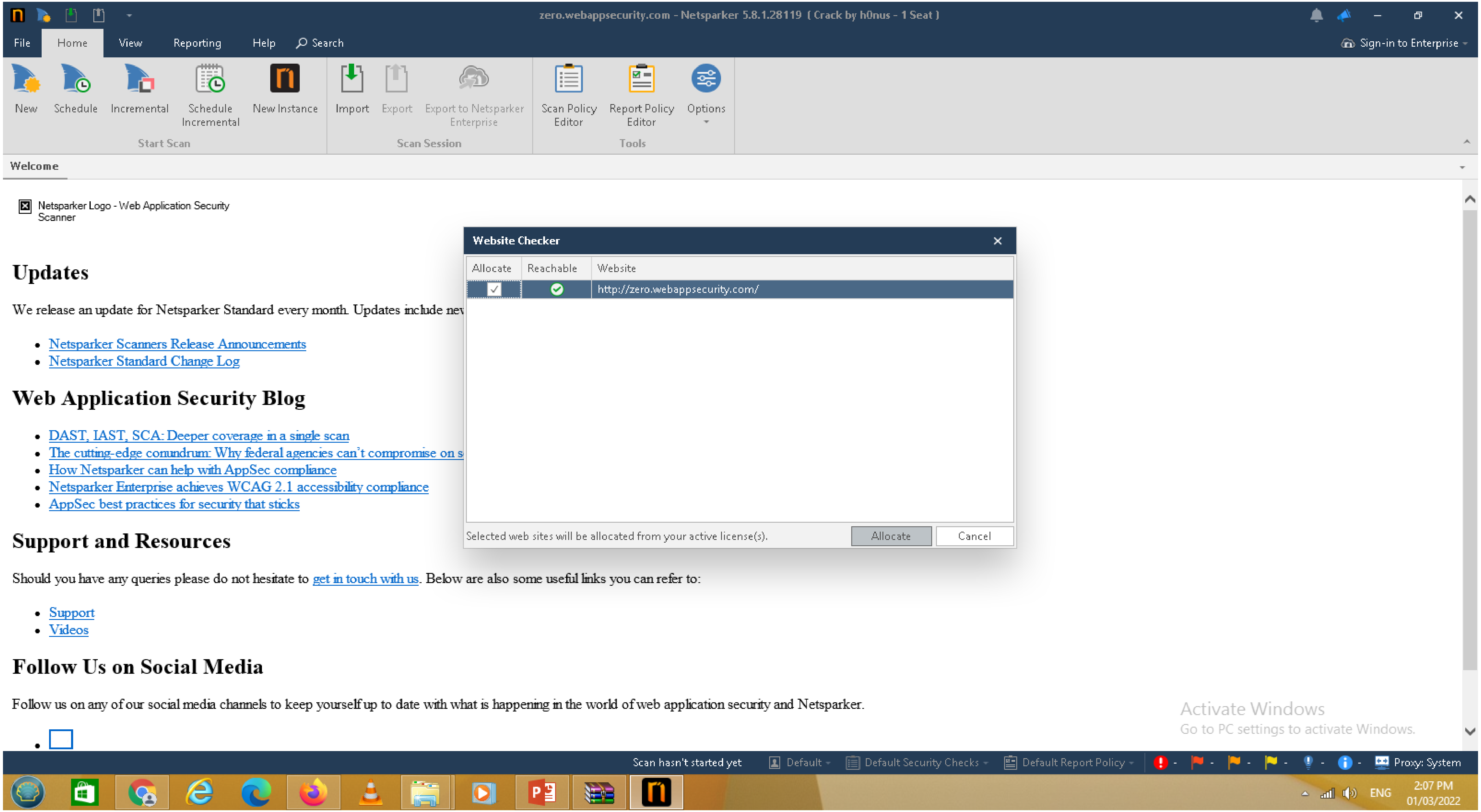
Project 2



Allocate	Reachable	Website
☑	✓	http://zero.webappsecurity.com/

Selected web sites will be allocated from your active license(s).

