INTERNSHIPSTUDIO_PROJECT_SUBMISSION

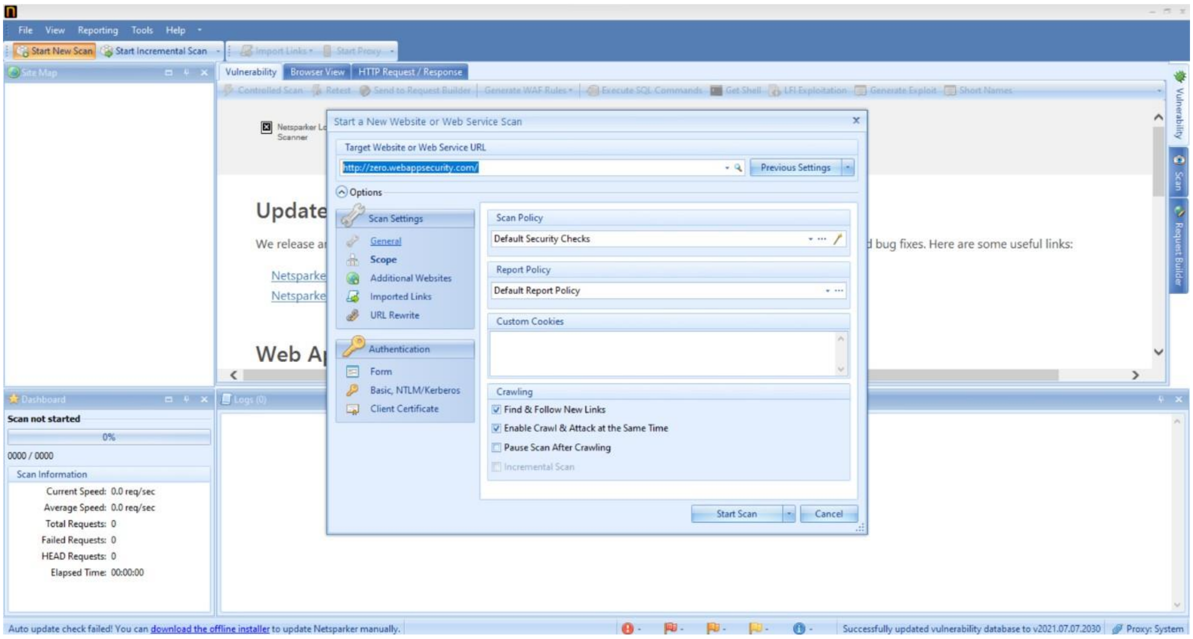
PROBLEM_STATEMENT

TASK-2:

http://zero.webappsecurity.com/ We have set up a real life-like web application in the form of an online bank portal. Your task is to test this website and find all possible vulnerabilities and loopholes in it. To do so you can use the automatic vulnerabilities scanner "Net sparker" which was taught to you in the session of Automatic Vulnerability Scanner. If you want you can download it using this link:

https://drive.google.com/drive/folders/193Ha6QVU9Joh-rhhOvH78HrTNO1OgaMx?usp =sharing You have to find 3 critical vulnerabilities. No matter if they are taught to you or not. Now just choose any 1 amongst that 3 and write a report in your own language. If you are using Net sparker you can use the report already generated by software but make sure you do not have to copy it. You have to then submit the report generated by you.

SOLUTION:



Start a New Website or Web Service Scan

Target Website or Web Service URL: http://zero.webappsecurity.com/

Options

Scan Settings

Scan Policy: Default Security Checks

Report Policy: Default Report Policy

Custom Cookies

Crawling

☑ Find & Follow New Links

☑ Enable Crawl & Attack at the Same Time

☐ Pause Scan After Crawling

☐ Incremental Scan

Scan not started

0%

0000 / 0000

Scan Information

Current Speed: 0.0 req/sec

Average Speed: 0.0 req/sec

Total Requests: 0

Failed Requests: 0

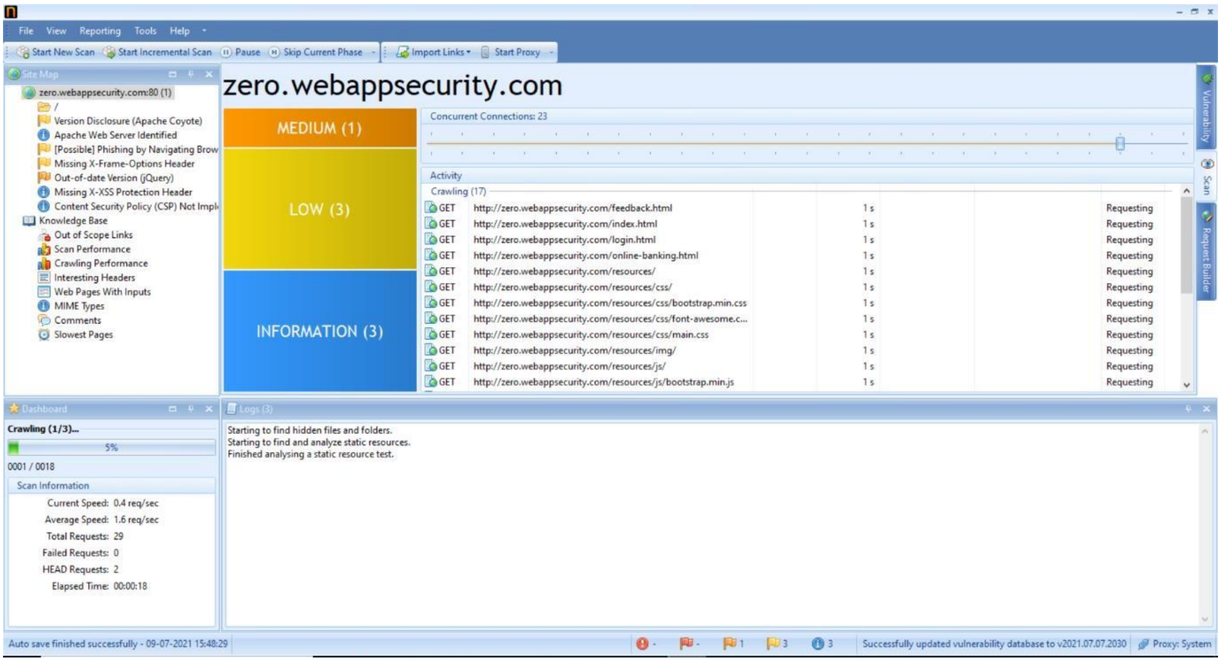
HEAD Requests: 0

Elapsed Time: 00:00:00

Auto update check failed! You can download the offline installer to update Netsparker manually.

Successfully updated vulnerability database to v2021.07.07.2030

Proxy: System



zero.webappsecurity.com

- zero.webappsecurity.com:80 (1)
  - /
  - Version Disclosure (Apache Coyote)
  - Apache Web Server Identified
  - [Possible] Phishing by Navigating Brow
  - Missing X-Frame-Options Header
  - Out-of-date Version (jQuery)
  - Missing X-XSS Protection Header
  - Content Security Policy (CSP) Not Impl
- Knowledge Base
  - Out of Scope Links
  - Scan Performance
  - Crawling Performance
  - Interesting Headers
  - Web Pages With Inputs
  - MIME Types
  - Comments
  - Slowest Pages

Concurrent Connections: 23

Activity

Crawling (17)

GET	http://zero.webappsecurity.com/feedback.html	1 s	Requesting
GET	http://zero.webappsecurity.com/index.html	1 s	Requesting
GET	http://zero.webappsecurity.com/login.html	1 s	Requesting
GET	http://zero.webappsecurity.com/online-banking.html	1 s	Requesting
GET	http://zero.webappsecurity.com/resources/	1 s	Requesting
GET	http://zero.webappsecurity.com/resources/css/	1 s	Requesting
GET	http://zero.webappsecurity.com/resources/css/bootstrap.min.css	1 s	Requesting
GET	http://zero.webappsecurity.com/resources/css/font-awesome.c...	1 s	Requesting
GET	http://zero.webappsecurity.com/resources/css/main.css	1 s	Requesting
GET	http://zero.webappsecurity.com/resources/img/	1 s	Requesting
GET	http://zero.webappsecurity.com/resources/js/	1 s	Requesting
GET	http://zero.webappsecurity.com/resources/js/bootstrap.min.js	1 s	Requesting

Crawling (1/3)...

