TASK 2:

FINDING VULNERABILITIES OF A GIVEN WEBSITE

Finding vulnerability of :

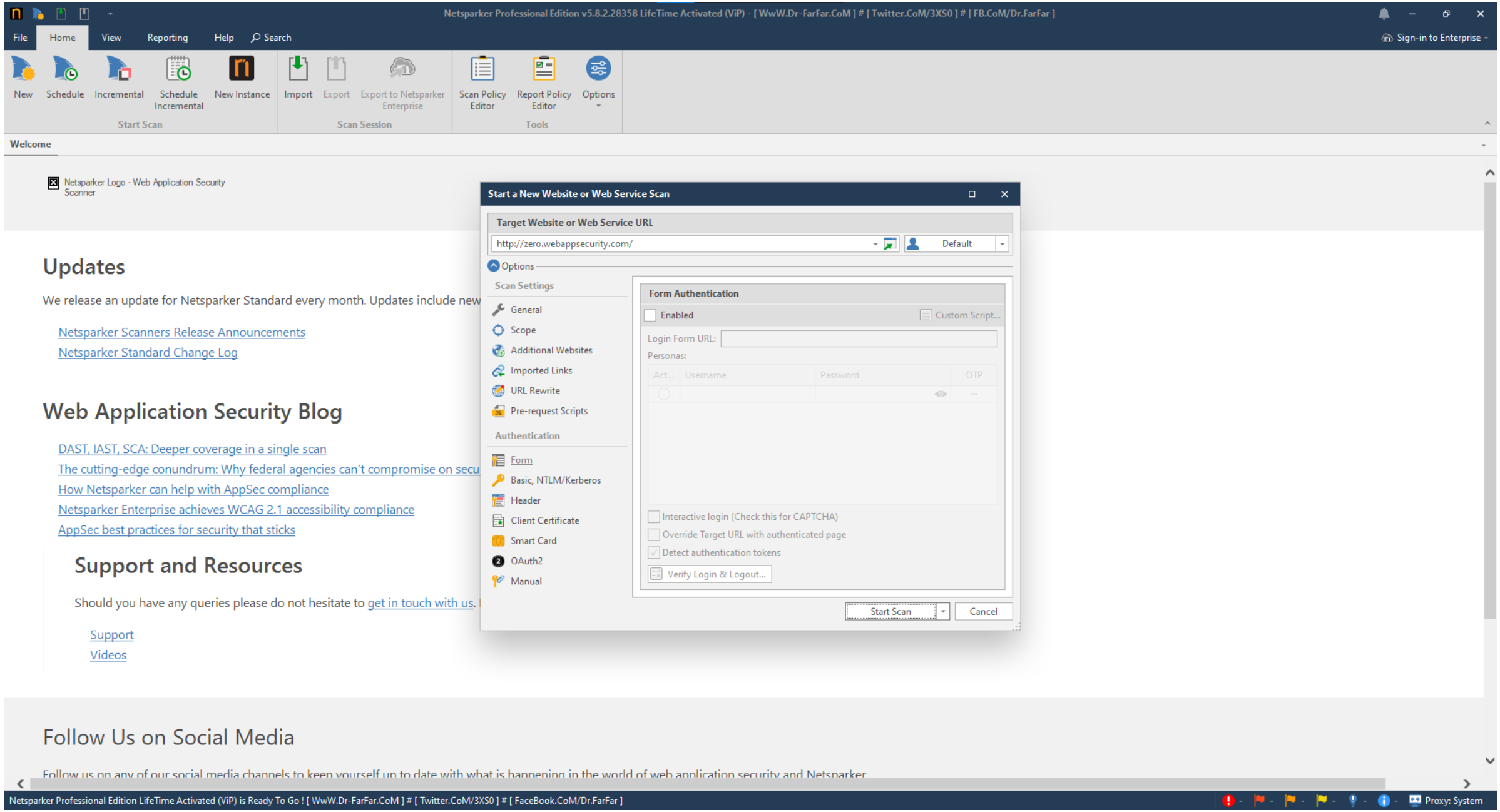
http://zero.webappsecurity.com/

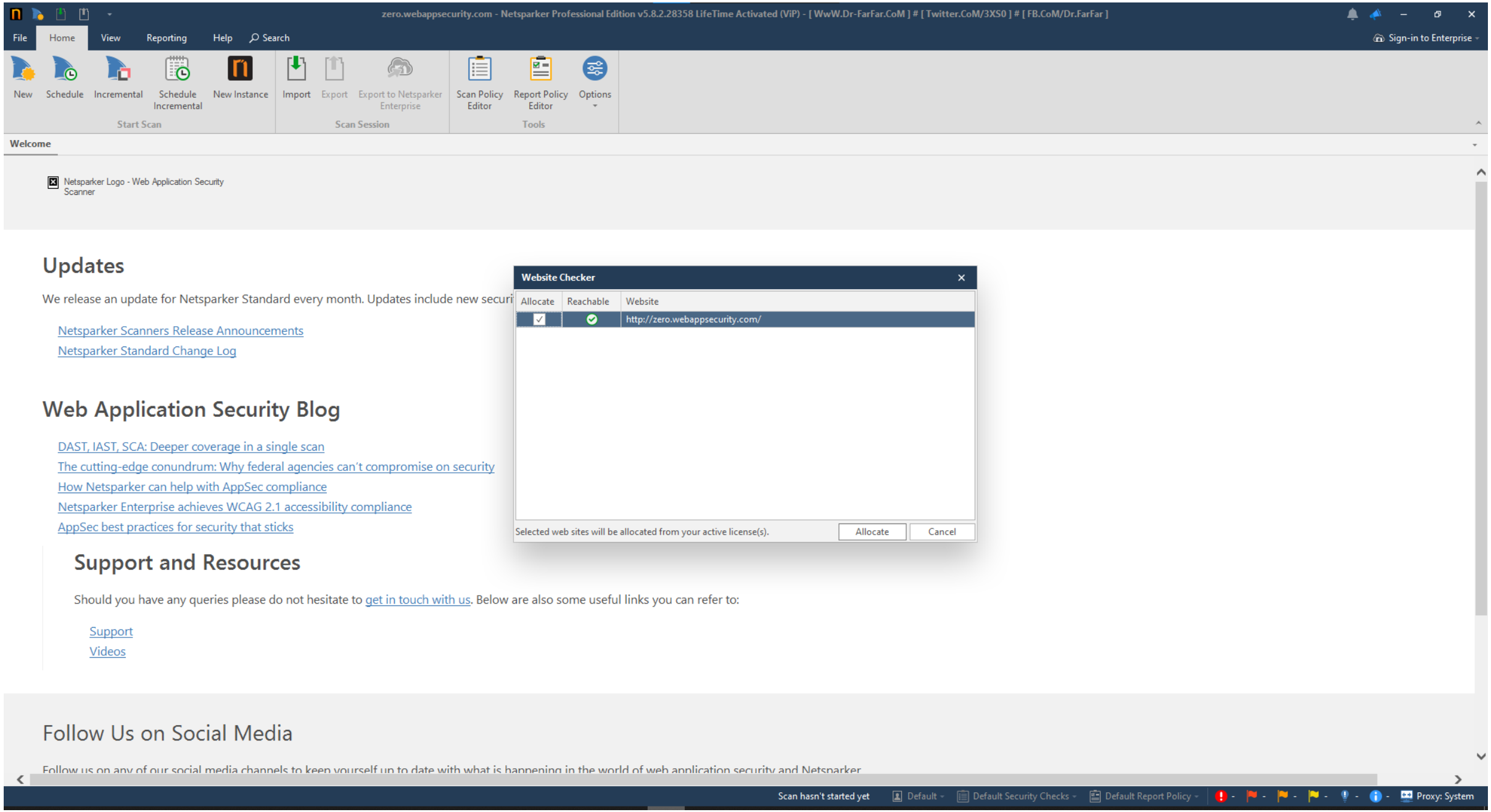
Problem Statement:

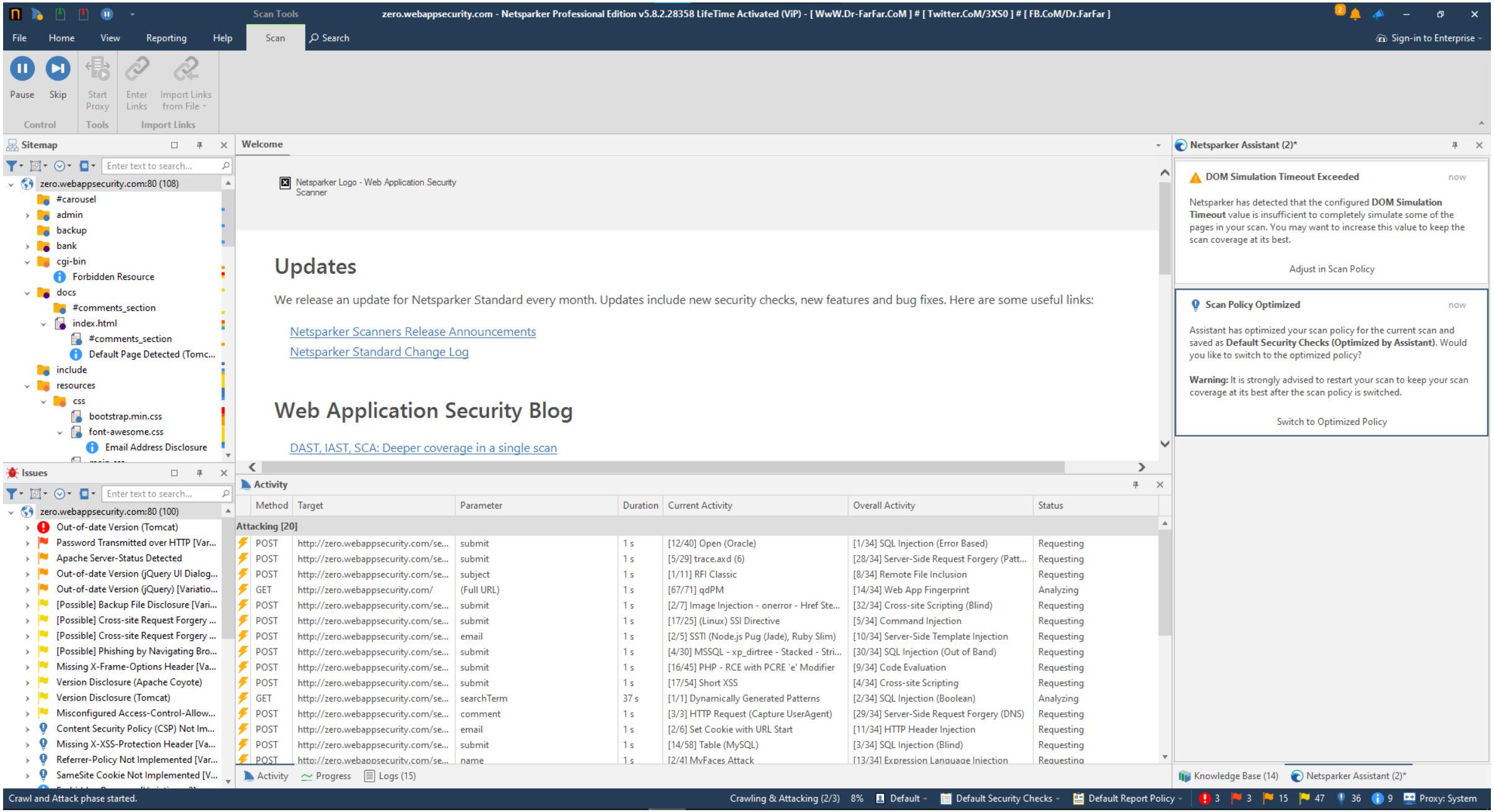
