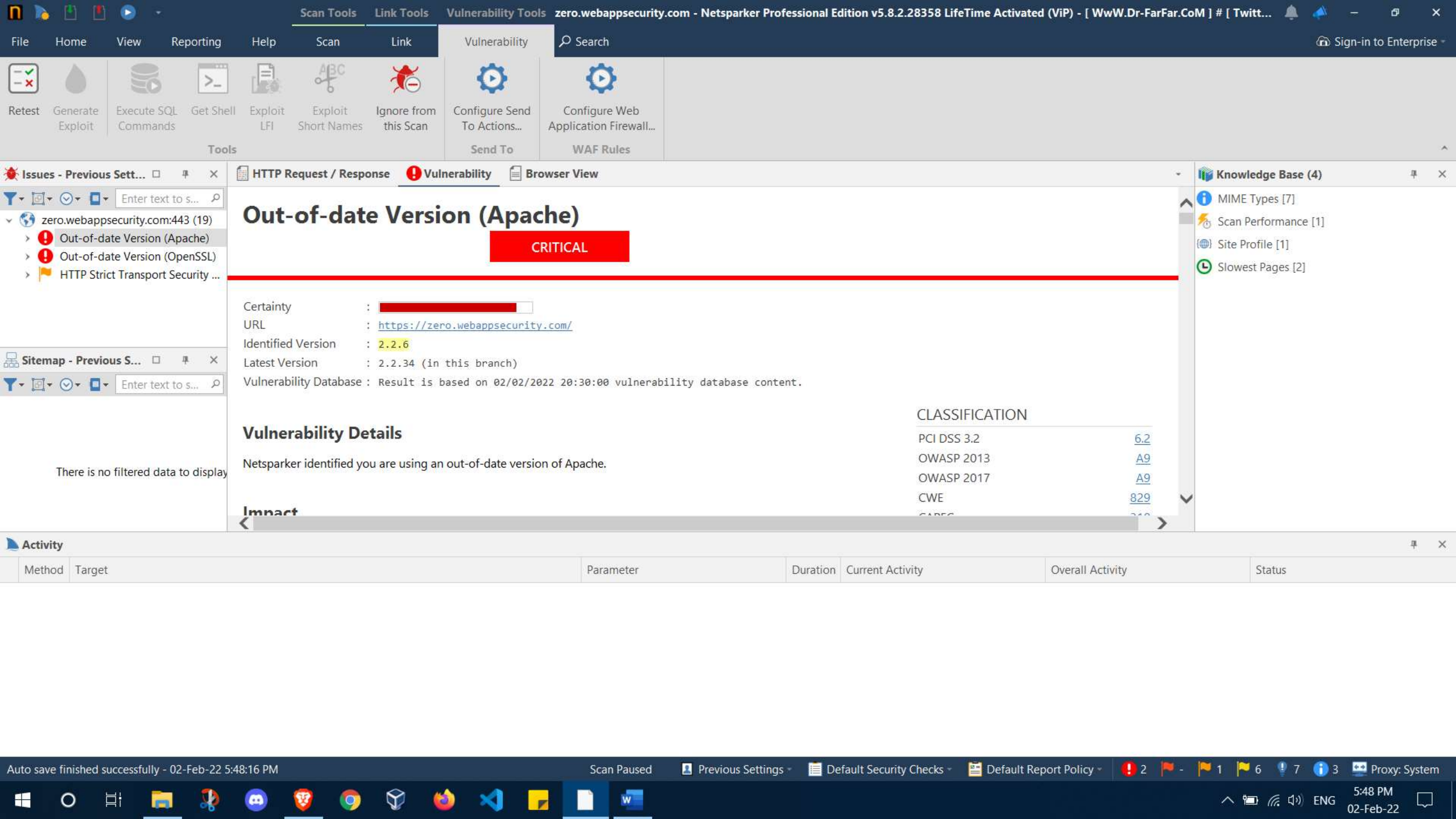
Scan Tools
Link Tools
Vulnerability Tools
zero.webappsecurity.com - Netsparker Professional Edition v5.8.2.28358 LifeTime Activated (ViP) - [WwW.Dr-FarFar.CoM] # [Twitt...
File
Home
View
Reporting
Help
Scan
Link
Vulnerability
Search
Sign-in to Enterprise
Retest
Generate Exploit
Execute SQL Commands
Get Shell
Exploit LFI
Exploit Short Names
Ignore from this Scan
Configure Send To Actions...
Configure Web Application Firewall...
Tools
Send To
WAF Rules
Issues - Previous Sett...
Enter text to s...
zero.webappsecurity.com:443 (19)
Out-of-date Version (Apache)
Out-of-date Version (OpenSSL)
HTTP Strict Transport Security ...
Sitemap - Previous S...
Enter text to s...
There is no filtered data to display
HTTP Request / Response
Vulnerability
Browser View
Out-of-date Version (Apache)
CRITICAL
Certainty :
URL : https://zero.webappsecurity.com/
Identified Version : 2.2.6
Latest Version : 2.2.34 (in this branch)
Vulnerability Database : Result is based on 02/02/2022 20:30:00 vulnerability database content.
Vulnerability Details
Netsparker identified you are using an out-of-date version of Apache.
Impact
CLASSIFICATION
PCI DSS 3.2 6.2
OWASP 2013 A9
OWASP 2017 A9
CWE 829
Knowledge Base (4)
MIME Types [7]
Scan Performance [1]
Site Profile [1]
Slowest Pages [2]
Activity
Method
Target
Parameter
Duration
Current Activity
Overall Activity
Status
Auto save finished successfully - 02-Feb-22 5:48:16 PM
Scan Paused
Previous Settings
Default Security Checks
Default Report Policy
2
1
6
7
3
Proxy: System
ENG
5:48 PM
02-Feb-22