5%

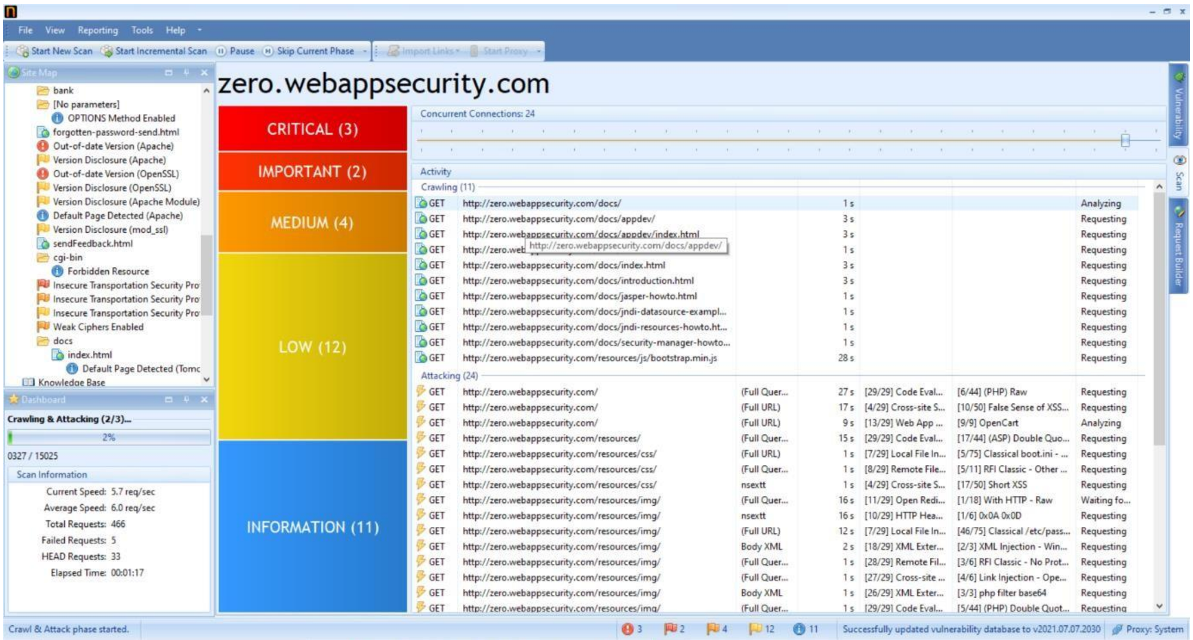
0001 / 0018

Scan Information

Current Speed: 0.4 req/sec
Average Speed: 1.6 req/sec
Total Requests: 29
Failed Requests: 0
HEAD Requests: 2
Elapsed Time: 00:00:18

```
Starting to find hidden files and folders.
Starting to find and analyze static resources.
Finished analysing a static resource test.
```

Auto save finished successfully - 09-07-2021 15:48:29 | - | - | 1 | 3 | 3 | Successfully updated vulnerability database to v2021.07.07.2030 | Proxy: System



zero.webappsecurity.com

- bank
- [No parameters]
  - OPTIONS Method Enabled
- forgotten-password-send.html
- Out-of-date Version (Apache)
- Version Disclosure (Apache)
- Out-of-date Version (OpenSSL)
- Version Disclosure (OpenSSL)
- Version Disclosure (Apache Module)
- Default Page Detected (Apache)
- Version Disclosure (mod_ssl)
- sendFeedback.html
- cgi-bin
  - Forbidden Resource
- Insecure Transportation Security Pro
- Insecure Transportation Security Pro
- Insecure Transportation Security Pro
- Weak Ciphers Enabled
- docs
  - index.html
    - Default Page Detected (Tomc
- Knowledge Base