Website Link: http://zero.webappsecurity.com/ We have set up a real life-like web application in the form of an online bank portal. Your task is to test this website and find all possible vulnerabilities and loopholes in it.

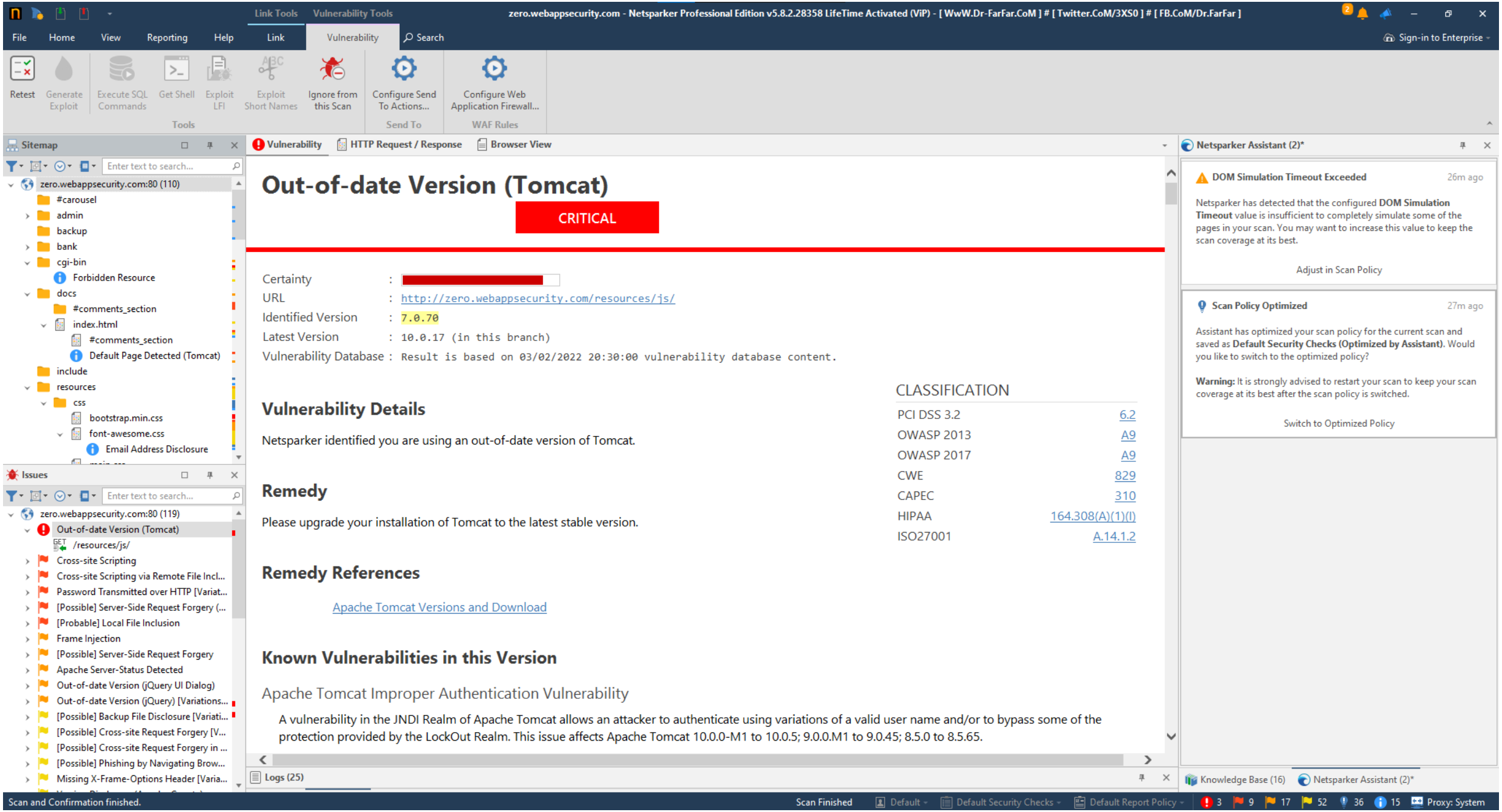
To do so you can use the automatic vulnerabilities scanner "Netsparker" which was taught to you in the session of Automatic Vulnerability Scanner. You have to find 3 critical vulnerabilities.

