Scan Report

November 18, 2025

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 "691bcd7a5e1554ee54f63537-691bcd7a5e1554ee54f63569-81a0efd9". The scan started at Tue Nov 18 01:36:18 2025 UTC and ended at Tue Nov 18 03:05:24 2025 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
77.37.76.204 ipwija.ac.id	0	0	1	20	0
147.79.120.130 ipwija.ac.id	0	0	1	19	0
2a02:4780:50:ab0f:28c0:13ac:4306:882b ipwija.ac.id	0	0	0	2	0
2a02:4780:4e:fa98:35c9:8f37:d5f6:6960 ipwija.ac.id	0	0	0	2	0
Total: 4	0	0	2	43	0

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

This report contains all 45 results selected by the filtering described above. Before filtering there were 47 results.

2 Results per Host

2.1 77.37.76.204

Host scan start	Tue Nov 18 01:37:38 2025 UTC
Host scan end	Tue Nov 18 03:05:03 2025 UTC

Service (Port)	Threat Level
general/tcp	Low
general/tcp	Log
general/CPE-T	Log
80/tcp	Log
443/tcp	Log

2.1.1 Low general/tcp

Low (CVSS: 2.6) NVT: TCP Timestamps Information Disclosure
. . . continues on next page . . .

... continued from previous page ...

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

Quality of Detection (QoD): 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: 2332776396
Packet 2: 971946214
```

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 77.37.76.204]

2.1.2 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 (QoD): 80%

Vulnerability Detection Result
```
Hostname determination for IP 77.37.76.204:
Hostname|Source
ipwija.ac.id|Forward-DNS
```

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: 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 (QoD): 80%

Vulnerability Detection Result
```
Best matching OS:
OS:           Linux Kernel
CPE:          cpe:/o:linux:kernel
Found by VT:  1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICM
↪P))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

Solution:

. . . continues on next page . . .

... continued from previous page ...

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2025-11-14T15:41:06Z

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

Log (CVSS: 0.0)
NVT: PHP Detection Consolidation

Summary
Consolidation of PHP detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Detected PHP
Version:       8.2.28
Location:      443/tcp
CPE:           cpe:/a:php:php:8.2.28
Concluded from version/product identification result:
X-Powered-By: PHP/8.2.28
Concluded from version/product identification location:
https://ipwija.ac.id/
```

Solution:

Log Method
Details: PHP Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.171722
Version used: 2025-09-24T05:39:03Z

References
url: https://www.php.net/

Log (CVSS: 0.0)
NVT: Traceroute

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

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Network route from scanner (172.18.0.5) to target (77.37.76.204):
172.18.0.5
10.206.6.215
10.206.35.35
10.206.32.2
173.255.239.102
23.203.156.16
62.115.50.170
62.115.137.18
62.115.139.35
62.115.138.71
62.115.137.55
153.92.2.201
62.115.139.130
62.115.125.55
62.115.33.63
148.51.252.130
148.51.251.151
38.104.17.154
153.92.2.35
77.37.76.204
Network distance between scanner and target: 20
```

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: 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)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)

... continues on next page ...

... continued from previous page ...

- 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 (QoD): 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: hcdn
Identified from: HTTP Server banner on port 443/tcp
Banner: Server: hcdn
Identified from: HTTP Server banner on port 80/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`

[return to 77.37.76.204]

2.1.3 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 (QoD): 80%

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

77.37.76.204|cpe:/a:php:php:8.2.28
77.37.76.204|cpe:/o:linux:kernel

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 77.37.76.204]

2.1.4 Log 80/tcp

Log (CVSS: 0.0)
NVT: Allowed HTTP Methods Enumeration

Summary
Enumerates which HTTP methods are allowed.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
The following list contains the URLs and corresponding supported HTTP methods.

URL	HTTP Methods
http://ipwija.ac.id/	DELETE,OPTIONS

Solution:

Vulnerability Insight
- Basic HTTP methods: GET, HEAD, POST, PUT, DELETE, CONNECT, OPTIONS, TRACE
- Extended HTTP methods: ACL, BASELINE-CONTROL, BIND, CHECKIN, CHECKOUT, COPY, LABEL, LINK, LOCK, MERGE, MKACTIVITY, MKCALENDAR, MKCOL, MKREDIRECTREF, MKWORKSPACE, MOVE, ORDERPATCH, PATCH, PRI, PROPFIND, PROPPATCH, REBIND, REPORT, SEARCH, UNBIND, UNCHECKOUT, UNLINK, UNLOCK, UPDATE, UPDATEREDIRECTREF, VERSION-CONTROL

Log Method
Sends multiple HTTP requests and checks the responses.
Disclaimer:

... continues on next page ...

... continued from previous page ...

- This enumeration script is provided 'as is' (means no support is given) and only providing rudimentary information about the possible enabled methods
- This script doesn't guarantee completeness or full reliability
For more reliable determination of the enabled HTTP methods please inspect the configuration of the web server manually and directly on the target host.
Details: `Allowed HTTP Methods Enumeration`
OID:1.3.6.1.4.1.25623.1.0.153974
Version used: `2025-02-28T05:38:49Z`

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 (QoD): 80%

Vulnerability Detection Result

```
Header Name             | Header Value
------------------------------------------------
Content-Security-Policy | upgrade-insecure-requests
Missing Headers                   | More Information
-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪-------------------------------------------------
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
```

... continues on next page ...

... continued from previous page ...

```
↪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: 2025-03-21T15:40:43Z

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 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 (QoD): 80%

Vulnerability Detection Result

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

Solution:

... continues on next page ...

. . . continued from previous page . . .

Log Method
Details: `HTTP Server Banner Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: `2025-01-31T15:39:24Z`

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 (QoD): 80%

Vulnerability Detection Result
```
The remote HTTP Server banner is:
Server: hcdn
```

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: Response Time / No 404 Error Code Check

Summary
This VT tests if the remote web server does not reply with a 404 error code and checks if it is replying to the scanners requests in a reasonable amount of time.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The host returns a 30x (e.g. 301) error code when a non-existent file is request
↪ed. Some HTTP-related checks have been disabled.
```

Solution:

Vulnerability Insight
. . . continues on next page . . .

... continued from previous page ...

This web server might show the following issues:
- it is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page, authentication page or redirect instead.
The Scanner might enabled some counter measures for that, however they might be insufficient. If a great number of security issues are reported for this port, they might not all be accurate.
- it doesn't response in a reasonable amount of time to various HTTP requests sent by this VT. In order to keep the scan total time to a reasonable amount, the remote web server might not be tested. If the remote server should be tested it has to be fixed to have it reply to the scanners requests in a reasonable amount of time.
Alternatively the 'Maximum response time (in seconds)' preference could be raised to a higher value if longer scan times are accepted.

