



ZAP by
Checkmatrix



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 been given permission to test.

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

Use traditional spider:

Use ajax spider: If Modern with Firefox

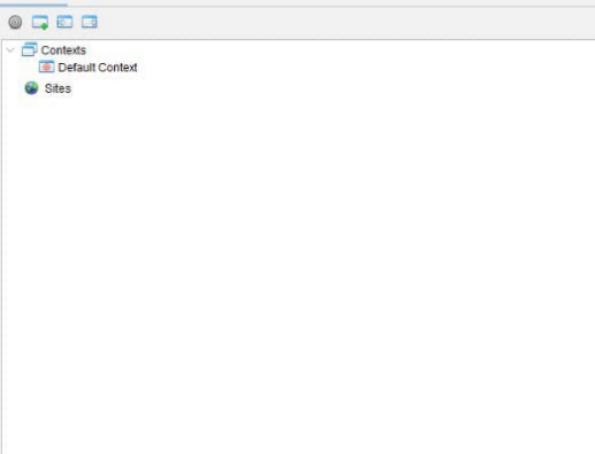
 Attack Stop

Progress: Attack complete - see the Alerts tab for details

 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)

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:	



Welcome to ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
If you are new to ZAP then it is best to start with one of the options below.



Automated Scan



Manual Explore

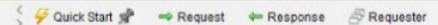


Learn More



Filter: OFF 

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
----	--------	----------------	--------	-----	------	--------	-----	-----------------	---------------	------	------



Sites

- Contexts
 - Default Context
- Sites
 - > https://testhtml5.vulnweb.com
 - > http://testhtml5.vulnweb.com

Automated Scan

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

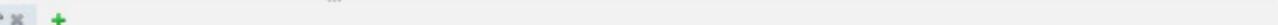
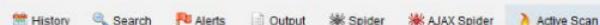
Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack:

Use traditional spider:

Use ajax spider: with

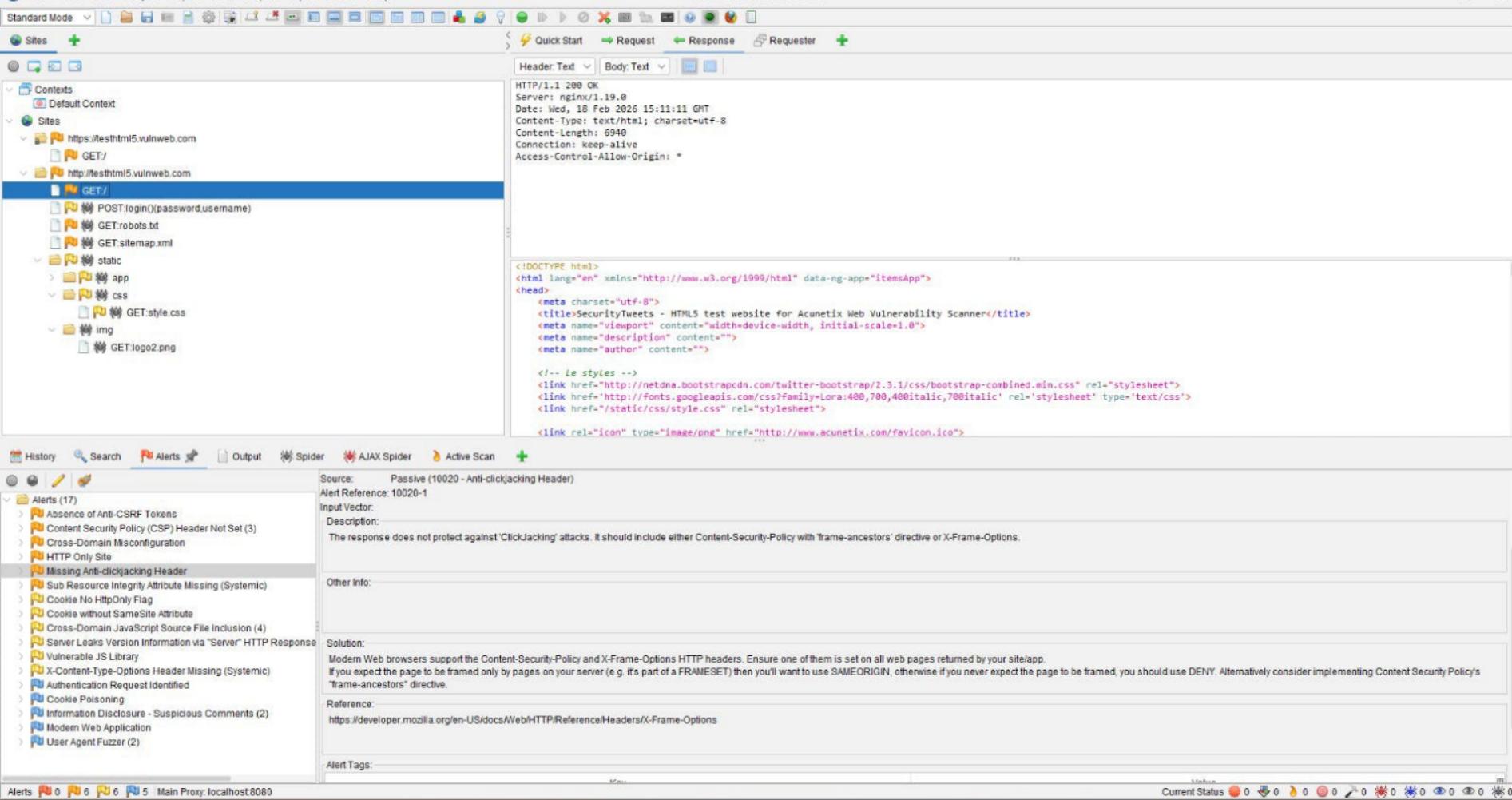
Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