Updates

We release an update for Netsparker Standard every month. Updates include nev

- 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 s
- How Netsparker can help with AppSec compliance
- Netsparker Enterprise achieves WCAG 2.1 accessibility compliance
- AppSec best practices for security that sticks

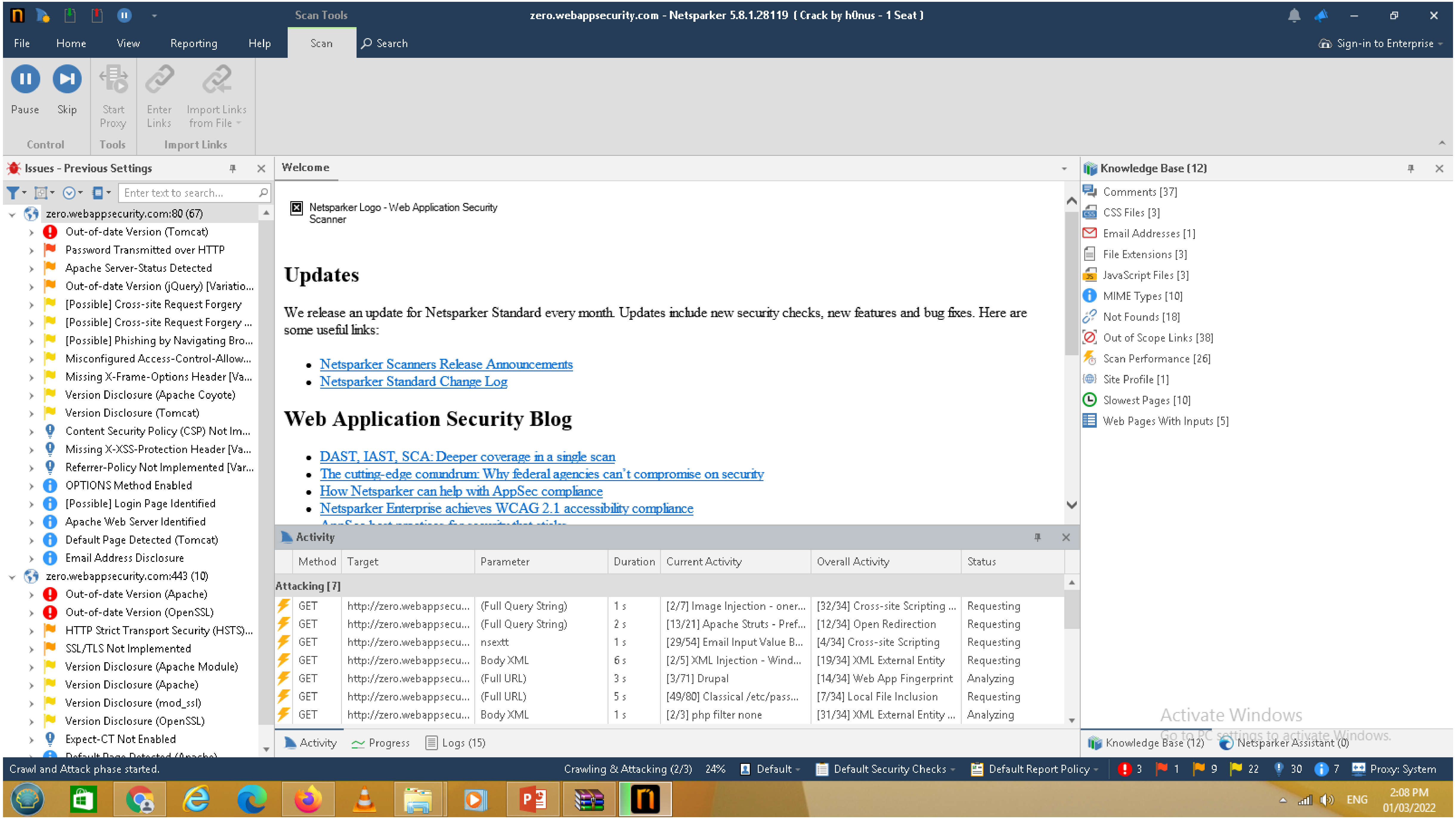
Support and Resources

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.



