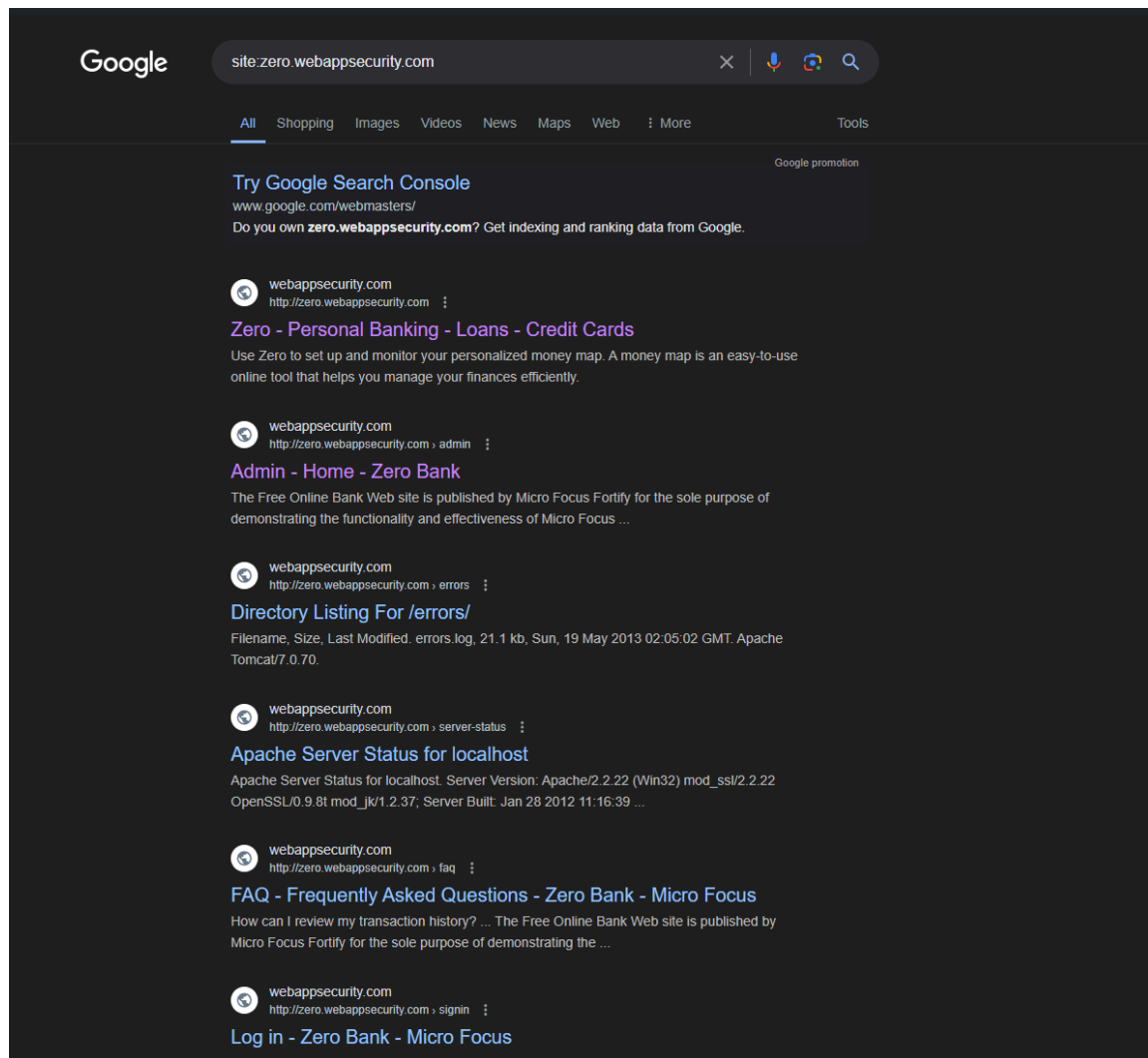


Checklist OWASP WSTG v4.2

OWASP Web Application Testing List.

WSTG-ID	Test Name	Result	Notes
Information Gathering			
INFO-01	Conduct Search Engine Discovery and Reconnaissance for Information Leakage	Issue	Menemukan bebera kebocoran data berupa halaman login admin, apache server status

Screenshot1 :



The screenshot shows a Google search interface with the query 'site:zero.webappsecurity.com' entered in the search bar. The search results are displayed in a list format, each preceded by a small circular icon containing a dollar sign. The results include links to various pages on the zero.webappsecurity.com domain, such as the Google Search Console, Zero - Personal Banking - Loans - Credit Cards, Admin - Home - Zero Bank, Directory Listing For /errors/, Apache Server Status for localhost, FAQ - Frequently Asked Questions - Zero Bank - Micro Focus, and Log in - Zero Bank - Micro Focus. Each result snippet provides a brief description of the page content.