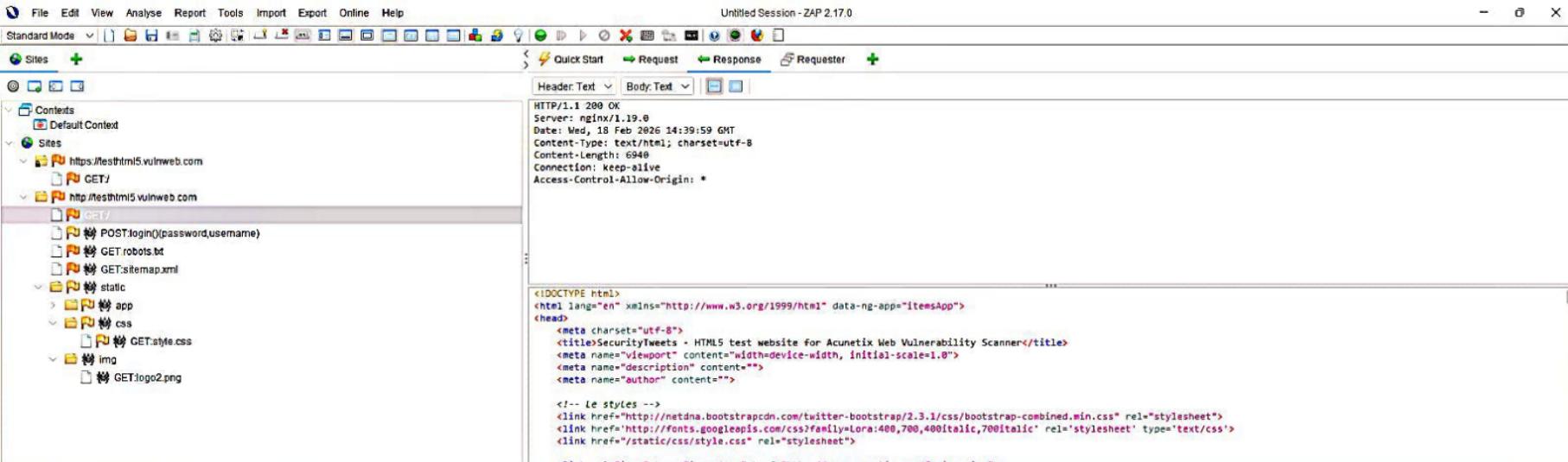


New Scan Progress: 2: http://testhtml5.vulnweb.com/

Sent Messages Filtered Messages

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
305	2/18/26, 8:21:22 PM	2/18/26, 8:21:23 PM	GET	http://testhtml5.vulnweb.com/static/87523943203276830	404	Not Found	300 ms	155 bytes	555 bytes
307	2/18/26, 8:21:23 PM	2/18/26, 8:21:23 PM	GET	http://testhtml5.vulnweb.com/static/app/34945280050430859...	404	Not Found	305 ms	155 bytes	555 bytes
309	2/18/26, 8:21:23 PM	2/18/26, 8:21:23 PM	GET	http://testhtml5.vulnweb.com/static/app/controllers/59708974...	404	Not Found	305 ms	155 bytes	555 bytes
311	2/18/26, 8:21:23 PM	2/18/26, 8:21:24 PM	GET	http://testhtml5.vulnweb.com/static/app/controllers/15236661844837...	404	Not Found	301 ms	155 bytes	555 bytes
313	2/18/26, 8:21:24 PM	2/18/26, 8:21:24 PM	GET	http://testhtml5.vulnweb.com/static/app/services/0778534611...	404	Not Found	259 ms	155 bytes	555 bytes
315	2/18/26, 8:21:24 PM	2/18/26, 8:21:24 PM	GET	http://testhtml5.vulnweb.com/static/css/81578103159636346...	404	Not Found	350 ms	155 bytes	555 bytes
317	2/18/26, 8:21:24 PM	2/18/26, 8:21:24 PM	GET	http://testhtml5.vulnweb.com/static/img/65702994404519321...	404	Not Found	323 ms	155 bytes	555 bytes
319	2/18/26, 8:21:24 PM	2/18/26, 8:21:25 PM	GET	http://testhtml5.vulnweb.com/WEB-INF/web.xml	404	NOT FOUND	382 ms	170 bytes	232 bytes
320	2/18/26, 8:21:25 PM	2/18/26, 8:21:25 PM	GET	http://testhtml5.vulnweb.com/WEB-INF/applicationContext.xml	404	NOT FOUND	306 ms	170 bytes	232 bytes
321	2/18/26, 8:21:25 PM	2/18/26, 8:21:25 PM	GET	http://testhtml5.vulnweb.com/WEB-INF/classes/3/2.class	404	NOT FOUND	294 ms	170 bytes	232 bytes
322	2/18/26, 8:21:25 PM	2/18/26, 8:21:26 PM	GET	http://testhtml5.vulnweb.com/?s	200	OK	258 ms	196 bytes	6,940 bytes
323	2/18/26, 8:21:28 PM	2/18/26, 8:21:29 PM	POST	http://testhtml5.vulnweb.com/?d+allow_url_include%3d1+d...	405	METHOD NOT ALLOWED	376 ms	206 bytes	178 bytes