zero.webappsecurity.com:80 (67)
- Out-of-date Version (Tomcat)
- Password Transmitted over HTTP
- Apache Server-Status Detected
- Out-of-date Version (jQuery) [Variatio...
- [Possible] Cross-site Request Forgery
- [Possible] Cross-site Request Forgery ...
- [Possible] Phishing by Navigating Bro...
- Misconfigured Access-Control-Allow...
- Missing X-Frame-Options Header [Va...
- Version Disclosure (Apache Coyote)
- Version Disclosure (Tomcat)
- Content Security Policy (CSP) Not Im...
- Missing X-XSS-Protection Header [Va...
- Referrer-Policy Not Implemented [Var...
- OPTIONS Method Enabled
- [Possible] Login Page Identified
- Apache Web Server Identified
- Default Page Detected (Tomcat)
- Email Address Disclosure

zero.webappsecurity.com:443 (10)
- Out-of-date Version (Apache)
- Out-of-date Version (OpenSSL)
- HTTP Strict Transport Security (HSTS)...
- SSL/TLS Not Implemented
- Version Disclosure (Apache Module)
- Version Disclosure (Apache)
- Version Disclosure (mod_ssl)
- Version Disclosure (OpenSSL)
- Expect-CT Not Enabled
- Default Page Detected (Apache)

☒ 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

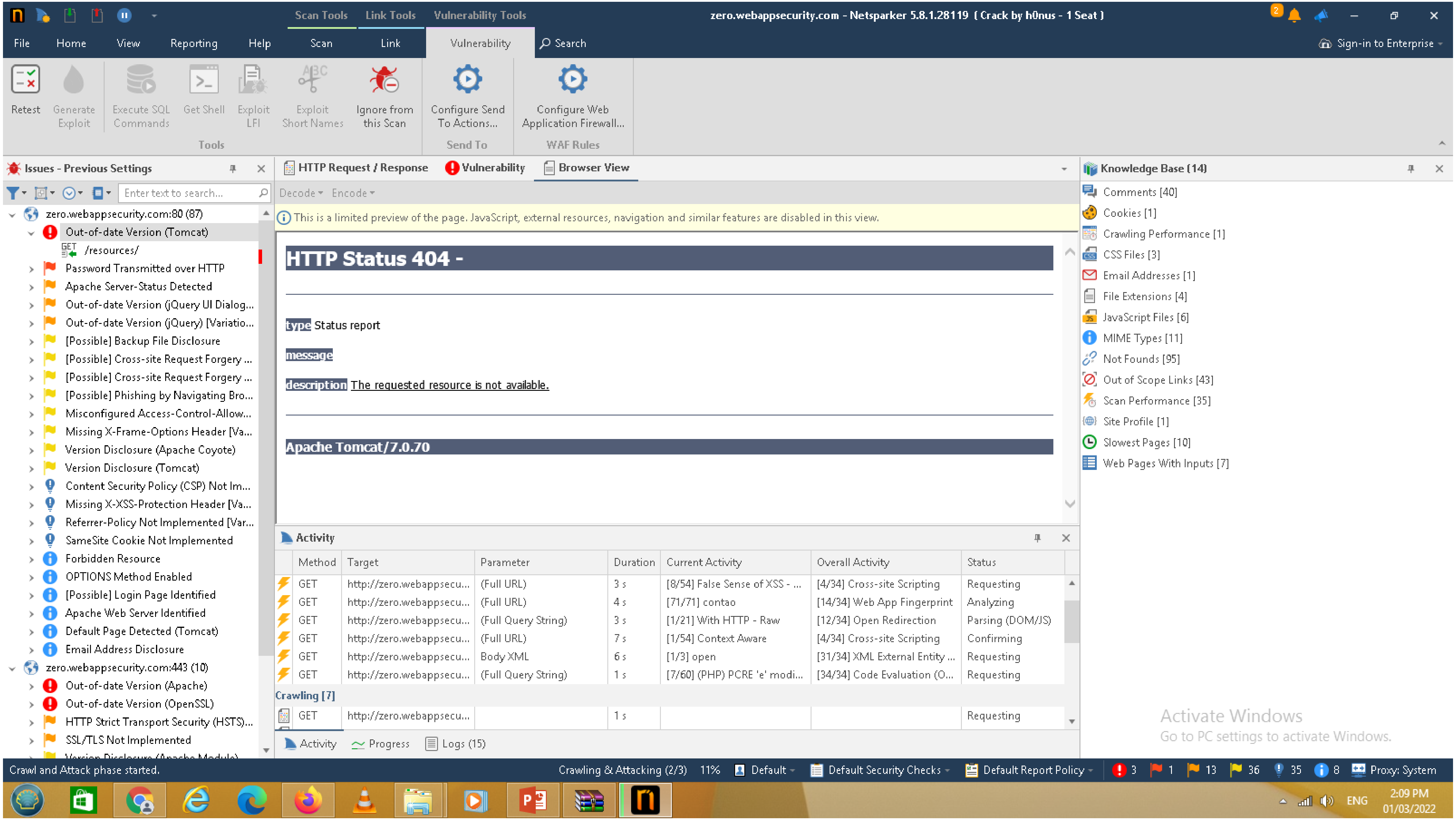
- DAST, IAST, SCA: Deeper coverage in a single scan
- The cutting-edge conundrum: Why federal agencies can't compromise on security
- How Netsparker can help with AppSec compliance
- Netsparker Enterprise achieves WCAG 2.1 accessibility compliance
- AppSec best practices for security that sticks

