EH - TASK 2

Vulnerabilities-Netsparker

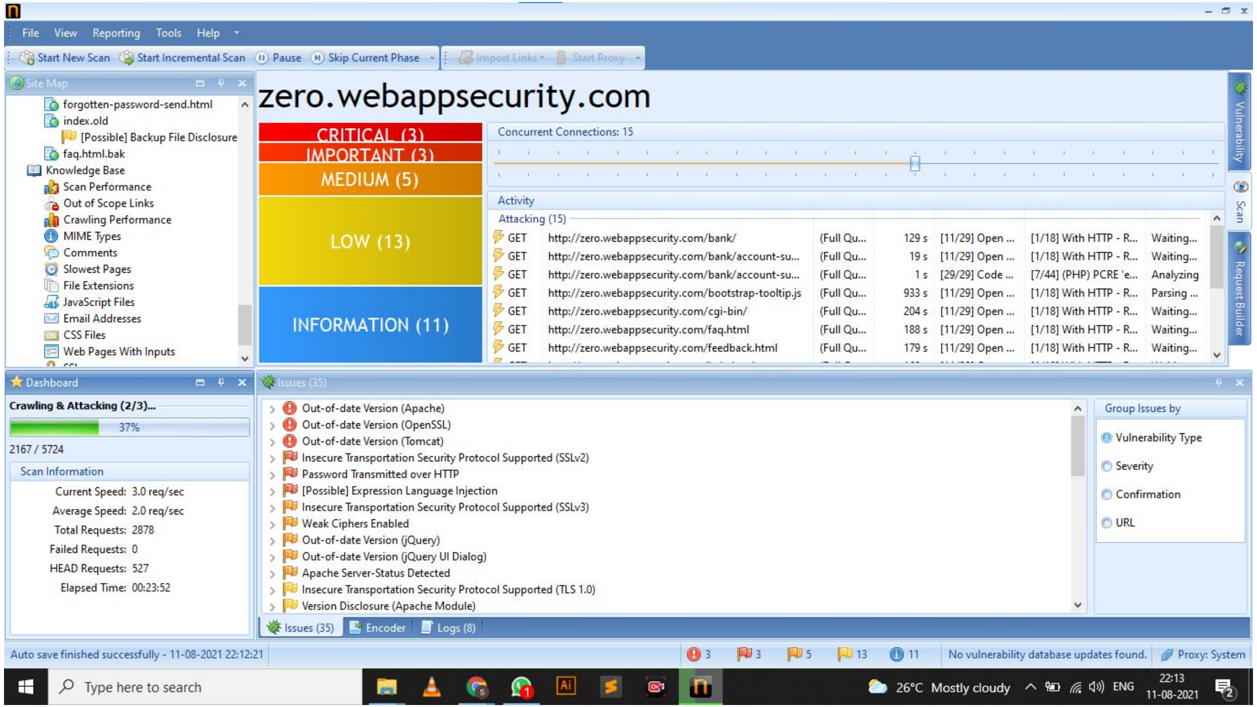
Step 1: open netsparker

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:



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
Web Pages With Inputs

zero.webappsecurity.com

CRITICAL (3)
IMPORTANT (3)
MEDIUM (5)
LOW (13)
INFORMATION (11)

Concurrent Connections: 15

Activity

Attacking (15)

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

Dashboard

Crawling & Attacking (2/3)...

37%

2167 / 5724

Scan Information

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)

- Out-of-date Version (Apache)
- Out-of-date Version (OpenSSL)
- Out-of-date Version (Tomcat)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- Out-of-date Version (jQuery)
- Out-of-date Version (jQuery UI Dialog)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)

