solution:

Vulnerability Insight

. . . continues on next page . . .

... continued from previous page ...

This plugin attempts to guess which service is running on the remote port(s). For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2023-06-14T05:05:19Z`

[return to 202.74.239.249]