Log Method
Details: `Response Time / No 404 Error Code Check`
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: `2025-04-11T15:45:04Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 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: `2025-03-05T05:38:53Z`

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

... continues on next page ...

... continued from previous page ...

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 (QoD): 80%

Vulnerability Detection Result

```
The Hostname/IP "ipwija.ac.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 23.8.5)" 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://ipwija.ac.id/
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: 2025-10-10T05:39:02Z

References

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

[return to 77.37.76.204]

2.1.5 Log 443/tcp

Log (CVSS: 0.0)
NVT: Allowed HTTP Methods Enumeration

Summary
Enumerates which HTTP methods are allowed.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
The following list contains the URLs and corresponding supported HTTP methods.
URL                   | HTTP Methods
-------------------------------------
https://ipwija.ac.id/ | GET
```

Solution:

Vulnerability Insight
- Basic HTTP methods: GET, HEAD, POST, PUT, DELETE, CONNECT, OPTIONS, TRACE
- Extended HTTP methods: ACL, BASELINE-CONTROL, BIND, CHECKIN, CHECKOUT, COPY, LABEL, LINK, LOCK, MERGE, MKACTIVITY, MKCALENDAR, MKCOL, MKREDIRECTREF, MKWORKSPACE, MOVE, ORDERPATCH, PATCH, PRI, PROPFIND, PROPPATCH, REBIND, REPORT, SEARCH, UNBIND, UNCHECKOUT, UNLINK, UNLOCK, UPDATE, UPDATEREDIRECTREF, VERSION-CONTROL

Log Method
Sends multiple HTTP requests and checks the responses.
Disclaimer:
- This enumeration script is provided 'as is' (means no support is given) and only providing rudimentary information about the possible enabled methods
- This script doesn't guarantee completeness or full reliability
For more reliable determination of the enabled HTTP methods please inspect the configuration of the web server manually and directly on the target host.
Details: `Allowed HTTP Methods Enumeration`
OID:1.3.6.1.4.1.25623.1.0.153974
Version used: `2025-02-28T05:38:49Z`

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 (QoD): 80%

Vulnerability Detection Result

```
Header Name             | Header Value
-----------------------------------------------------
Content-Security-Policy | upgrade-insecure-requests
Missing Headers                   | More Information
-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪----------
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
```

... continues on next page ...

... continued from previous page ...

```
↪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: 2025-03-21T15:40:43Z

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 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 (QoD): 80%

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner | Enumeration technique
--------------------------------------------------------------------------------
Server: hcdn  | 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: 2025-01-31T15:39:24Z

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 (QoD): 80%

Vulnerability Detection Result
```
The remote HTTP Server banner is:
Server: hcdn
```

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 (QoD): 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.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2025-03-05T05:38:53Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 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: `2025-03-05T05:38:53Z`

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 (QoD): 80%

Vulnerability Detection Result
```
The Hostname/IP "ipwija.ac.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
```

... continues on next page ...

... continued from previous page ...

```
↪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 23.8.5)" 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://ipwija.ac.id/
https://ipwija.ac.id/about
https://ipwija.ac.id/account
https://ipwija.ac.id/community
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
The following directories were excluded from web application scanning because th
↪e "Regex pattern to exclude directories from CGI scanning" setting of the VT "
↪Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was
↪: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graph
↪ic|grafik|picture|bilder|thumbnail|media/|skins?/)"
https://ipwija.ac.id/wp-content/plugins/chaty/admin/assets/js
https://ipwija.ac.id/wp-content/plugins/chaty/css
https://ipwija.ac.id/wp-content/plugins/chaty/js
https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/css
https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/js
https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/swv/js
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals
https://ipwija.ac.id/wp-content/plugins/elementor/assets/images
https://ipwija.ac.id/wp-content/plugins/elementor/assets/js
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/animations/styles
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/font-awesome/css
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/swiper/v8/css
https://ipwija.ac.id/wp-content/plugins/feeds-for-tiktok/vendor/smashballoon/cus
↪tomizer/sb-common/sb-customizer/build/static/css
https://ipwija.ac.id/wp-content/plugins/feeds-for-tiktok/vendor/smashballoon/cus
↪tomizer/sb-common/sb-customizer/build/static/js
https://ipwija.ac.id/wp-content/plugins/h5p/h5p-php-library/styles
https://ipwija.ac.id/wp-content/plugins/insta-gallery/build/frontend/css
https://ipwija.ac.id/wp-content/plugins/instagram-feed/css
https://ipwija.ac.id/wp-content/plugins/instagram-feed/img
https://ipwija.ac.id/wp-content/plugins/instagram-feed/js
https://ipwija.ac.id/wp-content/plugins/interactive-3d-flipbook-powered-physics-
↪engine/assets/js
```

... continues on next page ...

... continued from previous page ...

```
https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/css
https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/js
https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/js/vendor
https://ipwija.ac.id/wp-content/plugins/revslider/public/css
https://ipwija.ac.id/wp-content/plugins/revslider/public/js
https://ipwija.ac.id/wp-content/plugins/revslider/public/js/libs
https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/libraries/thim-
↪ekits/css
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/assets//css/frontend
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/assets//js/frontend
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//countdo
↪wn/css
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//countdo
↪wn/js
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//magnifi
↪c-popup/css
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//magnifi
↪c-popup/js
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//owl-car
↪ousel/css
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//owl-car
↪ousel/js
https://ipwija.ac.id/wp-content/plugins/wp-stats-manager/css
https://ipwija.ac.id/wp-content/themes/eduma
https://ipwija.ac.id/wp-content/themes/eduma/assets/css
https://ipwija.ac.id/wp-content/themes/eduma/assets/js
https://ipwija.ac.id/wp-includes/css/dist/block-library
https://ipwija.ac.id/wp-includes/js
https://ipwija.ac.id/wp-includes/js/dist
https://ipwija.ac.id/wp-includes/js/dist/vendor
https://ipwija.ac.id/wp-includes/js/jquery
https://ipwija.ac.id/wp-includes/js/jquery/ui
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
https://ipwija.ac.id/ (p [19775] )
https://ipwija.ac.id/\ (page [wsm_traffic] subPage [UsersOnline] subTab [summary
↪\] )
https://ipwija.ac.id/aktivitas/\ (page [wsm_traffic] subPage [UsersOnline] subTa
↪b [summary\] )
https://ipwija.ac.id/alumni-2/\ (page [wsm_traffic] subPage [UsersOnline] subTab
↪ [summary\] )
https://ipwija.ac.id/arsip/\ (page [wsm_traffic] subPage [UsersOnline] subTab [s
↪ummary\] )
https://ipwija.ac.id/biaya-kuliah-universitas-ipwija/\ (page [wsm_traffic] subPa
↪ge [UsersOnline] subTab [summary\] )
https://ipwija.ac.id/events/\ (page [wsm_traffic] subPage [UsersOnline] subTab [
↪summary\] )
```

... continues on next page ...

... continued from previous page ...