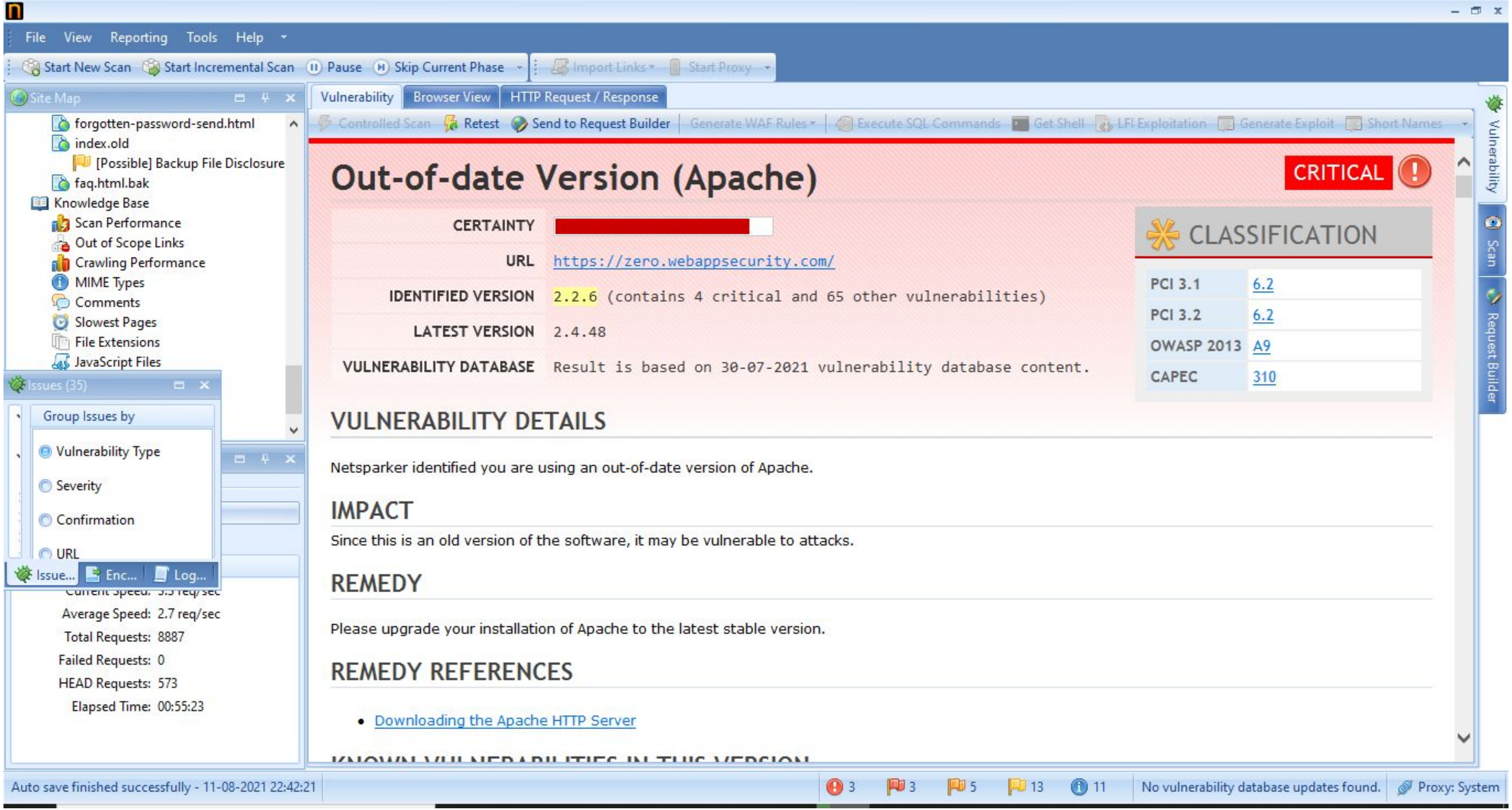
Group Issues by

● Vulnerability Type
○ Severity
○ Confirmation
○ URL

Issues (35) Encoder Logs (8)

Auto save finished successfully - 11-08-2021 22:12:21

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



Current Speed: 3.3 req/sec
Average Speed: 2.7 req/sec
Total Requests: 8887
Failed Requests: 0
HEAD Requests: 573
Elapsed Time: 00:55:23

