
EH - TASK 2

Vulnerabilities-Netsparker

Step 1: open netsparker

Step 2: Add Website “<http://zero.webappsecurity.com/>” to the dialogue box.

Step 3: Then click on start scan ,then it will start scanning it automatically

Step 4: Choose any one of the Critical Vulnerabilities.

SCREENSHOTS OF THE PROCESS:

The screenshot displays the Burp Suite application window. The top menu bar includes File, View, Reporting, Tools, and Help. The main toolbar contains buttons for Start New Scan, Start Incremental Scan, Pause, Skip Current Phase, Import Links, and Start Proxy.

Site Map: A tree view on the left shows the site structure, including links like forgotten-password-send.html, index.old, [Possible] Backup File Disclosure, faq.html.bak, Knowledge Base, Scan Performance, Out of Scope Links, Crawling Performance, MIME Types, Comments, Slowest Pages, File Extensions, JavaScript Files, Email Addresses, CSS Files, and Web Pages With Inputs.

Dashboard: The top section shows the target URL **zero.webappsecurity.com**. It includes a progress bar for 'Crawling & Attacking (2/3)...' at 37% and a status '2167 / 5724'. Below this, 'Scan Information' is provided:

- Current Speed: 3.0 req/sec
- Average Speed: 2.0 req/sec
- Total Requests: 2878
- Failed Requests: 0
- HEAD Requests: 527
- Elapsed Time: 00:23:52

Issues (35): A list of identified vulnerabilities is shown, including:

- Out-of-date Version (Apache)
- Out-of-date Version (OpenSSL)
- Out-of-date Version (Tomcat)
- Insecure Transportation Security Protocol Supported (SSLv2)
- Password Transmitted over HTTP
- [Possible] Expression Language Injection
- Insecure Transportation Security Protocol Supported (SSLv3)
- Weak Ciphers Enabled
- Out-of-date Version (jQuery)
- Out-of-date Version (jQuery UI Dialog)
- Apache Server-Status Detected
- Insecure Transportation Security Protocol Supported (TLS 1.0)
- Version Disclosure (Apache Module)

Activity (15): A table of network activity is displayed:

Method	URL	Time	Status	Response	Details
GET	http://zero.webappsecurity.com/bank/	129 s	[11/29] Open ...	[1/18] With HTTP - R...	Waiting...
GET	http://zero.webappsecurity.com/bank/account-su...	19 s	[11/29] Open ...	[1/18] With HTTP - R...	Waiting...
GET	http://zero.webappsecurity.com/bank/account-su...	1 s	[29/29] Code ...	[7/44] (PHP) PCRE 'e...	Analyzing...
GET	http://zero.webappsecurity.com/bootstrap-tooltip.js	933 s	[11/29] Open ...	[1/18] With HTTP - R...	Parsing...
GET	http://zero.webappsecurity.com/cgi-bin/	204 s	[11/29] Open ...	[1/18] With HTTP - R...	Waiting...
GET	http://zero.webappsecurity.com/faq.html	188 s	[11/29] Open ...	[1/18] With HTTP - R...	Waiting...
GET	http://zero.webappsecurity.com/feedback.html	179 s	[11/29] Open ...	[1/18] With HTTP - R...	Waiting...

The bottom status bar indicates 'Auto save finished successfully - 11-08-2021 22:12:21' and 'No vulnerability database updates found.' The system tray shows the date and time as 22:13 on 11-08-2021.

FileViewReportingToolsHelp

Start New ScanStart Incremental ScanPauseSkip Current PhaseImport LinksStart Proxy

Site Map

forgotten-password-send.htmlindex.old[Possible] Backup File Disclosurefaq.html.bakKnowledge BaseScan PerformanceOut of Scope LinksCrawling PerformanceMIME TypesCommentsSlowest PagesFile ExtensionsJavaScript Files

Issues (35)

Group Issues by

Vulnerability TypeSeverityConfirmationURL

Issue...Enc...Log...