```
https://ipwija.ac.id/fasilitas/\ (page [wsm_traffic] subPage [UsersOnline] subTa
↪b [summary\] )
https://ipwija.ac.id/hubungi-kami/\ (page [wsm_traffic] subPage [UsersOnline] su
↪bTab [summary\] )
https://ipwija.ac.id/informasi-beasiswa/\ (page [wsm_traffic] subPage [UsersOnli
↪ne] subTab [summary\] )
https://ipwija.ac.id/informasi-tes-seleksi/\ (page [wsm_traffic] subPage [UsersO
↪nline] subTab [summary\] )
https://ipwija.ac.id/kabar-terbaru/\ (page [wsm_traffic] subPage [UsersOnline] s
↪ubTab [summary\] )
https://ipwija.ac.id/kebijakan-dan-pengumuman/\ (page [wsm_traffic] subPage [Use
↪rsOnline] subTab [summary\] )
https://ipwija.ac.id/kemahasiswaan/\ (page [wsm_traffic] subPage [UsersOnline] s
↪ubTab [summary\] )
https://ipwija.ac.id/keseharian-di-kampus/\ (page [wsm_traffic] subPage [UsersOn
↪line] subTab [summary\] )
https://ipwija.ac.id/klinik/\ (page [wsm_traffic] subPage [UsersOnline] subTab [
↪summary\] )
https://ipwija.ac.id/magister-manajemen/\ (page [wsm_traffic] subPage [UsersOnli
↪ne] subTab [summary\] )
https://ipwija.ac.id/mengapa-ipwija/\ (page [wsm_traffic] subPage [UsersOnline]
↪subTab [summary\] )
https://ipwija.ac.id/pendaftaran/\ (page [wsm_traffic] subPage [UsersOnline] sub
↪Tab [summary\] )
https://ipwija.ac.id/pengumuman-penerimaan/\ (page [wsm_traffic] subPage [UsersO
↪nline] subTab [summary\] )
https://ipwija.ac.id/perpustakaan/\ (page [wsm_traffic] subPage [UsersOnline] su
↪bTab [summary\] )
https://ipwija.ac.id/program-studi-informatika/\ (page [wsm_traffic] subPage [Us
↪ersOnline] subTab [summary\] )
https://ipwija.ac.id/program-studi-kebidanan/\ (page [wsm_traffic] subPage [User
↪sOnline] subTab [summary\] )
https://ipwija.ac.id/program-studi-kewirausahaan/\ (page [wsm_traffic] subPage [
↪UsersOnline] subTab [summary\] )
https://ipwija.ac.id/program-studi-rekayasa-perangkat-lunak/\ (page [wsm_traffic
↪] subPage [UsersOnline] subTab [summary\] )
https://ipwija.ac.id/program-studi-sarajana-manajemen/\ (page [wsm_traffic] subP
↪age [UsersOnline] subTab [summary\] )
https://ipwija.ac.id/program-studi-sistem-informasi/\ (page [wsm_traffic] subPag
↪e [UsersOnline] subTab [summary\] )
https://ipwija.ac.id/pusat-karir/\ (page [wsm_traffic] subPage [UsersOnline] sub
↪Tab [summary\] )
https://ipwija.ac.id/pusat-konseling/\ (page [wsm_traffic] subPage [UsersOnline]
↪ subTab [summary\] )
https://ipwija.ac.id/pusat-teknologi-informasi/\ (page [wsm_traffic] subPage [Us
↪ersOnline] subTab [summary\] )
https://ipwija.ac.id/sekilas-ipwija/\ (page [wsm_traffic] subPage [UsersOnline]
```

... continues on next page ...

... continued from previous page ...

```
↪subTab [summary\] )
https://ipwija.ac.id/simulasi-rapor/\ (page [wsm_traffic] subPage [UsersOnline]
↪subTab [summary\] )
https://ipwija.ac.id/sorotan/\ (page [wsm_traffic] subPage [UsersOnline] subTab
↪[summary\] )
https://ipwija.ac.id/sosialisasi-p2mw-2025-di-universitas-ipwija-mahasiswa-didor
↪ong-jadi-wirausahawan-muda/\ (page [wsm_traffic] subPage [UsersOnline] subTab
↪[summary\] )
https://ipwija.ac.id/tanggal-penting/\ (page [wsm_traffic] subPage [UsersOnline]
↪ subTab [summary\] )
https://ipwija.ac.id/tentang-universitas-ipwija/\ (page [wsm_traffic] subPage [U
↪sersOnline] subTab [summary\] )
https://ipwija.ac.id/video/\ (page [wsm_traffic] subPage [UsersOnline] subTab [s
↪ummary\] )
https://ipwija.ac.id/wp-json/oembed/1.0/embed (#038;format [xml] url [https%3A%2
↪F%2Fipwija.ac.id%2F] )
https://ipwija.ac.id/xmlrpc.php (rsd [] )
The following cgi scripts were excluded from web application scanning because of
↪ the "Regex pattern to exclude cgi scripts" setting of the VT "Web mirroring"
↪(OID: 1.3.6.1.4.1.25623.1.0.10662) for this scan was: "\.(js|css)$"
Syntax : cginame (arguments [default value])
https://ipwija.ac.id/wp-content/plugins/chaty/admin/assets/js/picmo-latest-umd.m
↪in.js (ver [3.4.1] )
https://ipwija.ac.id/wp-content/plugins/chaty/admin/assets/js/picmo-umd.min.js (
↪ver [3.4.1] )
https://ipwija.ac.id/wp-content/plugins/chaty/css/chaty-front.min.css (ver [3.4.
↪11742195845] )
https://ipwija.ac.id/wp-content/plugins/chaty/js/cht-front-script.min.js (ver [3
↪.4.11742195845] )
https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/css/styles.css (
↪ver [6.0.6] )
https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/js/index.js (ver
↪ [6.0.6] )
https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/swv/js/index.js
↪(ver [6.0.6] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals/apple-
↪webkit.min.css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals/e-swip
↪er.min.css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals/shapes
↪.min.css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/frontend.min.css (v
↪er [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-divider.min.
↪css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-google_maps.
↪min.css (ver [3.28.4] )
```

... continues on next page ...

... continued from previous page ...

https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-heading.min.
↪css (ver [3.28.4])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-icon-box.min
↪.css (ver [3.28.4])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-image.min.cs
↪s (ver [3.28.4])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-nested-tabs.
↪min.css (ver [3.28.4])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-social-icons
↪.min.css (ver [3.28.4])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-spacer.min.c
↪ss (ver [3.28.4])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-video.min.cs
↪s (ver [3.28.4])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/js/frontend-modules.min
↪.js (ver [3.28.4])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/js/frontend.min.js (ver
↪ [3.28.4])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/js/webpack.runtime.min.
↪js (ver [3.28.4])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/animations/styles/e
↪-animation-pulse.min.css (ver [3.28.4])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/font-awesome/css/al
↪l.css (ver [1.3.2])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/swiper/v8/css/swipe
↪r.min.css (ver [8.4.5])
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/swiper/v8/swiper.mi
↪n.js (ver [8.4.5])
https://ipwija.ac.id/wp-content/plugins/feeds-for-tiktok/vendor/smashballoon/cus
↪tomizer/sb-common/sb-customizer/build/static/css/tikTokFeed.css (ver [6.8.1])
https://ipwija.ac.id/wp-content/plugins/feeds-for-tiktok/vendor/smashballoon/cus
↪tomizer/sb-common/sb-customizer/build/static/js/tikTokFeed.js (ver [1.1.1])
https://ipwija.ac.id/wp-content/plugins/h5p/h5p-php-library/styles/h5p.css (ver
↪[1.16.0])
https://ipwija.ac.id/wp-content/plugins/insta-gallery/assets/frontend/swiper/swi
↪per.min.css (ver [4.6.1])
https://ipwija.ac.id/wp-content/plugins/insta-gallery/assets/frontend/swiper/swi
↪per.min.js (ver [4.6.1])
https://ipwija.ac.id/wp-content/plugins/insta-gallery/build/frontend/css/style.c
↪ss (ver [4.6.1])
https://ipwija.ac.id/wp-content/plugins/instagram-feed/css/sbi-styles.min.css (v
↪er [6.9.0])
https://ipwija.ac.id/wp-content/plugins/instagram-feed/js/sbi-scripts.min.js (ve
↪r [6.9.0])
https://ipwija.ac.id/wp-content/plugins/interactive-3d-flipbook-powered-physics-
↪engine/assets/js/client-locale-loader.js (ver [1.16.15])
https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/css/pum-site.min.css

... continues on next page ...

... continued from previous page ...