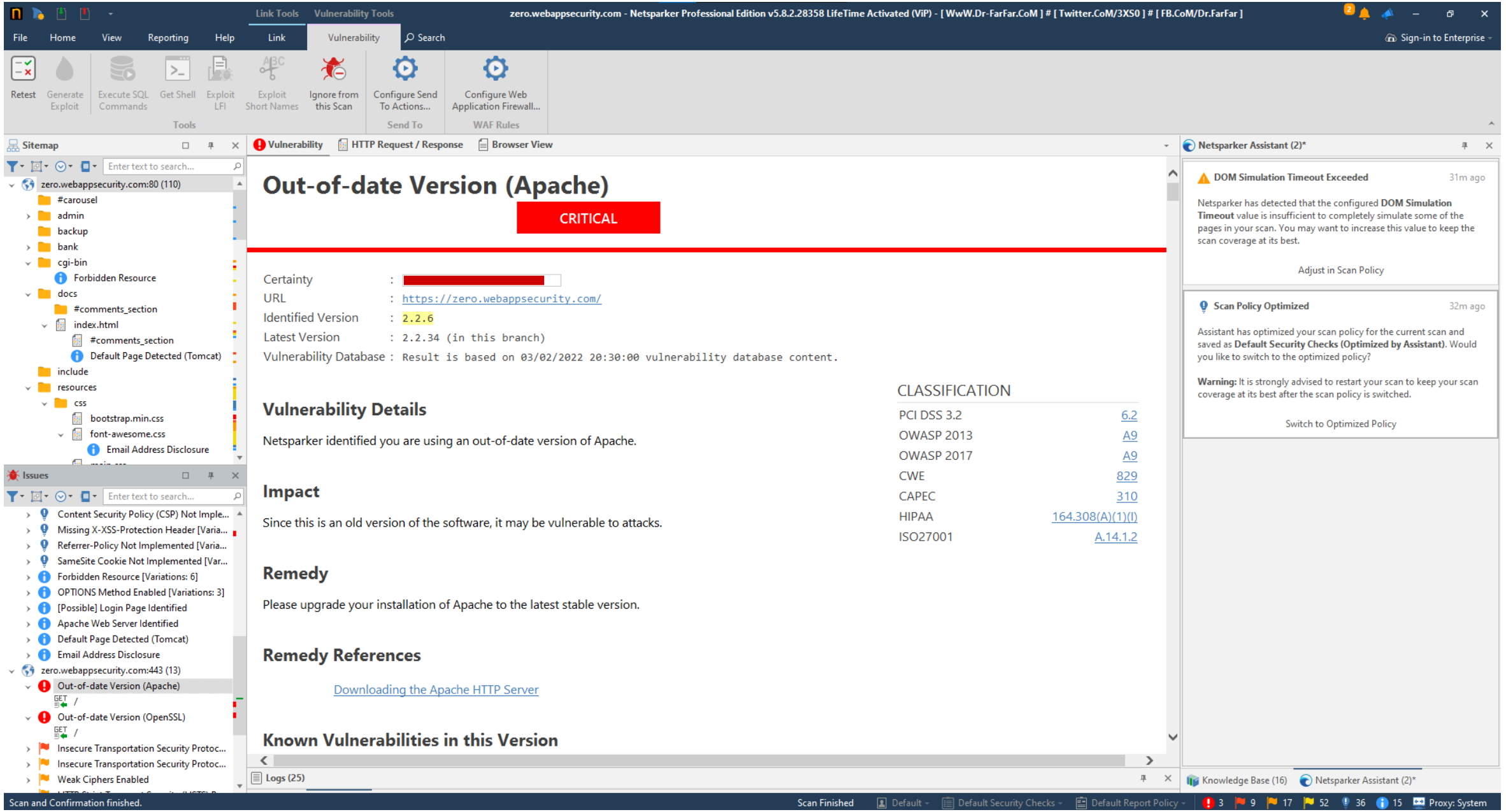
No matter if they are taught to you or not. Now just choose any 1 amongst that 3 and write a report in your own language. If you are using Netsparker you can use the report already generated by software but make sure you do not have to copy it. You have to then submit the report generated by you.