Report Generated By Netsparker

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Netsparker identified you are using an out-of-date version of Apache.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 Out-of-bounds Write Vulnerability

A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

Affected Versions

0.8.11 to 2.4.51

External References

CVE-2021-44790

Apache HTTP Server Numeric Errors Vulnerability

The stream_reqbody_cl function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, does not 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.

Affected Versions

2.2 to 2.2.6

External References

CVE-2009-1890

Apache HTTP Server Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') Vulnerability
ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.
Affected Versions
2.0 to 2.2.29
External References
CVE-2021-39275
Apache HTTP Server Server-Side Request Forgery (SSRF) Vulnerability
A crafted request uri-path can cause mod_proxy to forward the request to an origin server chosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

Affected Versions
0.8.11 to 2.4.48

External References
CVE-2021-40438
Apache HTTP Server NULL Pointer Dereference Vulnerability
Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

Affected Versions
0.8.11 to 2.4.48

External References
CVE-2021-34798
Apache HTTP Server Configuration Vulnerability
The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.
Affected Versions
2.2.6 to 2.2.10
External References
CVE-2009-1195

My report

- **Issue**: Out-of-date Version (Apache)
- **Severity**: Critical
- **Confidence**: Certain
- **URL:** https://zero.webappsecurity.com/
- **Identified Latest Version:** 2.2.6
- **Latest Version:** 2.2.34
- **Vulnerability Details:**
- Netsparker identified you are using an out-of-date version of Apache.
- **These are the potential threats:**

  1)Apache HTTP Server Out-of-bounds Write Vulnerability: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts).By this vulnerability the software writes data past the end, or before the beginning, of the intended buffer. Typically, this can result in corruption of data, a crash, or malicious code execution and stealing of user cookies or other confidential details.

  2)Apache HTTP Server NULL Pointer Dereference Vulnerability: Malformed requests may cause the server to dereference a NULL pointer. This vulnerability can be exploited by hackers to maliciously crash a process to cause a denial of service or execute an arbitrary malicious piece of œde.

  3)Apache HTTP Server Server-Side Request Forgery (SSRF) Vulnerability: A crafted request uri-path can cause mod_proxy to forward the request to an origin server chosen by the remote user. This issue is one of the most dangerous and malicious attacks where the attacker can read server-side user credentials.

- **Impact:** Since this is an old version of the software, it may be vulnerable to attacks and as a result the user credentials may be stolen and the company will end up in a huge loss of data as well as income.
- **Remedy:** Please upgrade your installation of Apache to the latest stable version.