```
↪(ver [1.20.3] )
https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/js/site.min.js (defer
↪ [] ver [1.20.3] )
https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/js/vendor/mobile-dete
↪ct.min.js (ver [1.3.3] )
https://ipwija.ac.id/wp-content/plugins/revslider/public/css/sr7.css (ver [6.7.2
↪3] )
https://ipwija.ac.id/wp-content/plugins/revslider/public/js/libs/tptools.js (ver
↪ [6.7.23] )
https://ipwija.ac.id/wp-content/plugins/revslider/public/js/sr7.js (ver [6.7.23]
↪ )
https://ipwija.ac.id/wp-content/plugins/say-what/assets/build/frontend.js (ver [
↪fd31684c45e4d85aeb4e] )
https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/frontend.css (v
↪er [1.3.2] )
https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/frontend.js (ve
↪r [1.3.2] )
https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/libraries/thim-
↪ekits/css/thim-ekits-icons.min.css (ver [1.3.2] )
https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/widgets.css (ve
↪r [1.3.2] )
https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/widgets.js (ver
↪ [c13831a42f8b44b55a13] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/assets//css/frontend/e
↪vents.min.css (ver [2.1.8] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/assets//js/frontend/ev
↪ents.min.js (ver [6.8.1] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//countdo
↪wn/css/jquery.countdown.css (ver [2.1.8] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//countdo
↪wn/js/jquery.countdown.min.js (ver [6.8.1] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//countdo
↪wn/js/jquery.plugin.min.js (ver [6.8.1] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//magnifi
↪c-popup/css/magnific-popup.css (ver [2.1.8] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//magnifi
↪c-popup/js/jquery.magnific-popup.min.js (ver [2.1.8] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//owl-car
↪ousel/css/owl.carousel.css (ver [2.1.8] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//owl-car
↪ousel/js/owl.carousel.min.js (ver [6.8.1] )
https://ipwija.ac.id/wp-content/plugins/wp-stats-manager/css/style.css (ver [1.2
↪] )
https://ipwija.ac.id/wp-content/themes/eduma/assets/css/v4-shims.min.css (ver [5
↪.6.6] )
https://ipwija.ac.id/wp-content/themes/eduma/assets/js/jquery.countTo.min.js (ve
↪r [5.6.6] )
```

... continues on next page ...

... continued from previous page ...

https://ipwija.ac.id/wp-content/themes/eduma/assets/js/jquery.waypoints.min.js (ver [5.6.6])
https://ipwija.ac.id/wp-content/themes/eduma/assets/js/main.min.js (ver [5.6.6])
https://ipwija.ac.id/wp-content/themes/eduma/assets/js/thim-scripts.min.js (ver [5.6.6])
https://ipwija.ac.id/wp-content/themes/eduma/style.css (ver [5.6.6])
https://ipwija.ac.id/wp-includes/css/dist/block-library/style.min.css (ver [6.8.1])
https://ipwija.ac.id/wp-includes/js/backbone.min.js (ver [1.6.0])
https://ipwija.ac.id/wp-includes/js/dist/api-fetch.min.js (ver [3623a576c78df404ff20])
https://ipwija.ac.id/wp-includes/js/dist/hooks.min.js (ver [4d63a3d491d11ffd8ac6])
https://ipwija.ac.id/wp-includes/js/dist/i18n.min.js (ver [5e580eb46a90c2b997e6])
https://ipwija.ac.id/wp-includes/js/dist/url.min.js (ver [6bf93e90403a1eec6501])
https://ipwija.ac.id/wp-includes/js/dist/vendor/wp-polyfill.min.js (ver [3.15.0])
https://ipwija.ac.id/wp-includes/js/imagesloaded.min.js (ver [5.0.0])
https://ipwija.ac.id/wp-includes/js/jquery/jquery-migrate.min.js (ver [3.4.1])
https://ipwija.ac.id/wp-includes/js/jquery/jquery.min.js (ver [3.7.1])
https://ipwija.ac.id/wp-includes/js/jquery/ui/core.min.js (ver [1.13.3])
https://ipwija.ac.id/wp-includes/js/masonry.min.js (ver [4.2.2])
https://ipwija.ac.id/wp-includes/js/underscore.min.js (ver [1.13.7])
https://ipwija.ac.id/wp-includes/js/wp-util.min.js (ver [6.8.1])

Solution:

Log Method
Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2025-10-10T05:39:02Z

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

[return to 77.37.76.204]

2.2 147.79.120.130

Host scan start	Tue Nov 18 01:37:38 2025 UTC
Host scan end	Tue Nov 18 03:04:04 2025 UTC

Service (Port)	Threat Level
general/tcp	Low
general/CPE-T	Log
general/tcp	Log
443/tcp	Log
80/tcp	Log

2.2.1 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.

Quality of Detection (QoD): 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: 4099560098
Packet 2: 3907143693
```

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.