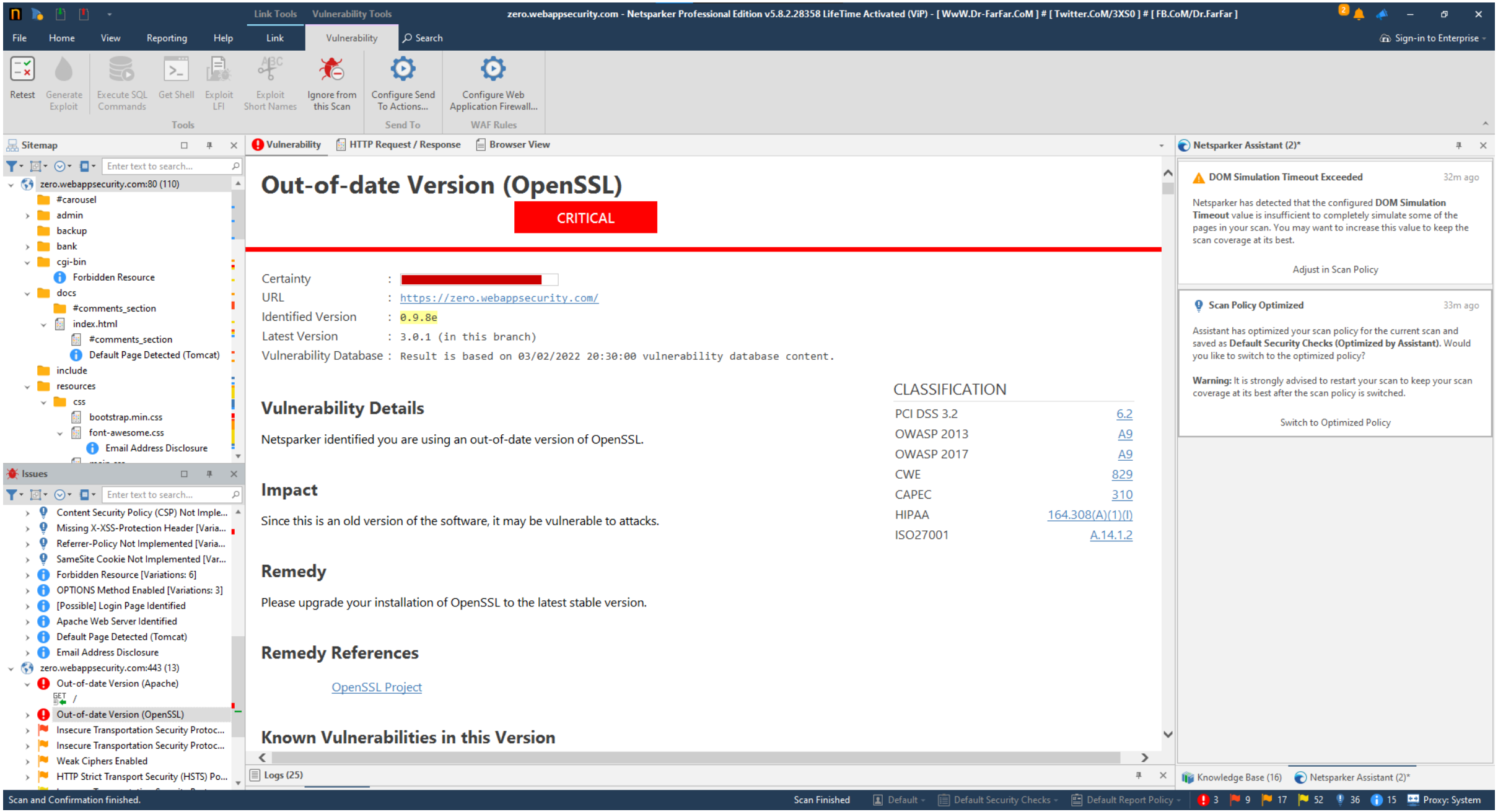

Netsparker Professional Edition v5.8.2.28358 LifeTime Activated (ViP) - [WwW.Dr-FarFar.CoM] # [Twitter.CoM/3XS0] # [FB.CoM/Dr.FarFar]
File
Home
View
Reporting
Help
Search
Sign-in to Enterprise
New
Schedule
Incremental
Schedule Incremental
New Instance
Import
Export
Export to Netsparker Enterprise
Scan Policy Editor
Report Policy Editor
Options
Start Scan
Scan Session
Tools
Welcome
Netsparker Logo - Web Application Security Scanner
Updates
We release an update for Netsparker Standard every month. Updates include new
Netsparker Scanners Release Announcements
Netsparker Standard Change Log
Web Application Security Blog
DAST, IAST, SCA: Deeper coverage in a single scan
The cutting-edge conundrum: Why federal agencies can't compromise on secu
How Netsparker can help with AppSec compliance
Netsparker Enterprise achieves WCAG 2.1 accessibility compliance
AppSec best practices for security that sticks
Support and Resources
Should you have any queries please do not hesitate to get in touch with us.