Current speed: 3.5 req/secAverage Speed: 2.7 req/secTotal Requests: 8887Failed Requests: 0HEAD Requests: 573Elapsed Time: 00:55:23

VulnerabilityBrowser ViewHTTP Request / Response

Controlled ScanRetestSend to Request BuilderGenerate WAF RulesExecute SQL CommandsGet ShellLFI ExploitationGenerate ExploitShort Names

Out-of-date Version (Apache)

CERTAINTY

URL

IDENTIFIED VERSION

LATEST VERSION

VULNERABILITY DATABASE

https://zero.webappsecurity.com/

2.2.6 (contains 4 critical and 65 other vulnerabilities)

2.4.48

Result is based on 30-07-2021 vulnerability database content.

CLASSIFICATION

PCI 3.1

PCI 3.2

OWASP 2013

CAPEC

6.2

6.2

A9

310

Vulnerability Details

Netsparker identified you are using an out-of-date version of Apache.

IMPACT

Since this is an old version of the software, it may be vulnerable to attacks.

REMEDY

Please upgrade your installation of Apache to the latest stable version.

REMEDY REFERENCES

Downloading the Apache HTTP Server

KNOWN VULNERABILITIES IN THIS VERSION

VulnerabilityScanRequest Builder

Auto save finished successfully - 11-08-2021 22:42:21

33511

No vulnerability database updates found.

Proxy: System

FileViewReportingToolsHelp

Start New ScanStart Incremental ScanPauseSkip Current PhaseImport LinksStart Proxy

Site Map

forgotten-password-send.html

index.old

[Possible] Backup File Disclosure

faq.html.bak

Knowledge Base

Scan Performance

Out of Scope Links

Crawling Performance

MIME Types

Comments

Slowest Pages

File Extensions

JavaScript Files

Issues (35)

Group Issues by

Vulnerability Type

Severity

Confirmation

URL

Issue...Enc...Log...

Current Speed: 2.0 req/sec

Average Speed: 2.7 req/sec

Total Requests: 8727

Failed Requests: 0

HEAD Requests: 573

Elapsed Time: 00:54:39

VulnerabilityBrowser ViewHTTP Request / Response

Controlled ScanRetestSend to Request BuilderGenerate WAF RulesExecute SQL CommandsGet ShellLFI ExploitationGenerate ExploitShort Names

Out-of-date Version (OpenSSL)

CRITICAL

CERTAINTY

URL

IDENTIFIED VERSION

LATEST VERSION

VULNERABILITY DATABASE

CLASSIFICATION

PCI 3.1

PCI 3.2

OWASP 2013

CAPEC

VULNERABILITY DETAILS

Netsparker identified you are using an out-of-date version of OpenSSL.

IMPACT

Since this is an old version of the software, it may be vulnerable to attacks.

REMEDY

Please upgrade your installation of OpenSSL to the latest stable version.

REMEDY REFERENCES

OpenSSL Project

KNOWN VULNERABILITIES IN THIS VERSION

Auto save finished successfully - 11-08-2021 22:42:21

33511

No vulnerability database updates found.

Proxy: System

FileViewReportingToolsHelp

Start New ScanStart Incremental ScanPauseSkip Current PhaseImport LinksStart Proxy

Site Map

forgotten-password-send.htmlindex.old[Possible] Backup File Disclosurefaq.html.bakKnowledge BaseScan PerformanceOut of Scope LinksCrawling PerformanceMIME TypesCommentsSlowest PagesFile ExtensionsJavaScript Files

Issues (35)

Group Issues by

Vulnerability TypeSeverityConfirmationURL

Issue...Enc...Log...

Current speed: 2.4 req/secAverage Speed: 2.7 req/secTotal Requests: 8948Failed Requests: 0HEAD Requests: 573Elapsed Time: 00:55:50

VulnerabilityBrowser ViewHTTP Request / Response

Controlled ScanRetestSend to Request BuilderGenerate WAF RulesExecute SQL CommandsGet ShellLFI ExploitationGenerate ExploitShort Names

Out-of-date Version (Tomcat)

CERTAINTY

URL

IDENTIFIED VERSION

LATEST VERSION

VULNERABILITY DATABASE

http://zero.webappsecurity.com/cgi-bin/

7.0.70 (contains 4 critical and 45 other vulnerabilities)

10.0.8

Result is based on 30-07-2021 vulnerability database content.

CLASSIFICATION

PCI 3.1

PCI 3.2

OWASP 2013

CAPEC

6.2

6.2

A9

310

VULNERABILITY DETAILS

Netsparker identified you are using an out-of-date version of Tomcat.