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

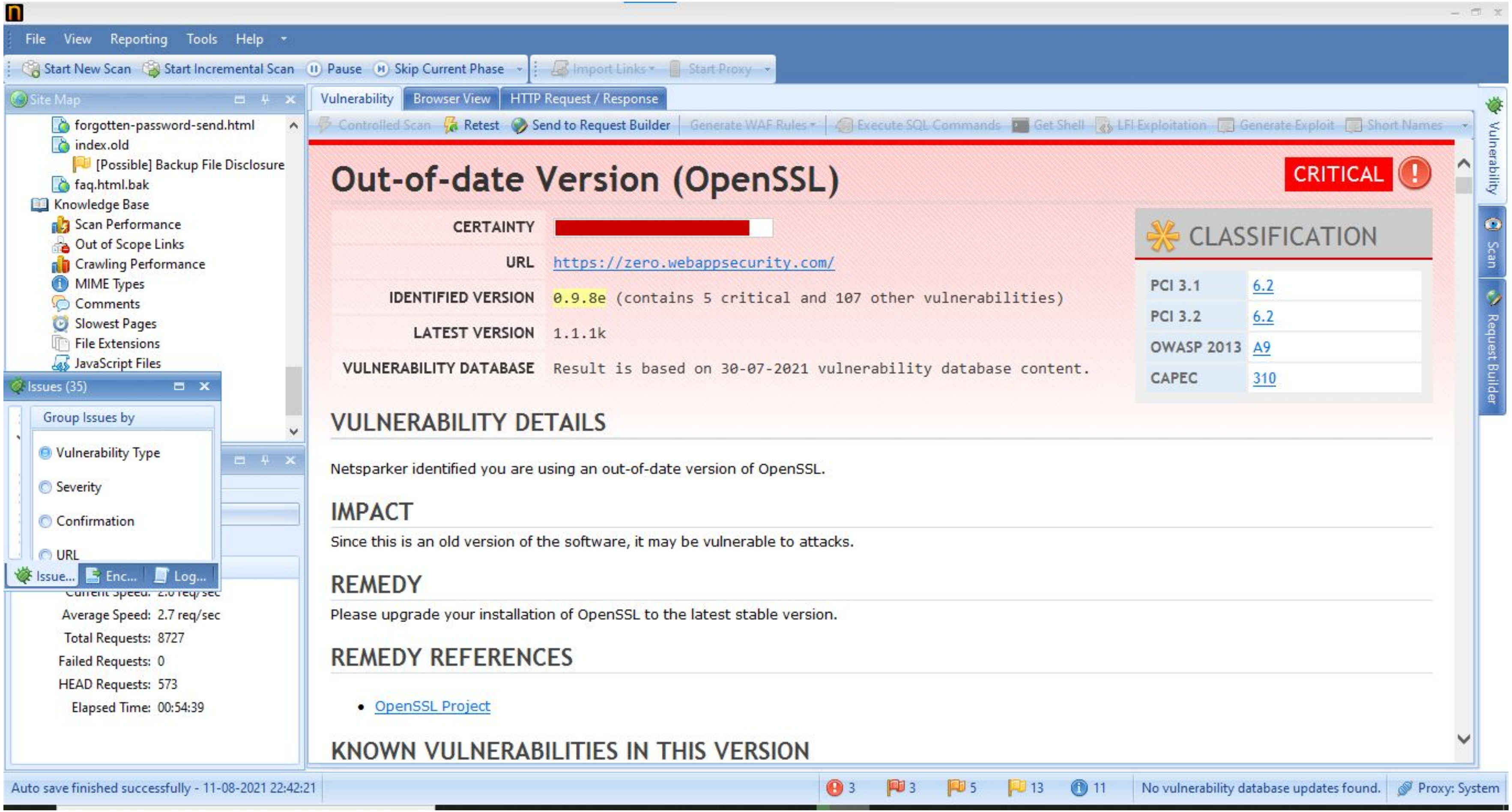
Please upgrade your installation of Apache to the latest stable version.

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



- 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

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

Out-of-date Version (OpenSSL)

CRITICAL !