... continues on next page ...

... continued from previous page ...

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 147.79.120.130]

2.2.2 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 (QoD): 80%

Vulnerability Detection Result
147.79.120.130|cpe:/a:php:php:8.2.28
147.79.120.130|cpe:/o:linux:kernel

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 147.79.120.130]

2.2.3 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 (QoD): 80%

Vulnerability Detection Result
```
Hostname determination for IP 147.79.120.130:
Hostname|Source
ipwija.ac.id|Forward-DNS
```

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: 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 (QoD): 80%

Vulnerability Detection Result
```
Best matching OS:
OS:           Linux Kernel
CPE:          cpe:/o:linux:kernel
Found by VT:  1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICM
↪P))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

Solution:

. . . continues on next page . . .

... continued from previous page ...

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2025-11-14T15:41:06Z

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

Log (CVSS: 0.0)
NVT: PHP Detection Consolidation

Summary
Consolidation of PHP detections.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Detected PHP
Version:       8.2.28
Location:      443/tcp
CPE:           cpe:/a:php:php:8.2.28
Concluded from version/product identification result:
X-Powered-By: PHP/8.2.28
Concluded from version/product identification location:
https://ipwija.ac.id/
```

Solution:

Log Method
Details: PHP Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.171722
Version used: 2025-09-24T05:39:03Z

References
url: https://www.php.net/

Log (CVSS: 0.0)
NVT: Traceroute

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

... continues on next page ...

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Network route from scanner (172.18.0.5) to target (147.79.120.130):
172.18.0.5
10.206.6.215
10.206.35.36
10.206.32.2
173.255.239.102
23.203.154.42
62.115.139.35
62.115.138.71
62.115.137.55
62.115.137.45
62.115.136.119
62.115.138.64
62.115.125.55
62.115.33.63
148.51.252.130
148.51.251.151
38.104.17.154
153.92.2.194
153.92.2.53
147.79.120.130
Network distance between scanner and target: 20
```

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: 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)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)

... continues on next page ...

... continued from previous page ...

- 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 (QoD): 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: hcdn
Identified from: HTTP Server banner on port 443/tcp
Banner: Server: hcdn
Identified from: HTTP Server banner on port 80/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

[return to 147.79.120.130]

2.2.4 Log 443/tcp

Log (CVSS: 0.0)
NVT: Allowed HTTP Methods Enumeration

Summary
Enumerates which HTTP methods are allowed.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The following list contains the URLs and corresponding supported HTTP methods.
URL                   | HTTP Methods
-------------------------------------
https://ipwija.ac.id/ | GET,OPTIONS
```

... continues on next page ...

... continued from previous page ...

Solution:

Vulnerability Insight
- Basic HTTP methods: GET, HEAD, POST, PUT, DELETE, CONNECT, OPTIONS, TRACE
- Extended HTTP methods: ACL, BASELINE-CONTROL, BIND, CHECKIN, CHECKOUT, COPY, LABEL, LINK, LOCK, MERGE, MKACTIVITY, MKCALENDAR, MKCOL, MKREDIRECTREF, MKWORKSPACE, MOVE, ORDERPATCH, PATCH, PRI, PROPFIND, PROPPATCH, REBIND, REPORT, SEARCH, UNBIND, UNCHECKOUT, UNLINK, UNLOCK, UPDATE, UPDATEREDIRECTREF, VERSION-CONTROL

Log Method
Sends multiple HTTP requests and checks the responses.
Disclaimer:
- This enumeration script is provided 'as is' (means no support is given) and only providing rudimentary information about the possible enabled methods
- This script doesn't guarantee completeness or full reliability
For more reliable determination of the enabled HTTP methods please inspect the configuration of the web server manually and directly on the target host.
Details: `Allowed HTTP Methods Enumeration`
OID:1.3.6.1.4.1.25623.1.0.153974
Version used: `2025-02-28T05:38:49Z`

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 (QoD): 80%

Vulnerability Detection Result
```
Header Name             | Header Value
------------------------------------------------
Content-Security-Policy | upgrade-insecure-requests
Missing Headers                   | More Information
-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪----------
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: 2025-03-21T15:40:43Z

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 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 (QoD): 80%

Vulnerability Detection Result
It was possible to enumerate the following HTTP server banner(s):
Server banner | Enumeration technique

Server: hcdn | 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: 2025-01-31T15:39:24Z

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 (QoD): 80%

Vulnerability Detection Result
The remote HTTP Server banner is:
Server: hcdn

Solution:

... continues on next page ...

. . . continued from previous page . . .

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 (QoD): 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.

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2025-03-05T05:38:53Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

Quality of Detection (QoD): 80%

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

Solution:

. . . continues on next page . . .

... continued from previous page ...

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: `2025-03-05T05:38:53Z`

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 (QoD): 80%

Vulnerability Detection Result
```
The Hostname/IP "ipwija.ac.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 23.8.5)" 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://ipwija.ac.id/
https://ipwija.ac.id/about
https://ipwija.ac.id/account
```

... continues on next page ...

... continued from previous page ...

```
https://ipwija.ac.id/community
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
The following directories were excluded from web application scanning because th
↪e "Regex pattern to exclude directories from CGI scanning" setting of the VT "
↪Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was
↪: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graph
↪ic|grafik|picture|bilder|thumbnail|media/|skins?/)"
https://ipwija.ac.id/wp-content/plugins/chaty/admin/assets/js
https://ipwija.ac.id/wp-content/plugins/chaty/css
https://ipwija.ac.id/wp-content/plugins/chaty/js
https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/css
https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/js
https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/swv/js
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals
https://ipwija.ac.id/wp-content/plugins/elementor/assets/images
https://ipwija.ac.id/wp-content/plugins/elementor/assets/js
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/animations/styles
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/font-awesome/css
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/swiper/v8/css
https://ipwija.ac.id/wp-content/plugins/feeds-for-tiktok/vendor/smashballoon/cus
↪tomizer/sb-common/sb-customizer/build/static/css
https://ipwija.ac.id/wp-content/plugins/feeds-for-tiktok/vendor/smashballoon/cus
↪tomizer/sb-common/sb-customizer/build/static/js
https://ipwija.ac.id/wp-content/plugins/h5p/h5p-php-library/styles
https://ipwija.ac.id/wp-content/plugins/insta-gallery/build/frontend/css
https://ipwija.ac.id/wp-content/plugins/instagram-feed/css
https://ipwija.ac.id/wp-content/plugins/instagram-feed/img
https://ipwija.ac.id/wp-content/plugins/instagram-feed/js
https://ipwija.ac.id/wp-content/plugins/interactive-3d-flipbook-powered-physics-
↪engine/assets/js
https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/css
https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/js
https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/js/vendor
https://ipwija.ac.id/wp-content/plugins/revslider/public/css
https://ipwija.ac.id/wp-content/plugins/revslider/public/js
https://ipwija.ac.id/wp-content/plugins/revslider/public/js/libs
https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/libraries/thim-
↪ekits/css
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/assets//css/frontend
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/assets//js/frontend
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//countdo
↪wn/css
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//countdo
↪wn/js
```

... continues on next page ...

... continued from previous page ...

