

ZAP_{by}
CheckmairX



Automated Scan



This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack: <http://testhtml5.vulnweb.com/>

Use traditional spider: ☒

Use ajax spider: If Modern with Firefox

 Attack Stop

Progress: Attack complete - see the Alerts tab for details of any issues found

History Search Alerts Output Spider AJAX Spider Active Scan +



Alerts (17)

- Absence of Anti-CSRF Tokens
- Content Security Policy (CSP) Header Not Set (3)
- Cross-Domain Misconfiguration
- HTTP Only Site
- **Missing Anti-clickjacking Header**
- Sub Resource Integrity Attribute Missing (Systemic)
- Cookie No HttpOnly Flag
- Cookie without SameSite Attribute
- Cross-Domain JavaScript Source File Inclusion (4)
- Server Leaks Version Information via "Server" HTTP Response
- Vulnerable JS Library
- X-Content-Type-Options Header Missing (Systemic)
- Authentication Request Identified
- Cookie Poisoning
- Information Disclosure - Suspicious Comments (2)
- Modern Web Application
- User Agent Fuzzer (2)

Source: Passive (10020 - Anti-clickjacking Header)

Alert Reference: 10020-1

Input Vector:

Description:

The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

Other Info: —

Solution: -

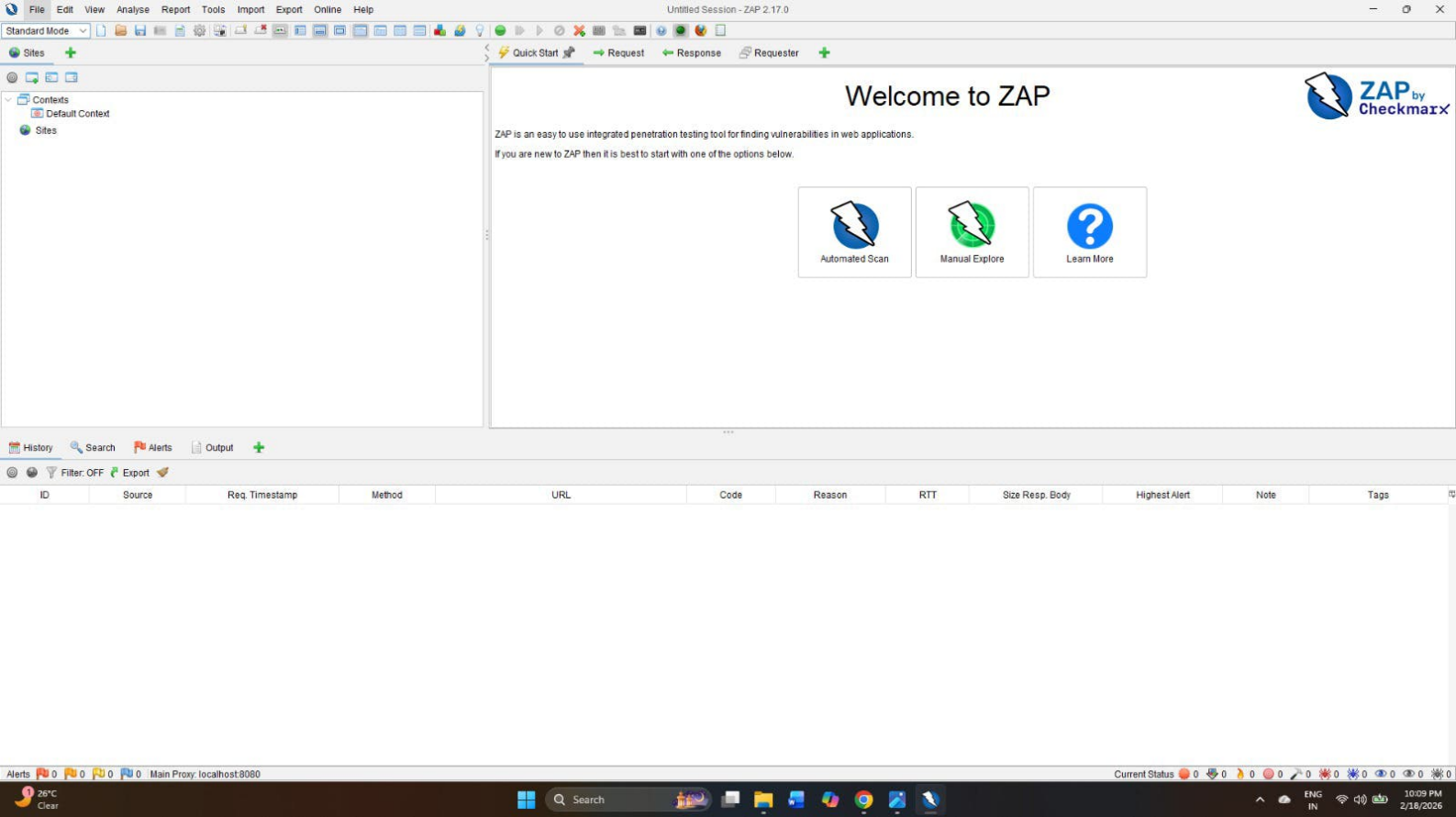
Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.