Concurrent Connections: 24

Activity

Crawling (11)

GET	http://zero.webappsecurity.com/docs/		1 s			Analyzing
GET	http://zero.webappsecurity.com/docs/appdev/		3 s			Requesting
GET	http://zero.webappsecurity.com/docs/appdev/index.html		3 s			Requesting
GET	http://zero.web http://zero.webappsecurity.com/docs/appdev/		1 s			Requesting
GET	http://zero.webappsecurity.com/docs/index.html		3 s			Requesting
GET	http://zero.webappsecurity.com/docs/introduction.html		3 s			Requesting
GET	http://zero.webappsecurity.com/docs/jasper-howto.html		1 s			Requesting
GET	http://zero.webappsecurity.com/docs/jndi-datasource-exampl...		1 s			Requesting
GET	http://zero.webappsecurity.com/docs/jndi-resources-howto.ht...		1 s			Requesting
GET	http://zero.webappsecurity.com/docs/security-manager-howto...		1 s			Requesting
GET	http://zero.webappsecurity.com/resources/js/bootstrap.min.js		28 s			Requesting

Attacking (24)

GET	http://zero.webappsecurity.com/	(Full Quer...	27 s	[29/29] Code Eval...	[6/44] (PHP) Raw	Requesting
GET	http://zero.webappsecurity.com/	(Full URL)	17 s	[4/29] Cross-site S...	[10/50] False Sense of XSS...	Requesting
GET	http://zero.webappsecurity.com/	(Full URL)	9 s	[13/29] Web App ...	[9/9] OpenCart	Analyzing
GET	http://zero.webappsecurity.com/resources/	(Full Quer...	15 s	[29/29] Code Eval...	[17/44] (ASP) Double Quo...	Requesting
GET	http://zero.webappsecurity.com/resources/css/	(Full URL)	1 s	[7/29] Local File In...	[5/75] Classical boot.ini - ...	Requesting
GET	http://zero.webappsecurity.com/resources/css/	(Full Quer...	1 s	[8/29] Remote File...	[5/11] RFI Classic - Other ...	Requesting
GET	http://zero.webappsecurity.com/resources/css/	nsextt	1 s	[4/29] Cross-site S...	[17/50] Short XSS	Requesting
GET	http://zero.webappsecurity.com/resources/img/	(Full Quer...	16 s	[11/29] Open Redi...	[1/18] With HTTP - Raw	Waiting fo...
GET	http://zero.webappsecurity.com/resources/img/	nsextt	16 s	[10/29] HTTP Hea...	[1/6] 0x0A 0x0D	Requesting
GET	http://zero.webappsecurity.com/resources/img/	(Full URL)	12 s	[7/29] Local File In...	[46/75] Classical /etc/pass...	Requesting
GET	http://zero.webappsecurity.com/resources/img/	Body XML	2 s	[18/29] XML Exter...	[2/3] XML Injection - Win...	Requesting
GET	http://zero.webappsecurity.com/resources/img/	(Full Quer...	1 s	[28/29] Remote Fil...	[3/6] RFI Classic - No Prot...	Requesting
GET	http://zero.webappsecurity.com/resources/img/	(Full Quer...	1 s	[27/29] Cross-site ...	[4/6] Link Injection - Ope...	Requesting
GET	http://zero.webappsecurity.com/resources/img/	Body XML	1 s	[26/29] XML Exter...	[3/3] php filter base64	Requesting
GET	http://zero.webappsecurity.com/resources/img/	(Full Quer...	1 s	[29/29] Code Eval...	[5/44] (PHP) Double Quot...	Requesting

Crawling & Attacking (2/3)...