```
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//magnifi
↪c-popup/css
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//magnifi
↪c-popup/js
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//owl-car
↪ousel/css
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//owl-car
↪ousel/js
https://ipwija.ac.id/wp-content/plugins/wp-stats-manager/css
https://ipwija.ac.id/wp-content/themes/eduma
https://ipwija.ac.id/wp-content/themes/eduma/assets/css
https://ipwija.ac.id/wp-content/themes/eduma/assets/js
https://ipwija.ac.id/wp-includes/css/dist/block-library
https://ipwija.ac.id/wp-includes/js
https://ipwija.ac.id/wp-includes/js/dist
https://ipwija.ac.id/wp-includes/js/dist/vendor
https://ipwija.ac.id/wp-includes/js/jquery
https://ipwija.ac.id/wp-includes/js/jquery/ui
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
https://ipwija.ac.id/ (p [19775] )
https://ipwija.ac.id/\ (page [wsm_traffic] subPage [UsersOnline] subTab [summary
↪\] )
https://ipwija.ac.id/aktivitas/\ (page [wsm_traffic] subPage [UsersOnline] subTa
↪b [summary\] )
https://ipwija.ac.id/alumni-2/\ (page [wsm_traffic] subPage [UsersOnline] subTab
↪ [summary\] )
https://ipwija.ac.id/arsip/\ (page [wsm_traffic] subPage [UsersOnline] subTab [s
↪ummary\] )
https://ipwija.ac.id/biaya-kuliah-universitas-ipwija/\ (page [wsm_traffic] subPa
↪ge [UsersOnline] subTab [summary\] )
https://ipwija.ac.id/events/\ (page [wsm_traffic] subPage [UsersOnline] subTab [
↪summary\] )
https://ipwija.ac.id/fasilitas/\ (page [wsm_traffic] subPage [UsersOnline] subTa
↪b [summary\] )
https://ipwija.ac.id/hubungi-kami/\ (page [wsm_traffic] subPage [UsersOnline] su
↪bTab [summary\] )
https://ipwija.ac.id/informasi-beasiswa/\ (page [wsm_traffic] subPage [UsersOnli
↪ne] subTab [summary\] )
https://ipwija.ac.id/informasi-tes-seleksi/\ (page [wsm_traffic] subPage [UsersO
↪nline] subTab [summary\] )
https://ipwija.ac.id/kabar-terbaru/\ (page [wsm_traffic] subPage [UsersOnline] s
↪ubTab [summary\] )
https://ipwija.ac.id/kebijakan-dan-pengumuman/\ (page [wsm_traffic] subPage [Use
↪rsOnline] subTab [summary\] )
https://ipwija.ac.id/kemahasiswaan/\ (page [wsm_traffic] subPage [UsersOnline] s
↪ubTab [summary\] )
```

... continues on next page ...

... continued from previous page ...

```
https://ipwija.ac.id/keseharian-di-kampus/\ (page [wsm_traffic] subPage [UsersOn
↪line] subTab [summary\] )
https://ipwija.ac.id/klinik/\ (page [wsm_traffic] subPage [UsersOnline] subTab [
↪summary\] )
https://ipwija.ac.id/magister-manajemen/\ (page [wsm_traffic] subPage [UsersOnli
↪ne] subTab [summary\] )
https://ipwija.ac.id/marina-goes-to-school-campus-di-universitas-ipwija-no-limit
↪-under-the-sun/\ (page [wsm_traffic] subPage [UsersOnline] subTab [summary\] )
https://ipwija.ac.id/mengapa-ipwija/\ (page [wsm_traffic] subPage [UsersOnline]
↪subTab [summary\] )
https://ipwija.ac.id/pendaftaran/\ (page [wsm_traffic] subPage [UsersOnline] sub
↪Tab [summary\] )
https://ipwija.ac.id/pengumuman-penerimaan/\ (page [wsm_traffic] subPage [UsersO
↪nline] subTab [summary\] )
https://ipwija.ac.id/perpustakaan/\ (page [wsm_traffic] subPage [UsersOnline] su
↪bTab [summary\] )
https://ipwija.ac.id/program-studi-informatika/\ (page [wsm_traffic] subPage [Us
↪ersOnline] subTab [summary\] )
https://ipwija.ac.id/program-studi-kebidanan/\ (page [wsm_traffic] subPage [User
↪sOnline] subTab [summary\] )
https://ipwija.ac.id/program-studi-kewirausahaan/\ (page [wsm_traffic] subPage [
↪UsersOnline] subTab [summary\] )
https://ipwija.ac.id/program-studi-rekayasa-perangkat-lunak/\ (page [wsm_traffic
↪] subPage [UsersOnline] subTab [summary\] )
https://ipwija.ac.id/program-studi-sarajana-manajemen/\ (page [wsm_traffic] subP
↪age [UsersOnline] subTab [summary\] )
https://ipwija.ac.id/program-studi-sistem-informasi/\ (page [wsm_traffic] subPag
↪e [UsersOnline] subTab [summary\] )
https://ipwija.ac.id/pusat-karir/\ (page [wsm_traffic] subPage [UsersOnline] sub
↪Tab [summary\] )
https://ipwija.ac.id/pusat-konseling/\ (page [wsm_traffic] subPage [UsersOnline]
↪ subTab [summary\] )
https://ipwija.ac.id/pusat-teknologi-informasi/\ (page [wsm_traffic] subPage [Us
↪ersOnline] subTab [summary\] )
https://ipwija.ac.id/sekilas-ipwija/\ (page [wsm_traffic] subPage [UsersOnline]
↪subTab [summary\] )
https://ipwija.ac.id/simulasi-rapor/\ (page [wsm_traffic] subPage [UsersOnline]
↪subTab [summary\] )
https://ipwija.ac.id/sorotan/\ (page [wsm_traffic] subPage [UsersOnline] subTab
↪[summary\] )
https://ipwija.ac.id/sosialisasi-p2mw-2025-di-universitas-ipwija-mahasiswa-didor
↪ong-jadi-wirausahawan-muda/\ (page [wsm_traffic] subPage [UsersOnline] subTab
↪[summary\] )
https://ipwija.ac.id/tanggal-penting/\ (page [wsm_traffic] subPage [UsersOnline]
↪ subTab [summary\] )
https://ipwija.ac.id/tentang-universitas-ipwija/\ (page [wsm_traffic] subPage [U
↪sersOnline] subTab [summary\] )
```

... continues on next page ...

... continued from previous page ...