CERTAINTY	🟥
URL	https://zero.webappsecurity.com/
IDENTIFIED VERSION	0.9.8e (contains 5 critical and 107 other vulnerabilities)
LATEST VERSION	1.1.1k
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 OpenSSL.

IMPACT

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

REMEDY

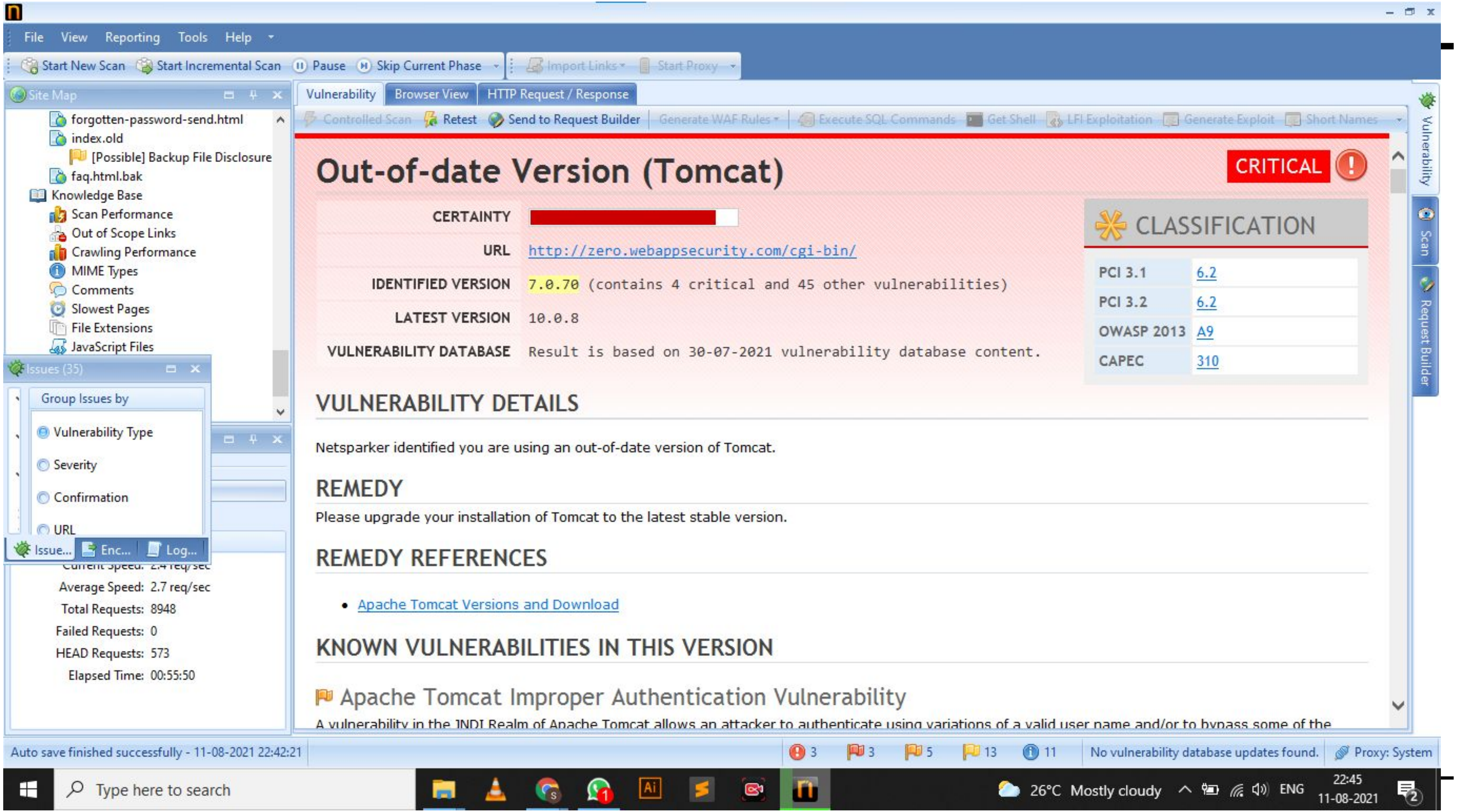
Please upgrade your installation of OpenSSL to the latest stable version.