Comments [37]
CSS Files [3]
Email Addresses [1]
File Extensions [3]
JavaScript Files [3]
MIME Types [10]
Not Founds [18]
Out of Scope Links [38]
Scan Performance [26]
Site Profile [1]
Slowest Pages [10]
Web Pages With Inputs [5]

Attacking [7]

Method	Target	Parameter	Duration	Current Activity	Overall Activity	Status
GET	http://zero.webappsecu...	(Full Query String)	1 s	[2/7] Image Injection - oner...	[32/34] Cross-site Scripting ...	Requesting
GET	http://zero.webappsecu...	(Full Query String)	2 s	[13/21] Apache Struts - Pref...	[12/34] Open Redirection	Requesting
GET	http://zero.webappsecu...	nsextt	1 s	[29/54] Email Input Value B...	[4/34] Cross-site Scripting	Requesting
GET	http://zero.webappsecu...	Body XML	6 s	[2/5] XML Injection - Wind...	[19/34] XML External Entity	Requesting
GET	http://zero.webappsecu...	(Full URL)	3 s	[3/71] Drupal	[14/34] Web App Fingerprint	Analyzing
GET	http://zero.webappsecu...	(Full URL)	5 s	[49/80] Classical /etc/pass...	[7/34] Local File Inclusion	Requesting
GET	http://zero.webappsecu...	Body XML	1 s	[2/3] php filter none	[31/34] XML External Entity ...	Analyzing

Crawl and Attack phase started. Crawling & Attacking (2/3) 24% Default Default Security Checks Default Report Policy 3 1 9 22 30 7 Proxy: System



Issues - Previous Settings

- zero.webappsecurity.com:80 (87)
  - Out-of-date Version (Tomcat)
    - GET /resources/
  - Password Transmitted over HTTP
  - Apache Server-Status Detected
  - Out-of-date Version (jQuery UI Dialog...
  - Out-of-date Version (jQuery) [Variatio...
  - [Possible] Backup File Disclosure
  - [Possible] Cross-site Request Forgery ...
  - [Possible] Cross-site Request Forgery ...
  - [Possible] Phishing by Navigating Bro...
  - Misconfigured Access-Control-Allow...
  - Missing X-Frame-Options Header [Va...
  - Version Disclosure (Apache Coyote)
  - Version Disclosure (Tomcat)
  - Content Security Policy (CSP) Not Im...
  - Missing X-XSS-Protection Header [Va...
  - Referrer-Policy Not Implemented [Var...
  - SameSite Cookie Not Implemented
  - Forbidden Resource
  - OPTIONS Method Enabled
  - [Possible] Login Page Identified
  - Apache Web Server Identified
  - Default Page Detected (Tomcat)
  - Email Address Disclosure
- zero.webappsecurity.com:443 (10)
  - Out-of-date Version (Apache)
  - Out-of-date Version (OpenSSL)
  - HTTP Strict Transport Security (HSTS)...
  - SSL/TLS Not Implemented
  - Version Disclosure (Apache Module)

This is a limited preview of the page. JavaScript, external resources, navigation and similar features are disabled in this view.