Google

site:zero.webappsecurity.com

All Shopping Images Videos News Maps Web More Tools

Google promotion

Try Google Search Console
www.google.com/webmasters/
Do you own **zero.webappsecurity.com**? Get indexing and ranking data from Google.

webappsecurity.com
http://zero.webappsecurity.com

Zero - Personal Banking - Loans - Credit Cards
Use Zero to set up and monitor your personalized money map. A money map is an easy-to-use online tool that helps you manage your finances efficiently.

webappsecurity.com
http://zero.webappsecurity.com › admin

Admin - Home - Zero Bank
The Free Online Bank Web site is published by Micro Focus Fortify for the sole purpose of demonstrating the functionality and effectiveness of Micro Focus ...

webappsecurity.com
http://zero.webappsecurity.com › errors

Directory Listing For /errors/
Filename, Size, Last Modified. errors.log, 21.1 kb, Sun, 19 May 2013 02:05:02 GMT. Apache Tomcat/7.0.70.

webappsecurity.com
http://zero.webappsecurity.com › server-status

Apache Server Status for localhost
Apache Server Status for localhost. Server Version: Apache/2.2.22 (Win32) mod_ssl/2.2.22 OpenSSL/0.9.8t mod_jk/1.2.37; Server Built: Jan 28 2012 11:16:39 ...

webappsecurity.com
http://zero.webappsecurity.com › faq

FAQ - Frequently Asked Questions - Zero Bank - Micro Focus
How can I review my transaction history? ... The Free Online Bank Web site is published by Micro Focus Fortify for the sole purpose of demonstrating the ...

webappsecurity.com
http://zero.webappsecurity.com › signin

Log in - Zero Bank - Micro Focus
The Free Online Bank Web site is published by Micro Focus Fortify for the sole purpose of

WSTG-ID	Test Name	Result	Notes
---------	-----------	--------	-------

GoBuster

```
(kookyarchon@kookyarchon)-[~]
$ gobuster dir -u http://zero.webappsecurity.com -w /usr/share/wordlists/dirb/big.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://zero.webappsecurity.com
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/admin (Status: 302) [Size: 0] [→ /admin/]
/cgi-bin (Status: 302) [Size: 0] [→ /cgi-bin/]
/cgi-bin/ (Status: 403) [Size: 961]
/docs (Status: 302) [Size: 0] [→ /docs/]
/errors (Status: 302) [Size: 0] [→ /errors/]
/help (Status: 302) [Size: 0] [→ /help/]
/include (Status: 302) [Size: 0] [→ /include/]
/manager (Status: 302) [Size: 0] [→ /manager/]
/resources (Status: 302) [Size: 0] [→ /resources/]
/server-status (Status: 200) [Size: 5523]
/web-services (Status: 200) [Size: 2230]
Progress: 20469 / 20470 (100.00%)

Finished
```

Online Banking

Click the button below to view online banking features.