```
https://ipwija.ac.id/video/\ (page [wsm_traffic] subPage [UsersOnline] subTab [s
↪ummary\] )
https://ipwija.ac.id/wp-json/oembed/1.0/embed (#038;format [xml] url [https%3A%2
↪F%2Fipwija.ac.id%2F] )
https://ipwija.ac.id/xmlrpc.php (rsd [] )
The following cgi scripts were excluded from web application scanning because of
↪ the "Regex pattern to exclude cgi scripts" setting of the VT "Web mirroring"
↪(OID: 1.3.6.1.4.1.25623.1.0.10662) for this scan was: "\.(js|css)$"
Syntax : cginame (arguments [default value])
https://ipwija.ac.id/wp-content/plugins/chaty/admin/assets/js/picmo-latest-umd.m
↪in.js (ver [3.4.1] )
https://ipwija.ac.id/wp-content/plugins/chaty/admin/assets/js/picmo-umd.min.js (
↪ver [3.4.1] )
https://ipwija.ac.id/wp-content/plugins/chaty/css/chaty-front.min.css (ver [3.4.
↪11742195845] )
https://ipwija.ac.id/wp-content/plugins/chaty/js/cht-front-script.min.js (ver [3
↪.4.11742195845] )
https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/css/styles.css (
↪ver [6.0.6] )
https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/js/index.js (ver
↪ [6.0.6] )
https://ipwija.ac.id/wp-content/plugins/contact-form-7/includes/swv/js/index.js
↪(ver [6.0.6] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals/apple-
↪webkit.min.css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals/e-swip
↪er.min.css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/conditionals/shapes
↪.min.css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/frontend.min.css (v
↪er [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-divider.min.
↪css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-google_maps.
↪min.css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-heading.min.
↪css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-icon-box.min
↪.css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-image.min.cs
↪s (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-nested-tabs.
↪min.css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-social-icons
↪.min.css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-spacer.min.c
↪ss (ver [3.28.4] )
```

... continues on next page ...

... continued from previous page ...

```
https://ipwija.ac.id/wp-content/plugins/elementor/assets/css/widget-video.min.cs
↪s (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/js/frontend-modules.min
↪.js (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/js/frontend.min.js (ver
↪ [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/js/webpack.runtime.min.
↪js (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/animations/styles/e
↪-animation-pulse.min.css (ver [3.28.4] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/font-awesome/css/al
↪l.css (ver [1.3.2] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/swiper/v8/css/swipe
↪r.min.css (ver [8.4.5] )
https://ipwija.ac.id/wp-content/plugins/elementor/assets/lib/swiper/v8/swiper.mi
↪n.js (ver [8.4.5] )
https://ipwija.ac.id/wp-content/plugins/feeds-for-tiktok/vendor/smashballoon/cus
↪tomizer/sb-common/sb-customizer/build/static/css/tikTokFeed.css (ver [6.8.1] )
https://ipwija.ac.id/wp-content/plugins/feeds-for-tiktok/vendor/smashballoon/cus
↪tomizer/sb-common/sb-customizer/build/static/js/tikTokFeed.js (ver [1.1.1] )
https://ipwija.ac.id/wp-content/plugins/h5p/h5p-php-library/styles/h5p.css (ver
↪[1.16.0] )
https://ipwija.ac.id/wp-content/plugins/insta-gallery/assets/frontend/swiper/swi
↪per.min.css (ver [4.6.1] )
https://ipwija.ac.id/wp-content/plugins/insta-gallery/assets/frontend/swiper/swi
↪per.min.js (ver [4.6.1] )
https://ipwija.ac.id/wp-content/plugins/insta-gallery/build/frontend/css/style.c
↪ss (ver [4.6.1] )
https://ipwija.ac.id/wp-content/plugins/instagram-feed/css/sbi-styles.min.css (v
↪er [6.9.0] )
https://ipwija.ac.id/wp-content/plugins/instagram-feed/js/sbi-scripts.min.js (ve
↪r [6.9.0] )
https://ipwija.ac.id/wp-content/plugins/interactive-3d-flipbook-powered-physics-
↪engine/assets/js/client-locale-loader.js (ver [1.16.15] )
https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/css/pum-site.min.css
↪(ver [1.20.3] )
https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/js/site.min.js (defer
↪ [] ver [1.20.3] )
https://ipwija.ac.id/wp-content/plugins/popup-maker/assets/js/vendor/mobile-dete
↪ct.min.js (ver [1.3.3] )
https://ipwija.ac.id/wp-content/plugins/revslider/public/css/sr7.css (ver [6.7.2
↪3] )
https://ipwija.ac.id/wp-content/plugins/revslider/public/js/libs/tptools.js (ver
↪ [6.7.23] )
https://ipwija.ac.id/wp-content/plugins/revslider/public/js/sr7.js (ver [6.7.23]
↪ )
https://ipwija.ac.id/wp-content/plugins/say-what/assets/build/frontend.js (ver [
```

... continues on next page ...

... continued from previous page ...