HTTP Status 404 -

type Status report

message

description The requested resource is not available.

Apache Tomcat/7.0.70

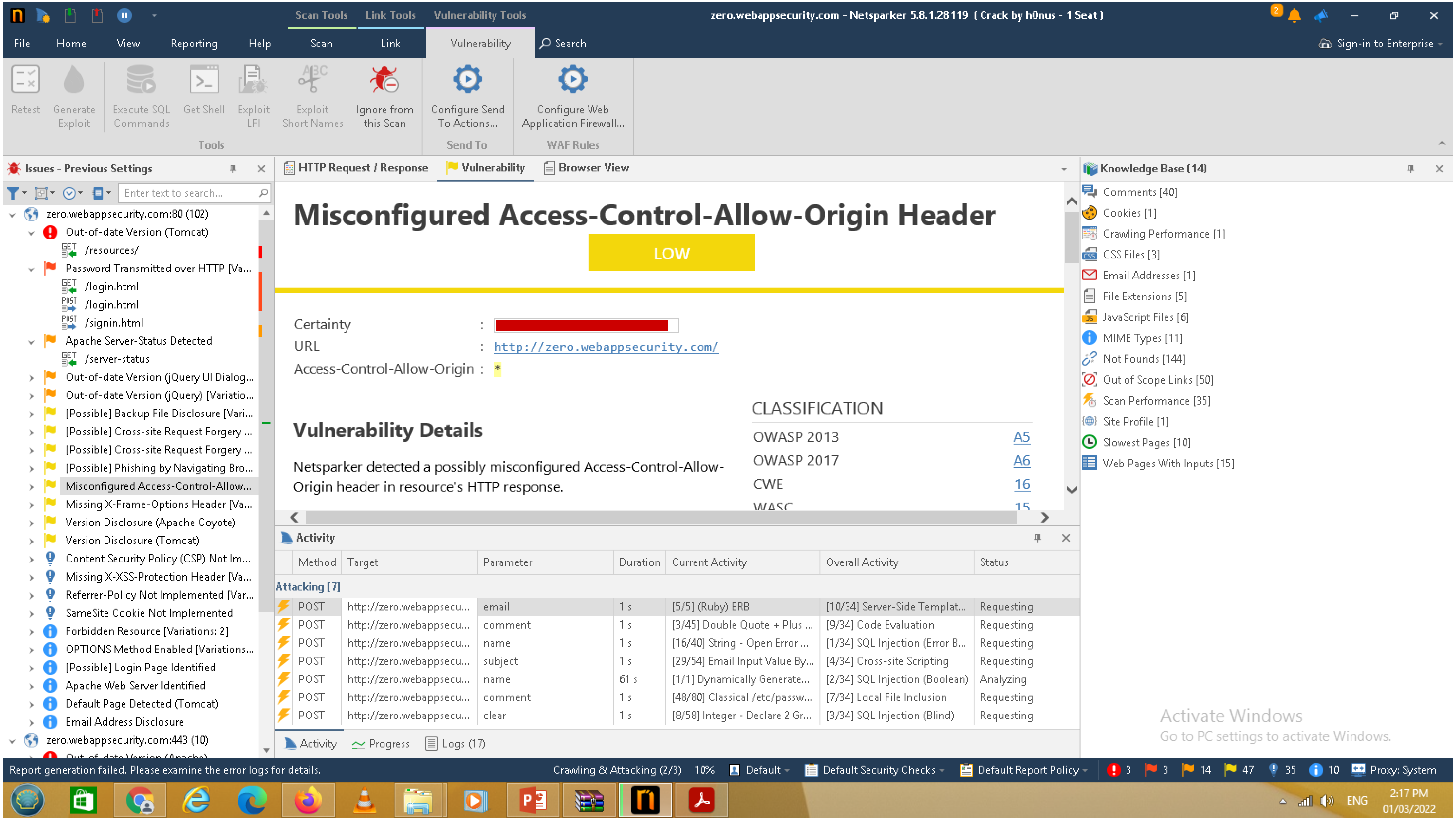
Activity

Method	Target	Parameter	Duration	Current Activity	Overall Activity	Status
GET	http://zero.webappsecu...	(Full URL)	3 s	[8/54] False Sense of XSS - ...	[4/34] Cross-site Scripting	Requesting
GET	http://zero.webappsecu...	(Full URL)	4 s	[71/71] contao	[14/34] Web App Fingerprint	Analyzing
GET	http://zero.webappsecu...	(Full Query String)	3 s	[1/21] With HTTP - Raw	[12/34] Open Redirection	Parsing (DOM/JS)
GET	http://zero.webappsecu...	(Full URL)	7 s	[1/54] Context Aware	[4/34] Cross-site Scripting	Confirming
GET	http://zero.webappsecu...	Body XML	6 s	[1/3] open	[31/34] XML External Entity ...	Requesting
GET	http://zero.webappsecu...	(Full Query String)	1 s	[7/60] (PHP) PCRE 'e' modi...	[34/34] Code Evaluation (O...	Requesting
Crawling [7]						
GET	http://zero.webappsecu...		1 s			Requesting

Knowledge Base (14)

- Comments [40]
- Cookies [1]
- Crawling Performance [1]
- CSS Files [3]
- Email Addresses [1]
- File Extensions [4]
- JavaScript Files [6]
- MIME Types [11]
- Not Founds [95]
- Out of Scope Links [43]
- Scan Performance [35]
- Site Profile [1]
- Slowest Pages [10]
- Web Pages With Inputs [7]

Crawl and Attack phase started. Crawling & Attacking (2/3) 11% Default Default Security Checks Default Report Policy 3 1 13 36 35 8 Proxy: System



zero.webappsecurity.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)

- zero.webappsecurity.com:80 (102)
  - Out-of-date Version (Tomcat)
    - GET /resources/
  - Password Transmitted over HTTP [Va...
    - GET /login.html
    - POST /login.html
    - POST /signin.html
  - Apache Server-Status Detected
    - GET /server-status
  - 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...
  - Misconfigured Access-Control-Allow...
  - Missing X-Frame-Options Header [Va...
  - Version Disclosure (Apache Coyote)
  - Version Disclosure (Tomcat)
  - Content Security Policy (CSP) Not Im...
  - Missing X-XSS-Protection Header [Va...
  - Referrer-Policy Not Implemented [Var...