Reference:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options>

Alert Tags:



Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

Alerts  0  6  6  5 Main Proxy: localhost:8080

Contexts

Sites

✓  <http://re>



History

Sent Messages

Alerts 0

http://testhtml5.vulnweb.com Scan Progress							
Progress		Response Chart					
Host		http://testhtml5.vulnweb.com					
Analysed	Strength	Progress	Elapsed	Reqs	Alerts	Status	
Plugin			00:02:59.1	8			
Path Traversal	Medium		00:00.008	0	0	✓	
Remote File Inclusion	Medium		00:00.004	0	0	✓	
Source Code Disclosure - /WEB-INF Folder	Medium		00:00.873	3	0	✓	
Remote Code Execution - Shell Shock	Medium		00:00.871	0	0	✓	
Heartbleed OpenSSL Vulnerability	Medium		00:03.031	0	0	✓	
Source Code Disclosure - CVE-2012-1823	Medium		00:03.031	1	0	✓	
Remote Code Execution - CVE-2012-1823	Medium		00:00.561	2	0	✓	
External Redirect	Medium		00:00.004	0	0	✓	
Server Side Include	Medium		00:00.005	0	0	✓	
Cross Site Scripting (Reflected)	Medium		00:00.004	0	0	✓	
Cross Site Scripting (Persistent) - Prime	Medium		00:00.005	0	0	✓	
Cross Site Scripting (Persistent) - Spider	Medium		00:00.264	1	0	✓	
Cross Site Scripting (Persistent)	Medium		00:00.005	0	0	✓	
SQL Injection	Medium		00:00.003	0	0	✓	
SQL Injection - MySQL (Time Based)	Medium		00:00.004	0	0	✓	
SQL Injection - Hypersonic SQL (Time Based)	Medium		00:00.003	0	0	✓	
SQL Injection - Oracle (Time Based)	Medium		00:00.004	0	0	✓	
SQL Injection - PostgreSQL (Time Based)	Medium		00:00.003	0	0	✓	
Cross Site Scripting (DOM Based)	Medium		00:00.147	0	0	✗	
SQL Injection - MsSQL (Time Based)	Medium		00:00.003	0	0	✓	
Log4Shell	Medium		00:00.002	0	0	✗	
Spring4Shell	Medium		00:00.554	2	0	✓	
Remote Code Execution (Read2Shell)	Medium		00:00.358	1	0	✓	
Server Side Code Injection	Medium		00:00.357	0	0	✓	
Remote OS Command Injection	Medium		00:00.005	0	0	✓	
XPath Injection	Medium		00:00.003	0	0	✓	
XML External Entity Attack	Medium		00:00.002	0	0	✓	
Generic Padding Oracle	Medium		00:00.005	0	0	✓	
Cloud Metadata Potentially Exposed	Medium		00:17.550	0	0	✓	
Server Side Template Injection	Medium		00:17.546	0	0	✓	
Server Side Template Injection (Blind)	Medium		00:00.003	0	0	✓	
Remote OS Command Injection (Time Based)	Medium		00:00.002	0	0	✓	

Copy

Close

Time	URL	Response	Status	Time
12 PM	GET http://testhtml5.vulnweb.com/vswebapp/docs	404 NOT FOUND	297 ms	
12 PM	GET http://testhtml5.vulnweb.com/swagger-ui/index.html	404 NOT FOUND	259 ms	
12 PM	GET http://testhtml5.vulnweb.com/vopenapi.yaml	404 NOT FOUND	259 ms	
12 PM	GET http://testhtml5.vulnweb.com/swagger.yaml	404 NOT FOUND	350 ms	
12 PM	GET http://testhtml5.vulnweb.com/swagger/ui/index.html	404 NOT FOUND	289 ms	

[illegible]

History Search Alerts Output Spider AJAX Spider Active Scan

🔔 Current Scans: 0 URLs Found: 27 Nodes Added: 0 📄 Export

URLs	Added Nodes	Messages
------	-------------	----------

Alerts 0 6 6 5 Main Proxy: localhost:8080