324	2/18/26, 8:21:29 PM	2/18/26, 8:21:29 PM	POST	http://testhtml5.vulnweb.com/?d+allow_url_include%3d1+d...	405	METHOD NOT ALLOWED	258 ms	206 bytes	178 bytes
325	2/18/26, 8:21:29 PM	2/18/26, 8:21:29 PM	GET	http://testhtml5.vulnweb.com/	200	OK	332 ms	196 bytes	6,940 bytes
326	2/18/26, 8:21:30 PM	2/18/26, 8:21:30 PM	GET	http://testhtml5.vulnweb.com/?class.module.classLoader.Def...	200	OK	308 ms	196 bytes	6,940 bytes
327	2/18/26, 8:21:30 PM	2/18/26, 8:21:30 PM	POST	http://testhtml5.vulnweb.com/	405	METHOD NOT ALLOWED	260 ms	206 bytes	178 bytes
328	2/18/26, 8:21:30 PM	2/18/26, 8:21:31 PM	POST	http://testhtml5.vulnweb.com/	405	METHOD NOT ALLOWED	291 ms	206 bytes	178 bytes





URLs	Added Nodes	Messages	Processed	Method	URI	Flags
				GET	http://www.twitter.com/acunetix/	Out of Scope
				GET	http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/css/bootstrap-combined.min.css	Out of Scope
				GET	http://fonts.googleapis.com/css?family=Lora:400,700,400italic,700italic	Out of Scope
				GET	http://testhtml5.vulnweb.com/static/css/style.css	Out of Scope
				GET	http://www.acunetix.com/favicon.ico	Out of Scope
				GET	http://code.jquery.com/jquery-1.9.1.min.js	Out of Scope
				GET	http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstrap.min.js	Out of Scope
				GET	https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js	Out of Scope
				GET	http://testhtml5.vulnweb.com/static/app/app.js	Out of Scope
				GET	http://testhtml5.vulnweb.com/static/app/fbsesvar.js	Out of Scope
				GET	http://testhtml5.vulnweb.com/static/app/post.js	Out of Scope
				GET	http://testhtml5.vulnweb.com/static/app/controllers/controllers.js	Out of Scope
				GET	http://testhtml5.vulnweb.com/static/app/services/itemsService.js	Out of Scope
				GET	http://xss.s3.amazonaws.com/vad.js	Out of Scope
				GET	http://testhtml5.vulnweb.com/static/img/logo2.png	Out of Scope
				POST	http://testhtml5.vulnweb.com/login	Out of Scope
				GET	http://www.facebook.com/	Out of Scope