  - SameSite Cookie Not Implemented
  - Forbidden Resource [Variations: 2]
  - OPTIONS Method Enabled [Variations...
  - [Possible] Login Page Identified
  - Apache Web Server Identified
  - Default Page Detected (Tomcat)
  - Email Address Disclosure
- zero.webappsecurity.com:443 (10)
  - Out-of-date Version (Apache)

Misconfigured Access-Control-Allow-Origin Header

LOW

Certainty :
URL : http://zero.webappsecurity.com/
Access-Control-Allow-Origin : *

Vulnerability Details

Netsparker detected a possibly misconfigured Access-Control-Allow-Origin header in resource's HTTP response.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15

Knowledge Base (14)

- Comments [40]
- Cookies [1]
- Crawling Performance [1]
- CSS Files [3]
- Email Addresses [1]
- File Extensions [5]
- JavaScript Files [6]
- MIME Types [11]
- Not Founds [144]
- Out of Scope Links [50]
- Scan Performance [35]
- Site Profile [1]
- Slowest Pages [10]
- Web Pages With Inputs [15]

Activity

Attacking [7]

Method	Target	Parameter	Duration	Current Activity	Overall Activity	Status
POST	http://zero.webappsecu...	email	1 s	[5/5] (Ruby) ERB	[10/34] Server-Side Templat...	Requesting
POST	http://zero.webappsecu...	comment	1 s	[3/45] Double Quote + Plus ...	[9/34] Code Evaluation	Requesting
POST	http://zero.webappsecu...	name	1 s	[16/40] String - Open Error ...	[1/34] SQL Injection (Error B...	Requesting
POST	http://zero.webappsecu...	subject	1 s	[29/54] Email Input Value By...	[4/34] Cross-site Scripting	Requesting
POST	http://zero.webappsecu...	name	61 s	[1/1] Dynamically Generate...	[2/34] SQL Injection (Boolean)	Analyzing
POST	http://zero.webappsecu...	comment	1 s	[48/80] Classical /etc/passw...	[7/34] Local File Inclusion	Requesting
POST	http://zero.webappsecu...	clear	1 s	[8/58] Integer - Declare 2 Gr...	[3/34] SQL Injection (Blind)	Requesting

Report generation failed. Please examine the error logs for details. Crawling & Attacking (2/3) 10% Default Default Security Checks Default Report Policy 3 3 14 47 35 10 Proxy: System

Vulnerability Details

Netsparker detected a possibly misconfigured Access-Control-Allow-Origin header in resource's HTTP response.