View online banking

Feroxbuster

```
(kookyarchon@kookyarchon)-[~]
$ feroxbuster -u http://zero.webappsecurity.com -w /usr/share/wordlists/dirb/big.txt

FERRIC OXIDE
by Ben "epi" Risher ver: 2.10.4

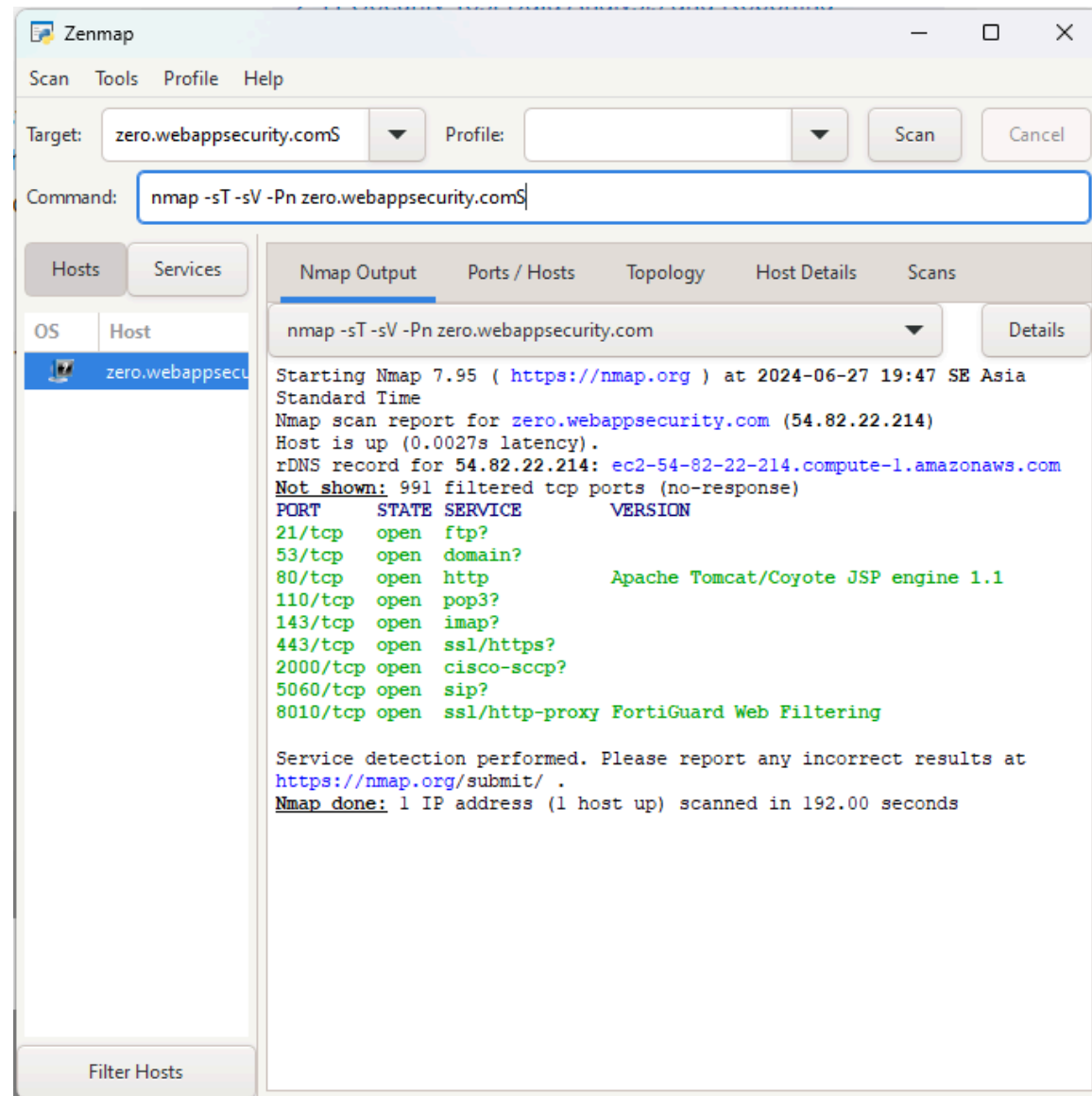
Target Url http://zero.webappsecurity.com
Threads 50
Wordlist /usr/share/wordlists/dirb/big.txt
Status Codes All Status Codes
Timeout (secs) 7
User-Agent feroxbuster/2.10.4
Config File /etc/feroxbuster/ferox-config.toml
Extract Links true
HTTP methods [GET]
Recursion Depth 4

Press [ENTER] to use the Scan Management Menu™

404 GET 1l 44w -c Auto-filtering found 404-like response and created new filter; toggle o
ff with --dont-filter
400 GET 1l 59w 1074c http://zero.webappsecurity.com/search.html
200 GET 775l 1567w 15037c http://zero.webappsecurity.com/resources/css/main.css
200 GET 11l 69w 5615c http://zero.webappsecurity.com/resources/js/placeholders.min.js
200 GET 278l 970w 12471c http://zero.webappsecurity.com/index.html
200 GET 540l 2071w 21752c http://zero.webappsecurity.com/resources/css/font-awesome.css
200 GET 7l 312w 26898c http://zero.webappsecurity.com/resources/js/bootstrap.min.js
200 GET 322l 2238w 204943c http://zero.webappsecurity.com/resources/img/main_carousel_2.jpg
200 GET 310l 1977w 183462c http://zero.webappsecurity.com/resources/img/main_carousel_3.jpg
200 GET 726l 4747w 115795c http://zero.webappsecurity.com/resources/css/bootstrap.min.css
200 GET 248l 1505w 140386c http://zero.webappsecurity.com/resources/img/main_carousel_1.jpg
200 GET 2l 1245w 93436c http://zero.webappsecurity.com/resources/js/jquery-1.8.2.min.js
200 GET 278l 970w 12471c http://zero.webappsecurity.com/
302 GET 0l 0w 0c http://zero.webappsecurity.com/admin => http://zero.webappsecurity.com/
admin/
302 GET 0l 0w 0c http://zero.webappsecurity.com/cgi-bin => http://zero.webappsecurity.com/cgi-bin/
403 GET 1l 46w 961c http://zero.webappsecurity.com/cgi-bin/
302 GET 0l 0w 0c http://zero.webappsecurity.com/docs => http://zero.webappsecurity.com/docs/
302 GET 0l 0w 0c http://zero.webappsecurity.com/errors => http://zero.webappsecurity.com/errors/
302 GET 0l 0w 0c http://zero.webappsecurity.com/help => http://zero.webappsecurity.com/help/
302 GET 0l 0w 0c http://zero.webappsecurity.com/include => http://zero.webappsecurity.com/include/
302 GET 0l 0w 0c http://zero.webappsecurity.com/manager => http://zero.webappsecurity.com/manager/
404 GET 44l 184w -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
302 GET 0l 0w 0c http://zero.webappsecurity.com/resources => http://zero.webappsecurity.com/resources/
200 GET 93l 531w 5523c http://zero.webappsecurity.com/server-status
400 GET 41l 46w 3860c http://zero.webappsecurity.com/web-services/infoService
```