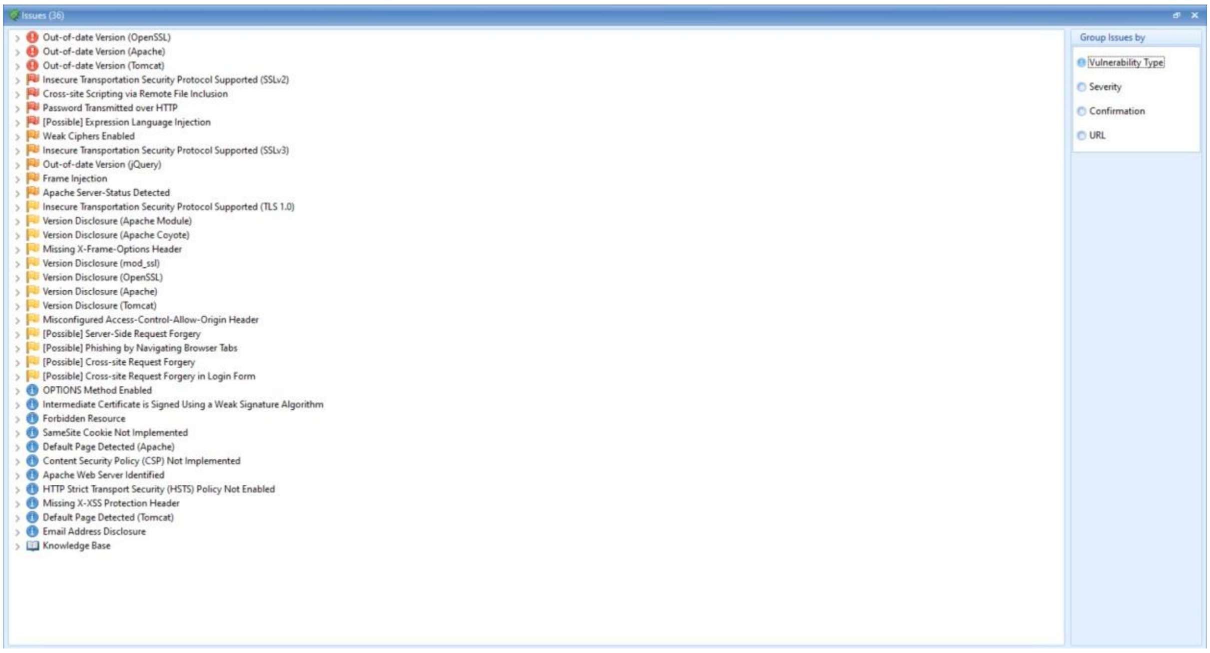
2%

0327 / 15025

Scan Information

Current Speed: 5.7 req/sec
Average Speed: 6.0 req/sec
Total Requests: 466
Failed Requests: 5
HEAD Requests: 33
Elapsed Time: 00:01:17

Crawl & Attack phase started. | 3 | 2 | 4 | 12 | 11 | Successfully updated vulnerability database to v2021.07.07.2030 | Proxy: System