Cross-origin resource sharing (CORS) is a mechanism that allows resources on a web page to be requested outside the domain through XMLHttpRequest.

Unless this HTTP header is present, such "cross-domain" requests are forbidden by web browsers, per the same-origin security policy.

Impact

This is generally not appropriate when using the same-origin security policy. The only case where this is appropriate when using the same-origin policy is when a page or API response is considered completely public content and it is intended to be accessible to everyone.

Remedy

If this page is intended to be accessible to everyone, you don't need to take any action. Otherwise please follow the guidelines for different architectures below in order to set this header and permit outside domain.

Apache

- Add the following line inside either the <directory>, <location>, <files> or <virtualhost> sections of your server config (usually located in httpd.conf or apache.conf), or within a .htaccess file.`Header set Access-Control-Allow-Origin "domain"`

IIS6

1. Open Internet Information Service (IIS) Manager
2. Right click the site you want to enable CORS for and go to Properties
3. Change to the HTTP Headers tab
4. In the Custom HTTP headers section, click Add
5. Enter Access-Control-Allow-Origin as the header name
6. Enter domain as the header value

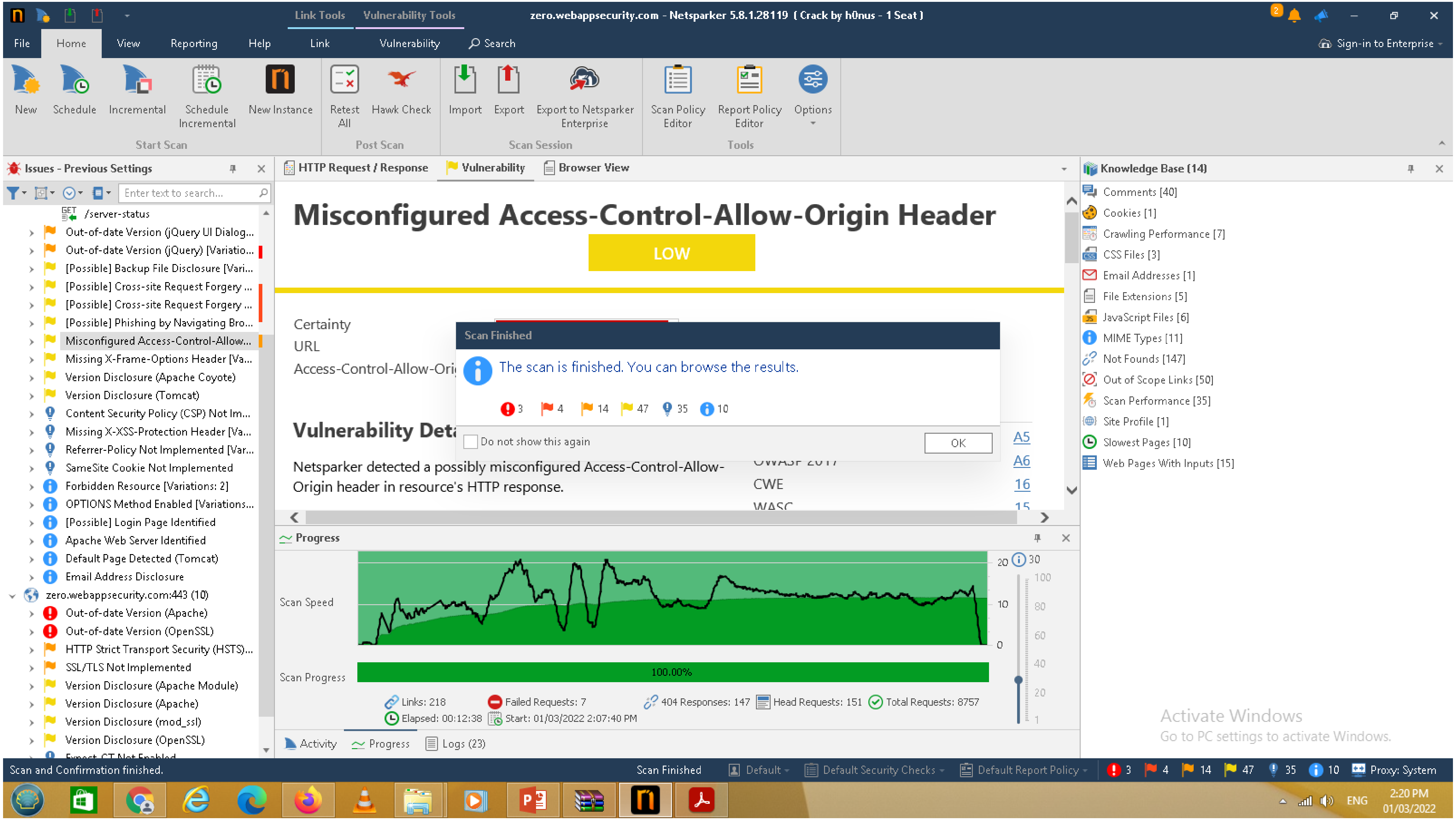
IIS7

- Merge the following xml into the web.config file at the root of your application or site:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration> <system.webserver> <httpprotocol> <customheaders> <add name="Access-Control-Allow-Origin" value="domain" /> </customheaders>
</httpprotocol> </system.webserver> </configuration>
```

ASP.NET

- If you don't have access to configure IIS, you can still add the header through ASP.NET by adding the following line to your source pages:`Response.AppendHeader("Access-Control-Allow-Origin", "domain");`