```
↪fd31684c45e4d85aeb4e] )
https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/frontend.css (v
↪er [1.3.2] )
https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/frontend.js (ve
↪r [1.3.2] )
https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/libraries/thim-
↪ekits/css/thim-ekits-icons.min.css (ver [1.3.2] )
https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/widgets.css (ve
↪r [1.3.2] )
https://ipwija.ac.id/wp-content/plugins/thim-elementor-kit/build/widgets.js (ver
↪ [c13831a42f8b44b55a13] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/assets//css/frontend/e
↪vents.min.css (ver [2.1.8] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/assets//js/frontend/ev
↪ents.min.js (ver [6.8.1] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//countdo
↪wn/css/jquery.countdown.css (ver [2.1.8] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//countdo
↪wn/js/jquery.countdown.min.js (ver [6.8.1] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//countdo
↪wn/js/jquery.plugin.min.js (ver [6.8.1] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//magnifi
↪c-popup/css/magnific-popup.css (ver [2.1.8] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//magnifi
↪c-popup/js/jquery.magnific-popup.min.js (ver [2.1.8] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//owl-car
↪ousel/css/owl.carousel.css (ver [2.1.8] )
https://ipwija.ac.id/wp-content/plugins/wp-events-manager/inc/libraries//owl-car
↪ousel/js/owl.carousel.min.js (ver [6.8.1] )
https://ipwija.ac.id/wp-content/plugins/wp-stats-manager/css/style.css (ver [1.2
↪] )
https://ipwija.ac.id/wp-content/themes/eduma/assets/css/v4-shims.min.css (ver [5
↪.6.6] )
https://ipwija.ac.id/wp-content/themes/eduma/assets/js/jquery.countTo.min.js (ve
↪r [5.6.6] )
https://ipwija.ac.id/wp-content/themes/eduma/assets/js/jquery.waypoints.min.js (
↪ver [5.6.6] )
https://ipwija.ac.id/wp-content/themes/eduma/assets/js/main.min.js (ver [5.6.6]
↪)
https://ipwija.ac.id/wp-content/themes/eduma/assets/js/thim-scripts.min.js (ver
↪[5.6.6] )
https://ipwija.ac.id/wp-content/themes/eduma/style.css (ver [5.6.6] )
https://ipwija.ac.id/wp-includes/css/dist/block-library/style.min.css (ver [6.8.
↪1] )
https://ipwija.ac.id/wp-includes/js/backbone.min.js (ver [1.6.0] )
https://ipwija.ac.id/wp-includes/js/dist/api-fetch.min.js (ver [3623a576c78df404
↪ff20] )
```

... continues on next page ...

... continued from previous page ...

```
https://ipwija.ac.id/wp-includes/js/dist/hooks.min.js (ver [4d63a3d491d11ffd8ac6
↪] )
https://ipwija.ac.id/wp-includes/js/dist/i18n.min.js (ver [5e580eb46a90c2b997e6]
↪ )
https://ipwija.ac.id/wp-includes/js/dist/url.min.js (ver [6bf93e90403a1eec6501]
↪)
https://ipwija.ac.id/wp-includes/js/dist/vendor/wp-polyfill.min.js (ver [3.15.0]
↪ )
https://ipwija.ac.id/wp-includes/js/imagesloaded.min.js (ver [5.0.0] )
https://ipwija.ac.id/wp-includes/js/jquery/jquery-migrate.min.js (ver [3.4.1] )
https://ipwija.ac.id/wp-includes/js/jquery/jquery.min.js (ver [3.7.1] )
https://ipwija.ac.id/wp-includes/js/jquery/ui/core.min.js (ver [1.13.3] )
https://ipwija.ac.id/wp-includes/js/masonry.min.js (ver [4.2.2] )
https://ipwija.ac.id/wp-includes/js/underscore.min.js (ver [1.13.7] )
https://ipwija.ac.id/wp-includes/js/wp-util.min.js (ver [6.8.1] )
```

Solution:

Log Method
Details: Web Application Scanning Consolidation / Info Reporting
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2025-10-10T05:39:02Z

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

[return to 147.79.120.130]

2.2.5 Log 80/tcp

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 (QoD): 80%

Vulnerability Detection Result

```
Header Name              | Header Value
-------------------------------------------------
Content-Security-Policy | upgrade-insecure-requests
Missing Headers                    | More Information
```

... continues on next page ...

... continued from previous page ...

```
------------------------------------------------------------------------------
↪------------------------------------------------------------------------------
↪-----------------------------------------------
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
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: 2025-03-21T15:40:43Z

... 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 (QoD): 80%

Vulnerability Detection Result
```
It was possible to enumerate the following HTTP server banner(s):
Server banner | Enumeration technique
--------------------------------------------------------------------------------
Server: hcdn  | 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: 2025-01-31T15:39:24Z

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 (QoD): 80%

Vulnerability Detection Result
```
The remote HTTP Server banner is:
Server: hcdn
```

Solution:

... continues on next page ...

. . . continued from previous page . . .

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: Response Time / No 404 Error Code Check

Summary
This VT tests if the remote web server does not reply with a 404 error code and checks if it is replying to the scanners requests in a reasonable amount of time.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The host returns a 30x (e.g. 301) error code when a non-existent file is request ↪ed. Some HTTP-related checks have been disabled.`

Solution:

Vulnerability Insight
This web server might show the following issues:
- it is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page, authentication page or redirect instead.
The Scanner might enabled some counter measures for that, however they might be insufficient. If a great number of security issues are reported for this port, they might not all be accurate.
- it doesn't response in a reasonable amount of time to various HTTP requests sent by this VT. In order to keep the scan total time to a reasonable amount, the remote web server might not be tested. If the remote server should be tested it has to be fixed to have it reply to the scanners requests in a reasonable amount of time.
Alternatively the 'Maximum response time (in seconds)' preference could be raised to a higher value if longer scan times are accepted.

Log Method
Details: `Response Time / No 404 Error Code Check`
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: `2025-04-11T15:45:04Z`

Log (CVSS: 0.0)
NVT: Services

Summary
This plugin performs service detection.

. . . continues on next page . . .

... continued from previous page ...

Quality of Detection (QoD): 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: `2025-03-05T05:38:53Z`

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 (QoD): 80%

Vulnerability Detection Result

```
The Hostname/IP "ipwija.ac.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 23.8.5)" was used to access
```

... continues on next page ...

... continued from previous page ...

```
↪ 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://ipwija.ac.id/
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: `2025-10-10T05:39:02Z`

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

[return to 147.79.120.130]

2.3 2a02:4780:50:ab0f:28c0:13ac:4306:882b

Host scan start	Tue Nov 18 01:37:38 2025 UTC
Host scan end	Tue Nov 18 01:42:57 2025 UTC

Service (Port)	Threat Level
general/tcp	Log

2.3.1 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 (QoD): 80%

Vulnerability Detection Result
`Hostname determination for IP 2a02:4780:50:ab0f:28c0:13ac:4306:882b:`
`Hostname|Source`

... continues on next page ...

... continued from previous page ...

ipwija.ac.id|Forward-DNS

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: 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 (QoD): 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: 2025-11-14T15:41:06Z

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

[return to 2a02:4780:50:ab0f:28c0:13ac:4306:882b]

2.4 2a02:4780:4e:fa98:35c9:8f37:d5f6:6960

Host scan start	Tue Nov 18 01:37:38 2025 UTC
Host scan end	Tue Nov 18 01:42:52 2025 UTC

Service (Port)	Threat Level
general/tcp	Log

2.4.1 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 (QoD): 80%

Vulnerability Detection Result
```
Hostname determination for IP 2a02:4780:4e:fa98:35c9:8f37:d5f6:6960:
Hostname|Source
ipwija.ac.id|Forward-DNS
```

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: 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 (QoD): 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:

. . . continues on next page . . .

... continued from previous page ...

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2025-11-14T15:41:06Z

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

[return to 2a02:4780:4e:fa98:35c9:8f37:d5f6:6960]

This file was automatically generated.