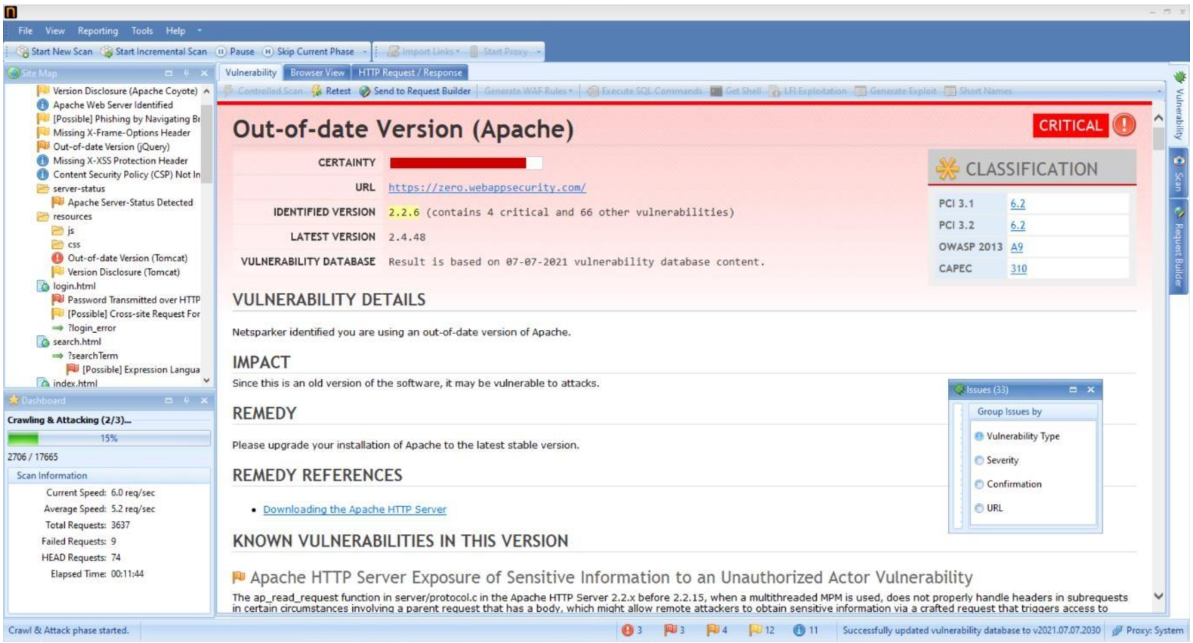
Issues (36)

- Out-of-date Version (OpenSSL)
- Out-of-date Version (Apache)
- Out-of-date Version (Tomcat)
- Insecure Transportation Security Protocol Supported (SSLv2)
- Cross-site Scripting via Remote File Inclusion
- Password Transmitted over HTTP
- [Possible] Expression Language Injection
- Weak Ciphers Enabled
- Insecure Transportation Security Protocol Supported (SSLv3)
- Out-of-date Version (jQuery)
- Frame Injection
- Apache Server-Status Detected
- Insecure Transportation Security Protocol Supported (TLS 1.0)
- Version Disclosure (Apache Module)
- Version Disclosure (Apache Coyote)
- Missing X-Frame-Options Header
- Version Disclosure (mod_ssl)
- Version Disclosure (OpenSSL)
- Version Disclosure (Apache)
- Version Disclosure (Tomcat)
- Misconfigured Access-Control-Allow-Origin Header
- [Possible] Server-Side Request Forgery
- [Possible] Phishing by Navigating Browser Tabs
- [Possible] Cross-site Request Forgery
- [Possible] Cross-site Request Forgery in Login Form
- OPTIONS Method Enabled
- Intermediate Certificate is Signed Using a Weak Signature Algorithm
- Forbidden Resource
- SameSite Cookie Not Implemented
- Default Page Detected (Apache)
- Content Security Policy (CSP) Not Implemented
- Apache Web Server Identified
- HTTP Strict Transport Security (HSTS) Policy Not Enabled
- Missing X-XSS Protection Header
- Default Page Detected (Tomcat)
- Email Address Disclosure
- Knowledge Base

Group Issues by

● Vulnerability Type
○ Severity
○ Confirmation
○ URL

REPORT GENERATED BY NETSPARKER:



Crawling & Attacking (2/3)...

15%

2706 / 17665

Scan Information

Current Speed:	6.0 req/sec
Average Speed:	5.2 req/sec
Total Requests:	3637
Failed Requests:	9
HEAD Requests:	74
Elapsed Time:	00:11:44

Out-of-date Version (Apache)

CRITICAL

CERTAINTY	
URL	https://zero.webappsecurity.com/
IDENTIFIED VERSION	2.2.6 (contains 4 critical and 66 other vulnerabilities)
LATEST VERSION	2.4.48
VULNERABILITY DATABASE	Result is based on 07-07-2021 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

Apache HTTP Server Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to

Issues (33)