zero.webappsecurity.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)

GET /server-status
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...
Misconfigured Access-Control-Allow...
Missing X-Frame-Options Header [Va...
Version Disclosure (Apache Coyote)
Version Disclosure (Tomcat)
Content Security Policy (CSP) Not Im...
Missing X-XSS-Protection Header [Va...
Referrer-Policy Not Implemented [Var...
SameSite Cookie Not Implemented
Forbidden Resource [Variations: 2]
OPTIONS Method Enabled [Variations...
[Possible] Login Page Identified
Apache Web Server Identified
Default Page Detected (Tomcat)
Email Address Disclosure
zero.webappsecurity.com:443 (10)
Out-of-date Version (Apache)
Out-of-date Version (OpenSSL)
HTTP Strict Transport Security (HSTS)...
SSL/TLS Not Implemented
Version Disclosure (Apache Module)
Version Disclosure (Apache)
Version Disclosure (mod_ssl)
Version Disclosure (OpenSSL)
Expect-CT Not Enabled

Misconfigured Access-Control-Allow-Origin Header

LOW

Certainty
URL
Access-Control-Allow-Ori

Vulnerability Deta

Netsparker detected a possibly misconfigured Access-Control-Allow-Origin header in resource's HTTP response.

OWASP 2017 A5
A6
CWE 16
WASC 15

Scan Finished

The scan is finished. You can browse the results.

3 4 14 47 35 10

□ Do not show this again

Comments [40]
Cookies [1]
Crawling Performance [7]
CSS Files [3]
Email Addresses [1]
File Extensions [5]
JavaScript Files [6]
MIME Types [11]
Not Founds [147]
Out of Scope Links [50]
Scan Performance [35]
Site Profile [1]
Slowest Pages [10]
Web Pages With Inputs [15]

20 30 100 10 80 60 0 40 20 1

100.00%

Links: 218 Failed Requests: 7 404 Responses: 147 Head Requests: 151 Total Requests: 8757
Elapsed: 00:12:38 Start: 01/03/2022 2:07:40 PM

Activate Windows
Go to PC settings to activate Windows.

Scan and Confirmation finished. Scan Finished Default Default Security Checks Default Report Policy 3 4 14 47 35 10 Proxy: System

ENG 2:20 PM 01/03/2022