WSTG-ID	Test Name	Result	Notes
INFO-02	Fingerprint Web Server		Semua port terbuka

Screenshot



INFO-03	Review Webserver Metafiles for Information Leakage	N/A	
---------	--	-----	--

Screenshot :

INFO-04	Enumerate Application on Webserver		
---------	------------------------------------	--	--

1. NMAP

WSTG-ID	Test Name	Result	Notes
Screenshot			
<pre> (kookyarchon@kookyarchon)-[~] \$ sudo nmap -sV -sC -p- --min-rate 1000 zero.webappsecurity.com Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-02 14:59 +08 Stats: 0:02:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan SYN Stealth Scan Timing: About 63.86% done; ETC: 15:02 (0:01:04 remaining) Nmap scan report for zero.webappsecurity.com (54.82.22.214) Host is up (0.000065s latency). rDNS record for 54.82.22.214: ec2-54-82-22-214.compute-1.amazonaws.com Not shown: 65532 filtered tcp ports (no-response) PORT STATE SERVICE VERSION 80/tcp open http Apache Tomcat/Coyote JSP engine 1.1 _http-title: Zero - Personal Banking - Loans - Credit Cards _http-methods: _ Potentially risky methods: PUT DELETE TRACE PATCH _http-server-header: Apache-Coyote/1.1 443/tcp open ssl/http Apache httpd 2.2.6 ((Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40) _http-title: Site doesn't have a title (text/html). _sslv2: _ SSLv2 supported _ ciphers: _ SSL2_DES_192_EDE3_CBC_WITH_MD5 _ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 _ SSL2_RC2_128_CBC_WITH_MD5 _ SSL2_RC4_128_EXPORT40_WITH_MD5 _ SSL2_RC4_128_WITH_MD5 _ SSL2_DES_64_CBC_WITH_MD5 _http-server-header: Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40 _ssl-cert: Subject: commonName=zero.webappsecurity.com/organizationName=Micro Focus LLC/stateOrProvinceName=California/countryName=US _ Subject Alternative Name: DNS:zero.webappsecurity.com _ Not valid before: 2021-04-26T00:00:00 _ Not valid after: 2022-05-04T23:59:59 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1 _http-title: Zero - Personal Banking - Loans - Credit Cards _http-methods: _ Potentially risky methods: PUT DELETE TRACE PATCH _http-server-header: Apache-Coyote/1.1 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 235.83 seconds </pre>			
INFO-05	Review Webpage Content for Information Leakage		

User Credentials

Screenshot :



WSTG-ID	Test Name	Result	Notes
<div>Zero Bank</div> <div> <h3>Log in to ZeroBank</h3> <div> <div>Login <input type="text"/></div> <div> <div>?</div> <div>Login/Password - username/password</div> </div> </div> <div> <div>Password <input type="password"/></div> <div> <div>Keep me signed in</div> <div><input type="checkbox"/></div> </div> </div> <div> <div>Sign in</div> </div> <div> Forgot your password ? </div> </div>			
INFO-06	Identify Application Entry Points		
Screenshot :			
INFO-07	Map Execution Paths Through Application		
Screenshot :			
INFO-08	Fingerprint Web Application Framework		
Screenshot :			
INFO-09	Fingerprint Web Application		