Group Issues by

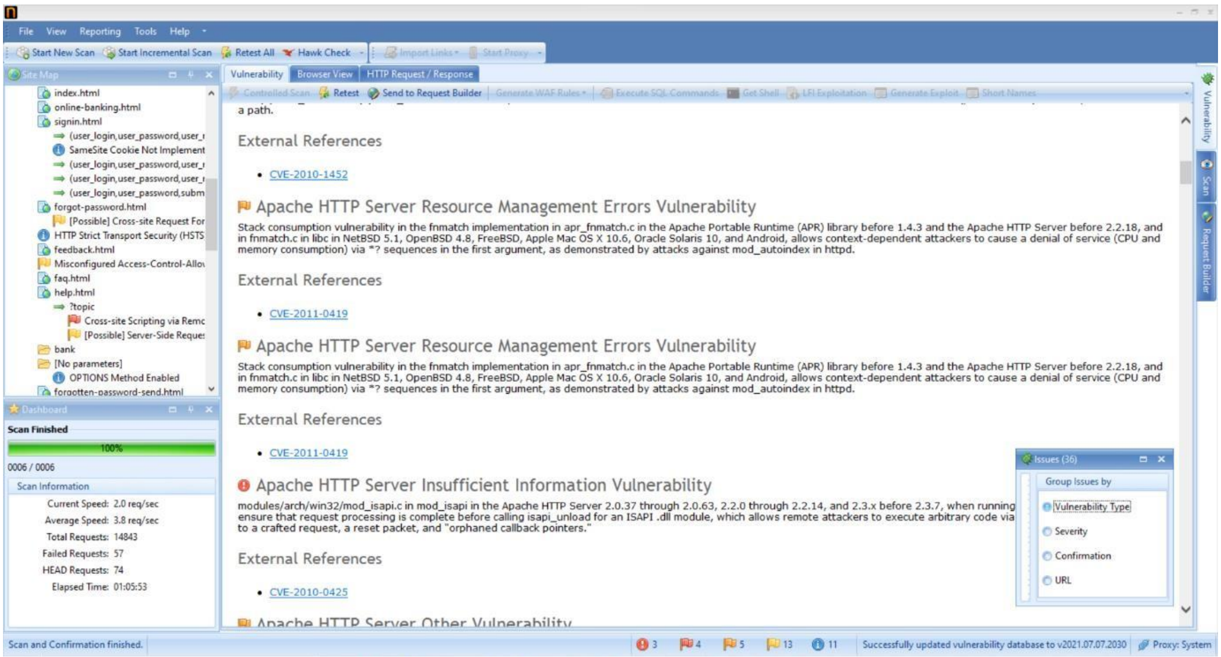
● Vulnerability Type
○ Severity
○ Confirmation
○ URL

Crawl & Attack phase started.

3 3 4 12 11

Successfully updated vulnerability database to v2021.07.07.2030

Proxy: System



a path.

External References

- CVE-2010-1452

Apache HTTP Server Resource Management Errors Vulnerability

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

External References

- CVE-2011-0419

Apache HTTP Server Resource Management Errors Vulnerability

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

External References

- CVE-2011-0419

Apache HTTP Server Insufficient Information Vulnerability

modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via to a crafted request, a reset packet, and "orphaned callback pointers."