Support
Videos
Start a New Website or Web Service Scan
Target Website or Web Service URL
http://zero.webappsecurity.com/
Default
Options
Scan Settings
General
Scope
Additional Websites
Imported Links
URL Rewrite
Pre-request Scripts
Authentication
Form
Basic, NTLM/Kerberos
Header
Client Certificate
Smart Card
OAuth2
Manual
Form Authentication
Enabled
Custom Script...
Login Form URL:
Personas:
Act...
Username
Password
OTP
Interactive login (Check this for CAPTCHA)
Override Target URL with authenticated page
Detect authentication tokens
Verify Login & Logout...
Start Scan
Cancel
Follow Us on Social Media
Follow us on any of our social media channels to keep yourself up to date with what is happening in the world of web application security and Netsparker
Netsparker Professional Edition LifeTime Activated (ViP) is Ready To Go ! [WwW.Dr-FarFar.CoM] # [Twitter.CoM/3XS0] # [FaceBook.CoM/Dr.FarFar]
Proxy: System


zero.webappsecurity.com - Netsparker Professional Edition v5.8.2.28358 LifeTime Activated (ViP) - [WwW.Dr-FarFar.CoM] # [Twitter.CoM/3XS0] # [FB.CoM/Dr.FarFar]
File
Home
View
Reporting
Help
Search
Sign-in to Enterprise
New
Schedule
Incremental
Schedule Incremental
New Instance
Start Scan
Import
Export
Export to Netsparker Enterprise
Scan Session
Scan Policy Editor
Report Policy Editor
Options
Tools
Welcome
Netsparker Logo - Web Application Security Scanner
Updates
We release an update for Netsparker Standard every month. Updates include new securi
Netsparker Scanners Release Announcements
Netsparker Standard Change Log
Website Checker
Allocate
Reachable
Website
http://zero.webappsecurity.com/
Selected web sites will be allocated from your active license(s).
Allocate
Cancel
Web Application Security Blog
DAST, IAST, SCA: Deeper coverage in a single scan
The cutting-edge conundrum: Why federal agencies can't compromise on security
How Netsparker can help with AppSec compliance
Netsparker Enterprise achieves WCAG 2.1 accessibility compliance
AppSec best practices for security that sticks
Support and Resources
Should you have any queries please do not hesitate to get in touch with us. Below are also some useful links you can refer to:
Support
Videos
Follow Us on Social Media
Follow us on any of our social media channels to keep yourself up to date with what is happening in the world of web application security and Netsparker
Scan hasn't started yet
Default
Default Security Checks
Default Report Policy
Proxy: System


Scan Tools
zero.webappsecurity.com - Netsparker Professional Edition v5.8.2.28358 LifeTime Activated (ViP) - [WwW.Dr-FarFar.CoM] # [Twitter.CoM/3XS0] # [FB.CoM/Dr.FarFar]
File
Home
View
Reporting
Help
Scan
Search
Sign-in to Enterprise
Pause
Skip
Start Proxy
Enter Links
Import Links from File
Control
Tools
Import Links
Sitemap
Enter text to search...
zero.webappsecurity.com:80 (108)
#carousel
admin
backup
bank
cgi-bin
Forbidden Resource
docs
#comments_section
index.html
#comments_section
Default Page Detected (Tomc...
include
resources
css
bootstrap.min.css
font-awesome.css
Email Address Disclosure
Issues
Enter text to search...
zero.webappsecurity.com:80 (100)
Out-of-date Version (Tomcat)
Password Transmitted over HTTP [Var...
Apache Server-Status Detected
Out-of-date Version (jQuery UI Dialog...
Out-of-date Version (jQuery) [Variatio...
[Possible] Backup File Disclosure [Vari...
[Possible] Cross-site Request Forgery ...
[Possible] Cross-site Request Forgery ...
[Possible] Phishing by Navigating Bro...
Missing X-Frame-Options Header [Va...
Version Disclosure (Apache Coyote)
Version Disclosure (Tomcat)
Misconfigured Access-Control-Allow...
Content Security Policy (CSP) Not Im...
Missing X-XSS-Protection Header [Va...
Referrer-Policy Not Implemented [Var...
SameSite Cookie Not Implemented [V...