1. httprecon

Screenshot

httprecon 7.3 Report

Target: http://zero.webappsecurity.com:80

Tests: 9 test cases

Auditor: USER

Scan: 7/2/2024 - 2:33:27 PM

Export: 7/2/2024 - 2:34:22 PM

Contents

1. Summary

2. Matches

3. Responses

4. Details

Summary ↑

An advanced web server fingerprinting for the host zero.webappsecurity.com and port tcp/80 was done with 9 test cases at 7/2/2024 2:33:27 PM.

This analysis was able to determine the target httpd service as Apache 1.3.37 with 71 fingerprint hits in the database.

List of Matches ↑

	Name	Hits	Match
1.	Apache 1.3.37	71	100%
2.	Apache 2.0.59	67	94.37%
3.	Zope 2.7.7	66	92.96%
4.	Apache 2.2.3	65	91.55%
5.	Microsoft IIS 6.0	65	91.55%
6.	Zope 2.8.6	65	91.55%
7.	Zope 2.9.3	65	91.55%
8.	Zope 2.9.8	65	91.55%
9.	Apache 1.3.26	64	90.14%
10.	Apache 1.3.27	64	90.14%
11.	Apache 1.3.34	64	90.14%
12.	Apache 2.0.54	64	90.14%
13.	Zope 2.8.7	64	90.14%
14.	Apache 1.3.29	63	88.73%
15.	Apache 1.3.33	63	88.73%
16.	Apache 2.0.46	63	88.73%
17.	Apache 2.0.49	63	88.73%
18.	Apache 2.0.52	63	88.73%
19.	Apache 2.0.55	63	88.73%
20.	Apache 2.0.58	63	88.73%

HTTP Response Header ↑

Timing Minimum: 0.039 seconds

Timing Maximum: 0.742 seconds

Timing Average: 0.326 seconds

get_existing

HTTP/1.1 200 OK
Date: Tue, 02 Jul 2024 07:33:32 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html; charset=UTF-8
Content-Language: en-US
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked

get_long

HTTP/1.1 404 Not Found
Date: Tue, 02 Jul 2024 07:33:32 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Length: 2999
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

get_nonexisting

```
HTTP/1.1 404 Not Found
Date: Tue, 02 Jul 2024 07:33:33 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Length: 949
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

head_existing

```
HTTP/1.1 200 OK
Date: Tue, 02 Jul 2024 07:33:34 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html; charset=UTF-8
Content-Language: en-US
Content-Length: 12471
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

options

```
HTTP/1.1 200 OK
Date: Tue, 02 Jul 2024 07:33:34 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH
Content-Length: 0
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/plain
```

delete_existing

```
HTTP/1.1 200 OK
Date: Tue, 02 Jul 2024 07:33:35 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html; charset=UTF-8
Content-Language: en-US
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Transfer-Encoding: chunked
```

wrong_method

```
HTTP/1.1 501 Not Implemented
Date: Tue, 02 Jul 2024 07:33:35 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Length: 1104
Connection: close
```

wrong_version

```
HTTP/1.1 200 OK
Date: Tue, 02 Jul 2024 07:33:34 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html; charset=UTF-8
Content-Language: en-US
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
```

attack_request

```
HTTP/1.1 404 Not Found
Date: Tue, 02 Jul 2024 07:33:36 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Length: 971
```

Fingerprint Details ↑

get_existing

```
Protocol Name HTTP
Protocol Version 1.1
Statuscode 200
Statustext
Banner Apache-Coyote/1.1
X-Powered-By
Header Spaces 1
Capital after Dash 1
Header-Order Full Date,Server,Access-Control-Allow-Origin,Cache-Control,Content-Type,Content-
Language,Keep-Alive,Connection,Transfer-Encoding
Header-Order Limit Date,Server,Access-Control-Allow-Origin,Cache-Control,Content-Type,Content-
Language,Keep-Alive,Connection,Transfer-Encoding
Options-Allowed
Options-Public
Options-Delimiter
ETag
ETag-Length 0
ETag-Quotes
Content-Type text/html;charset=UTF-8
Accept-Range
Connection Keep-Alive
Cache-Control no-cache, max-age=0, must-revalidate, no-store
Pragma
Vary-Order
Vary-Capitalized
Vary-Delimiter
htaccess-Realm
```