External References

- CVE-2010-0425

Apache HTTP Server Other Vulnerability

Scan Finished

100%

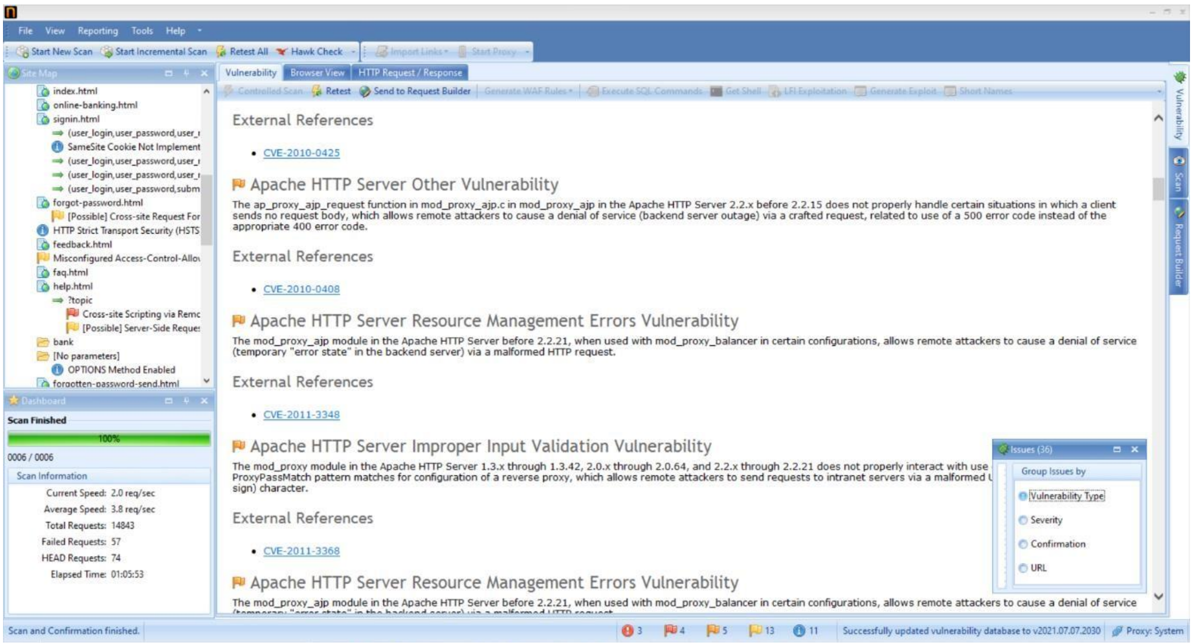
0006 / 0006

Scan Information

Current Speed: 2.0 req/sec
Average Speed: 3.8 req/sec
Total Requests: 14843
Failed Requests: 57
HEAD Requests: 74
Elapsed Time: 01:05:53

● Vulnerability Type
○ Severity
○ Confirmation
○ URL

Scan and Confirmation finished. 3 4 5 13 11 Successfully updated vulnerability database to v2021.07.07.2030 Proxy: System



External References

- CVE-2010-0425

Apache HTTP Server Other Vulnerability

The ap_proxy_ajp_request function in mod_proxy_ajp.c in mod_proxy_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.

External References

- CVE-2010-0408

Apache HTTP Server Resource Management Errors Vulnerability

The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

External References

- CVE-2011-3348

Apache HTTP Server Improper Input Validation Vulnerability

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed U sign) character.

External References

- CVE-2011-3368

Apache HTTP Server Resource Management Errors Vulnerability

The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service

Scan Finished

100%

0006 / 0006

Scan Information

Current Speed: 2.0 req/sec
Average Speed: 3.8 req/sec
Total Requests: 14843
Failed Requests: 57
HEAD Requests: 74
Elapsed Time: 01:05:53

● Vulnerability Type
○ Severity
○ Confirmation
○ URL

Scan and Confirmation finished. 3 4 5 13 11 Successfully updated vulnerability database to v2021.07.07.2030 Proxy: System

INTERNSHIPSTUDIO_PROJECT_SUBMISSION

MY REPORT:
Title -Out-Of-Date Version(Apache)

Domain - https://zero.webappsecurity.com/

Vulnerability details: You are using out of

date version of Apache.

Impact -it may be vulnerable to attacks

because of its old version(version 2.6)

1. your systems/devices will be more vulnerable to random ware attacks,malware and data breaches.
2. Some times it might be the back door for your systems/devices/servers for hackers .
3. Hackers can steal yours user details because of its vulnerability.

Remedy: - found that latest version:2.4.48

Please Upgrade your Apache to latest version of Apache otherwise you will face above mention problems.

update to latest version and secure your website from hackers.