Scan Report

October 8, 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 "Unnamed". The scan started at Wed Oct 8 05:47:13 2025 UTC and ended at Wed Oct 8 05:59:46 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
127.8.0.1 dvwa	1	3	0	0	0
Total: 1	1	3	0	0	0

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

This report contains all 4 results selected by the filtering described above. Before filtering there were 54 results.

2 Results per Host

2.1 127.8.0.1

Host scan start	Wed Oct 8 05:48:13 2025 UTC
Host scan end	Wed Oct 8 05:59:39 2025 UTC

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

2.1.1 High general/tcp

High (CVSS: 10.0)

NVT: Operating System (OS) End of Life (EOL) Detection

Product detection result

```
cpe:/o:debian:debian_linux:9
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)
```

... continues on next page ...

... continued from previous page ...

Summary
The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The "Debian GNU/Linux" Operating System on the remote host has reached the end o
↪f life.
CPE:                cpe:/o:debian:debian_linux:9
Installed version,
build or SP:        9
EOL date:           2022-06-30
EOL info:           https://en.wikipedia.org/wiki/List_of_Debian_releases#Release
↪_table
```

Impact
An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:
Solution type: Mitigation
Update the OS on the remote host to a version which is still supported and receiving security updates by the vendor.
Note / Important: Please create an override for this result if the target host is a:
- Windows system with Extended Security Updates (ESU)
- System with additional 3rd-party / non-vendor security updates like e.g. from 'TuxCare', 'Freexian Extended LTS' or similar

Vulnerability Detection Method
Checks if an EOL version of an OS is present on the target host.
Details: `Operating System (OS) End of Life (EOL) Detection`
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: `2025-05-21T05:40:19Z`

Product Detection Result
Product: `cpe:/o:debian:debian_linux:9`
Method: `OS Detection Consolidation and Reporting`
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 127.8.0.1]

2.1.2 Medium 80/tcp

Medium (CVSS: 5.0)

NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

Summary
The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
The cookie(s):
Set-Cookie: PHPSESSID=***replaced***; path=/
Set-Cookie: PHPSESSID=***replaced***; path=/
Set-Cookie: security=low
is/are missing the "HttpOnly" cookie attribute.
```

Solution:
Solution type: Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

Affected Software/OS
Any web application with session handling in cookies.

Vulnerability Insight
The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute.
This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method
Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute.
Details: `Missing 'HttpOnly' Cookie Attribute (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `2024-01-12T16:12:12Z`

References
```
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6
url: https://owasp.org/www-community/HttpOnly
url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0
↪02)
```

Medium (CVSS: 5.0)

NVT: Backup File Scanner (HTTP) - Reliable Detection Reporting

Summary
The script reports backup files left on the web server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The following backup files were identified (<URL>:<Matching pattern>):`
`http://dvwa/config/config.inc.php.bak:^<\?(php|=)`

Impact
Based on the information provided in these files an attacker might be able to gather sensitive information stored in these files.

Solution:
Solution type: Mitigation
Delete the backup files.

Vulnerability Insight
Notes:
- 'Reliable Detection' means that a file was detected based on a strict (regex) and reliable pattern matching the response of the remote web server when a file was requested.
- As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method
Reports previous enumerated backup files accessible on the remote web server.
Details: `Backup File Scanner (HTTP) - Reliable Detection Reporting`
OID:1.3.6.1.4.1.25623.1.0.108976
Version used: `2022-09-13T10:15:09Z`

References
`url: http://www.openwall.com/lists/oss-security/2017/10/31/1`

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

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

. . . continues on next page . . .

... continued from previous page ...

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The following input fields were identified (URL:input name):`
`http://dvwa/login.php:password`

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

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

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

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

References
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[return to 127.8.0.1]