Welcome
Netsparker Logo - Web Application Security Scanner
Updates
We release an update for Netsparker Standard every month. Updates include new security checks, new features and bug fixes. Here are some useful links:
Netsparker Scanners Release Announcements
Netsparker Standard Change Log
Web Application Security Blog
DAST, IAST, SCA: Deeper coverage in a single scan
Activity
Method
Target
Parameter
Duration
Current Activity
Overall Activity
Status
Attacking [20]
POST http://zero.webappsecurity.com/se... submit 1 s [12/40] Open (Oracle) [1/34] SQL Injection (Error Based) Requesting
POST http://zero.webappsecurity.com/se... submit 1 s [5/29] trace.axd (6) [28/34] Server-Side Request Forgery (Patt... Requesting
POST http://zero.webappsecurity.com/se... subject 1 s [1/11] RFI Classic [8/34] Remote File Inclusion Requesting
GET http://zero.webappsecurity.com/ (Full URL) 1 s [67/71] qdPM [14/34] Web App Fingerprint Analyzing
POST http://zero.webappsecurity.com/se... submit 1 s [2/7] Image Injection - onerror - Href Ste... [32/34] Cross-site Scripting (Blind) Requesting
POST http://zero.webappsecurity.com/se... submit 1 s [17/25] (Linux) SSI Directive [5/34] Command Injection Requesting
POST http://zero.webappsecurity.com/se... email 1 s [2/5] SSTI (Node.js Pug (Jade), Ruby Slim) [10/34] Server-Side Template Injection Requesting
POST http://zero.webappsecurity.com/se... submit 1 s [4/30] MSSQL - xp_dirtree - Stacked - Stri... [30/34] SQL Injection (Out of Band) Requesting
POST http://zero.webappsecurity.com/se... submit 1 s [16/45] PHP - RCE with PCRE 'e' Modifier [9/34] Code Evaluation Requesting
POST http://zero.webappsecurity.com/se... submit 1 s [17/54] Short XSS [4/34] Cross-site Scripting Requesting
GET http://zero.webappsecurity.com/se... searchTerm 37 s [1/1] Dynamically Generated Patterns [2/34] SQL Injection (Boolean) Analyzing
POST http://zero.webappsecurity.com/se... comment 1 s [3/3] HTTP Request (Capture UserAgent) [29/34] Server-Side Request Forgery (DNS) Requesting
POST http://zero.webappsecurity.com/se... email 1 s [2/6] Set Cookie with URL Start [11/34] HTTP Header Injection Requesting
POST http://zero.webappsecurity.com/se... submit 1 s [14/58] Table (MySQL) [3/34] SQL Injection (Blind) Requesting
POST http://zero.webappsecurity.com/se... name 1 s [2/4] MyFaces Attack [13/34] Expression Language Injection Requesting
Activity
Progress
Logs (15)
Netsparker Assistant (2)*
DOM Simulation Timeout Exceeded
now
Netsparker has detected that the configured DOM Simulation Timeout value is insufficient to completely simulate some of the pages in your scan. You may want to increase this value to keep the scan coverage at its best.
Adjust in Scan Policy
Scan Policy Optimized
now
Assistant has optimized your scan policy for the current scan and saved as Default Security Checks (Optimized by Assistant). Would you like to switch to the optimized policy?
Warning: It is strongly advised to restart your scan to keep your scan coverage at its best after the scan policy is switched.
Switch to Optimized Policy
Knowledge Base (14)
Netsparker Assistant (2)*
Crawl and Attack phase started.
Crawling & Attacking (2/3) 8%
Default
Default Security Checks
Default Report Policy
3
3
15
47
36
9
Proxy: System


zero.webappsecurity.com - Netsparker Professional Edition v5.8.2.28358 LifeTime Activated (ViP) - [WwW.Dr-FarFar.CoM] # [Twitter.CoM/3XS0] # [FB.CoM/Dr.FarFar]
Link Tools
Vulnerability Tools
File
Home
View
Reporting
Help
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
Sitemap
Enter text to search...
zero.webappsecurity.com:80 (110)
#carousel
admin
backup
bank
cgi-bin
Forbidden Resource
docs
#comments_section
index.html
#comments_section
Default Page Detected (Tomcat)
include
resources
css
bootstrap.min.css
font-awesome.css
Email Address Disclosure
Issues
Enter text to search...
zero.webappsecurity.com:80 (119)
Out-of-date Version (Tomcat)
/resources/js/
Cross-site Scripting
Cross-site Scripting via Remote File Incl...
Password Transmitted over HTTP [Variat...
[Possible] Server-Side Request Forgery (...
[Probable] Local File Inclusion
Frame Injection
[Possible] Server-Side Request Forgery
Apache Server-Status Detected
Out-of-date Version (jQuery UI Dialog)
Out-of-date Version (jQuery) [Variations...
[Possible] Backup File Disclosure [Variati...
[Possible] Cross-site Request Forgery [V...
[Possible] Cross-site Request Forgery in ...
[Possible] Phishing by Navigating Brow...
Missing X-Frame-Options Header [Varia...
Vulnerability
HTTP Request / Response
Browser View
Out-of-date Version (Tomcat)
CRITICAL
Certainty :
URL : http://zero.webappsecurity.com/resources/js/
Identified Version : 7.0.70
Latest Version : 10.0.17 (in this branch)
Vulnerability Database : Result is based on 03/02/2022 20:30:00 vulnerability database content.
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 protection provided by the LockOut Realm. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.