REMEDY REFERENCES

- OpenSSL Project

KNOWN VULNERABILITIES IN THIS VERSION

Auto save finished successfully - 11-08-2021 22:42:21 | 3 | 3 | 5 | 13 | 11 | No vulnerability database updates found. | Proxy: System



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

Current Speed: 2.4 req/sec
Average Speed: 2.7 req/sec
Total Requests: 8948
Failed Requests: 0
HEAD Requests: 573
Elapsed Time: 00:55:50

Out-of-date Version (Tomcat)

CRITICAL

CERTAINTY	
URL	http://zero.webappsecurity.com/cgi-bin/
IDENTIFIED VERSION	7.0.70 (contains 4 critical and 45 other vulnerabilities)
LATEST VERSION	10.0.8
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 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

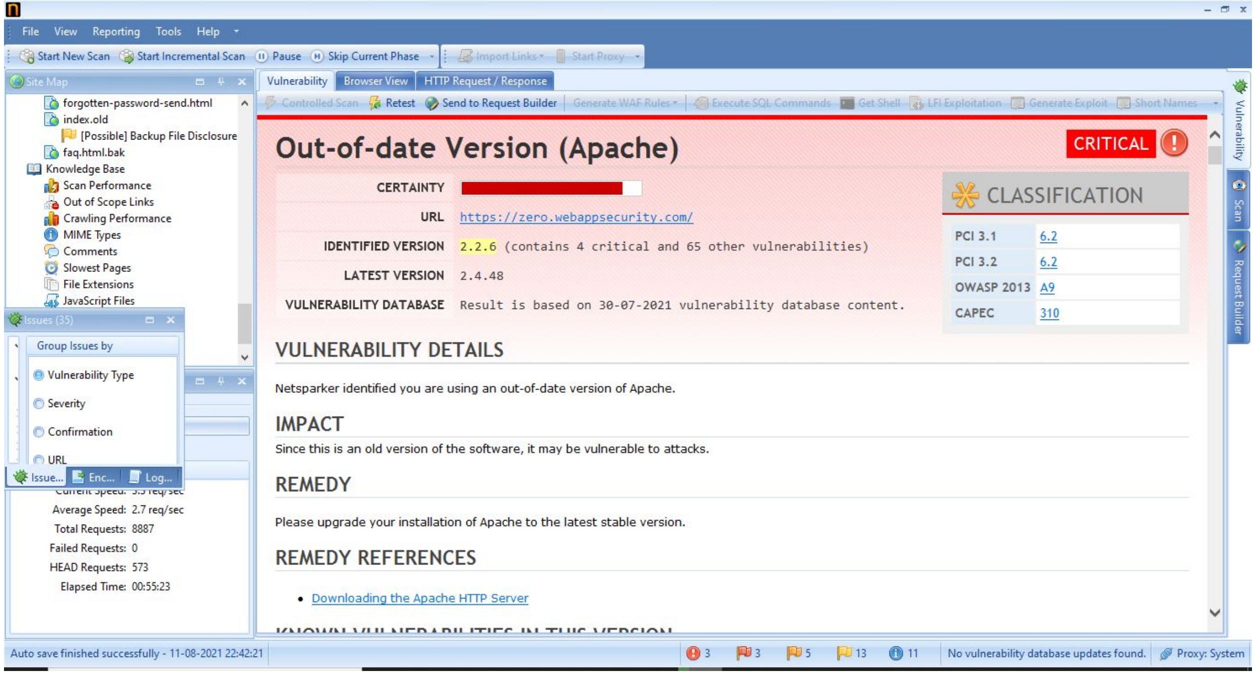
Auto save finished successfully - 11-08-2021 22:42:21

3 3 5 13 11

No vulnerability database updates found.

Proxy: System

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



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

Current Speed: 3.3 req/sec
Average Speed: 2.7 req/sec
Total Requests: 8887
Failed Requests: 0
HEAD Requests: 573
Elapsed Time: 00:55:23

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

No vulnerability database updates found.

- 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.