REMEDY

Please upgrade your installation of Tomcat to the latest stable version.

REMEDY REFERENCES

Apache Tomcat Versions and Download

KNOWN VULNERABILITIES IN THIS VERSION

Apache Tomcat Improper Authentication Vulnerability

A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of the

Auto save finished successfully - 11-08-2021 22:42:21

33511No vulnerability database updates found.Proxy: System

22:4511-08-202126°C Mostly cloudyENG

REPORT ON THE VULNERABILITY “Out-of-date Version (Apache)” :

The screenshot displays the Nessus vulnerability scanner interface. The main window shows a vulnerability report for 'Out-of-date Version (Apache)', which is marked as 'CRITICAL'. The report includes details such as the URL (<https://zero.webappsecurity.com/>), the identified version (2.2.6), and the latest version (2.4.48). It also provides a classification table with scores for PCI 3.1, PCI 3.2, OWASP 2013, and CAPEC. The 'VULNERABILITY DETAILS' section states that Netsparker identified the use of an out-of-date version of Apache. The 'IMPACT' section notes that since this is an old version of the software, it may be vulnerable to attacks. The 'REMEDY' section advises upgrading the installation of Apache to the latest stable version. The 'REMEDY REFERENCES' section includes a link to 'Downloading the Apache HTTP Server'. The 'KNOWN VULNERABILITIES IN THIS VERSION' section is partially visible at the bottom.

Out-of-date Version (Apache) CRITICAL

CERTAINTY

URL <https://zero.webappsecurity.com/>

IDENTIFIED VERSION 2.2.6 (contains 4 critical and 65 other vulnerabilities)

LATEST VERSION 2.4.48

VULNERABILITY DATABASE Result is based on 30-07-2021 vulnerability database content.

CLASSIFICATION	
PCI 3.1	6.2
PCI 3.2	6.2
OWASP 2013	A9
CAPEC	310

VULNERABILITY DETAILS

Netsparker identified you are using an out-of-date version of Apache.

IMPACT

Since this is an old version of the software, it may be vulnerable to attacks.

REMEDY

Please upgrade your installation of Apache to the latest stable version.

REMEDY REFERENCES

- [Downloading the Apache HTTP Server](#)

KNOWN VULNERABILITIES IN THIS VERSION

Auto save finished successfully - 11-08-2021 22:42:21

3 3 5 13 11 No vulnerability database updates found. Proxy: System

-
- It had found that the vulnerability of this is “critical”
 - Identified version: 2.2.6 Latest version:2.4.48
 - To make it better: Upgrade your installation of Apache to the latest stable version.
 - It Contains 69 vulnerabilities . out of which 4 of them is critical and 65 other is vulnerable
-

Four (4) critical vulnerabilities are:

- **Apache HTTP Server Resource Management Errors Vulnerability**
 - **Apache HTTP Server Numeric Errors Vulnerability**
 - **Apache HTTP Server Insufficient Information Vulnerability**
 - **Apache HTTP Server Out-of-bounds Read Vulnerability**
-

Apache HTTP Server Resource Management Errors Vulnerability:

Unspecified vulnerability in mod_proxy_balancer for Apache HTTP Server 2.2.x before 2.2.7-dev, when running on Windows, allows remote attackers to trigger memory corruption via an extended URL. NOTE: the seller couldn't reproduce this issue.

Apache HTTP Server Numeric Errors Vulnerability:

The `stream_reqbody_cl` function in `mod_proxy_http.c` within the `mod_proxy` module within the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, doesn't properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.

Apache HTTP Server Insufficient Information Vulnerability:

mod_session_dbd.c within the mod_session_dbd module within the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and therefore the requirement for a replacement session ID, which has unspecified impact and remote attack vectors.

Apache HTTP Server Out-of-bounds Read Vulnerability:

A specially crafted HTTP request header could have crashed the Apache HTTP Server before version 2.4.30 thanks to an out of bound read while preparing data to be cached in shared memory. It might be used as a Denial of Service attack against users of `mod_cache_socache`. The vulnerability is taken into account as low risk since `mod_cache_socache` isn't widely used, `mod_cache_disk` isn't concerned by this vulnerability.