CLASSIFICATION
PCI DSS 3.2 6.2
OWASP 2013 A9
OWASP 2017 A9
CWE 829
CAPEC 310
HIPAA 164.308(A)(1)(I)
ISO27001 A.14.1.2
Logs (25)
Netsparker Assistant (2)*
DOM Simulation Timeout Exceeded
26m ago
Netsparker has detected that the configured DOM Simulation Timeout value is insufficient to completely simulate some of the pages in your scan. You may want to increase this value to keep the scan coverage at its best.
Adjust in Scan Policy
Scan Policy Optimized
27m ago
Assistant has optimized your scan policy for the current scan and saved as Default Security Checks (Optimized by Assistant). Would you like to switch to the optimized policy?
Warning: It is strongly advised to restart your scan to keep your scan coverage at its best after the scan policy is switched.
Switch to Optimized Policy
Knowledge Base (16)
Netsparker Assistant (2)*
Scan and Confirmation finished.
Scan Finished
Default
Default Security Checks
Default Report Policy
3
9
17
52
36
15
Proxy: System


zero.webappsecurity.com - Netsparker Professional Edition v5.8.2.28358 LifeTime Activated (ViP) - [WwW.Dr-FarFar.CoM] # [Twitter.CoM/3XS0] # [FB.CoM/Dr.FarFar]
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 03/02/2022 20:30:00 vulnerability database content.
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
CLASSIFICATION
PCI DSS 3.2 6.2
OWASP 2013 A9
OWASP 2017 A9
CWE 829
CAPEC 310
HIPAA 164.308(A)(1)(I)
ISO27001 A.14.1.2
DOM Simulation Timeout Exceeded
Netsparker has detected that the configured DOM Simulation Timeout value is insufficient to completely simulate some of the pages in your scan. You may want to increase this value to keep the scan coverage at its best.
Adjust in Scan Policy
Scan Policy Optimized
Assistant has optimized your scan policy for the current scan and saved as Default Security Checks (Optimized by Assistant). Would you like to switch to the optimized policy?
Warning: It is strongly advised to restart your scan to keep your scan coverage at its best after the scan policy is switched.
Switch to Optimized Policy
Scan and Confirmation finished.
Scan Finished


zero.webappsecurity.com - Netsparker Professional Edition v5.8.2.28358 LifeTime Activated (ViP) - [WwW.Dr-FarFar.CoM] # [Twitter.CoM/3XS0] # [FB.CoM/Dr.FarFar]
Link Tools
Vulnerability Tools
File
Home
View
Reporting
Help
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
Sitemap
Enter text to search...
zero.webappsecurity.com:80 (110)
#carousel
admin
backup
bank
cgi-bin
Forbidden Resource
docs
#comments_section
index.html
#comments_section
Default Page Detected (Tomcat)
include
resources
css
bootstrap.min.css
font-awesome.css
Email Address Disclosure
Issues
Content Security Policy (CSP) Not Imple...
Missing X-XSS-Protection Header [Varia...
Referrer-Policy Not Implemented [Varia...
SameSite Cookie Not Implemented [Var...
Forbidden Resource [Variations: 6]
OPTIONS Method Enabled [Variations: 3]
[Possible] Login Page Identified
Apache Web Server Identified
Default Page Detected (Tomcat)
Email Address Disclosure
zero.webappsecurity.com:443 (13)
Out-of-date Version (Apache)
GET /
Out-of-date Version (OpenSSL)
Insecure Transportation Security Protoc...
Insecure Transportation Security Protoc...
Weak Ciphers Enabled
HTTP Strict Transport Security (HSTS) Po...
Vulnerability
HTTP Request / Response
Browser View
Out-of-date Version (OpenSSL)
CRITICAL
Certainty :
URL : https://zero.webappsecurity.com/
Identified Version : 0.9.8e
Latest Version : 3.0.1 (in this branch)
Vulnerability Database : Result is based on 03/02/2022 20:30:00 vulnerability database content.
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
CLASSIFICATION
PCI DSS 3.2 6.2
OWASP 2013 A9
OWASP 2017 A9
CWE 829
CAPEC 310
HIPAA 164.308(A)(1)(I)
ISO27001 A.14.1.2
Logs (25)
Netsparker Assistant (2)*
DOM Simulation Timeout Exceeded
32m ago
Netsparker has detected that the configured DOM Simulation Timeout value is insufficient to completely simulate some of the pages in your scan. You may want to increase this value to keep the scan coverage at its best.
Adjust in Scan Policy
Scan Policy Optimized
33m ago
Assistant has optimized your scan policy for the current scan and saved as Default Security Checks (Optimized by Assistant). Would you like to switch to the optimized policy?
Warning: It is strongly advised to restart your scan to keep your scan coverage at its best after the scan policy is switched.
Switch to Optimized Policy
Knowledge Base (16)
Netsparker Assistant (2)*
Scan and Confirmation finished.
Scan Finished
Default
Default Security Checks
Default Report Policy
3
9
17
52
36
15
Proxy: System