get_long

```
Protocol Name HTTP
Protocol Version 1.1
Statuscode 404
Statustext
Banner Apache-Coyote/1.1
X-Powered-By
Header Spaces 1
Capital after Dash 1
Header-Order Full Date,Server,Access-Control-Allow-Origin,Content-Type,Content-
Language,Content-Length,Keep-Alive,Connection
Header-Order Limit Date,Server,Access-Control-Allow-Origin,Content-Type,Content-
Language,Content-Length,Keep-Alive,Connection
Options-Allowed
Options-Public
Options-Delimiter
ETag
ETag-Length 0
ETag-Quotes
Content-Type text/html;charset=utf-8
Accept-Range
Connection Keep-Alive
Cache-Control
Pragma
Vary-Order
Vary-Capitalized
Vary-Delimiter
htaccess-Realm
```

get_nonexisting

```
Protocol Name HTTP
Protocol Version 1.1
Statuscode 404
Statustext
Banner Apache-Coyote/1.1
X-Powered-By
Header Spaces 1
Capital after Dash 1
Header-Order Full Date,Server,Access-Control-Allow-Origin,Cache-Control,Content-Type,Content-
Language,Content-Length,Keep-Alive,Connection
Header-Order Limit Date,Server,Access-Control-Allow-Origin,Cache-Control,Content-Type,Content-
Language,Content-Length,Keep-Alive,Connection
Options-Allowed
Options-Public
Options-Delimiter
ETag
ETag-Length 0
ETag-Quotes
Content-Type text/html;charset=utf-8
Accept-Range
Connection Keep-Alive
Cache-Control no-cache, max-age=0, must-revalidate, no-store
Pragma
Vary-Order
Vary-Capitalized
```

head_existing

```
Protocol Name HTTP
Protocol Version 1.1
Statuscode 200
Statustext
Banner Apache-Coyote/1.1
X-Powered-By
Header Spaces 1
Capital after Dash 1
Header-Order Full Date, Server, Access-Control-Allow-Origin, Cache-Control, Content-Type, Content-
Language, Content-Length, Keep-Alive, Connection
Header-Order Limit Date, Server, Access-Control-Allow-Origin, Cache-Control, Content-Type, Content-
Language, Content-Length, Keep-Alive, Connection
Options-Allowed
Options-Public
Options-Delimiter
ETag
ETag-Length 0
ETag-Quotes
Content-Type text/html; charset=UTF-8
Accept-Range
Connection Keep-Alive
Cache-Control no-cache, max-age=0, must-revalidate, no-store
Pragma
Vary-Order
Vary-Capitalized
Vary-Delimiter
htaccess-Realm
```

options

```
Protocol Name HTTP
Protocol Version 1.1
Statuscode 200
Statustext
Banner Apache-Coyote/1.1
X-Powered-By
Header Spaces 1
Capital after Dash 1
Header-Order Full Date, Server, Access-Control-Allow-Origin, Cache-Control, Allow, Content-
Length, Keep-Alive, Connection, Content-Type
Header-Order Limit Date, Server, Access-Control-Allow-Origin, Cache-Control, Allow, Content-
Length, Keep-Alive, Connection, Content-Type
Options-Allowed GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH
Options-Public
Options-Delimiter ,
ETag
ETag-Length 0
ETag-Quotes
Content-Type text/plain
Accept-Range
Connection Keep-Alive
Cache-Control no-cache, max-age=0, must-revalidate, no-store
Pragma
Vary-Order
Vary-Capitalized
Vary-Delimiter
htaccess-Realm
```

delete_existing

```
Protocol Name HTTP
Protocol Version 1.1
Statuscode 200
Statustext
Banner Apache-Coyote/1.1
X-Powered-By
Header Spaces 1
Capital after Dash 1
Header-Order Full Date, Server, Access-Control-Allow-Origin, Cache-Control, Content-Type, Content-
Language, Keep-Alive, Connection, Transfer-Encoding
Header-Order Limit Date, Server, Access-Control-Allow-Origin, Cache-Control, Content-Type, Content-
Language, Keep-Alive, Connection, Transfer-Encoding
Options-Allowed
Options-Public
Options-Delimiter
ETag
ETag-Length 0
ETag-Quotes
Content-Type text/html; charset=UTF-8
Accept-Range
Connection Keep-Alive
Cache-Control no-cache, max-age=0, must-revalidate, no-store
Pragma
Vary-Order
Vary-Capitalized
Vary-Delimiter
htaccess-Realm
```

wrong_method

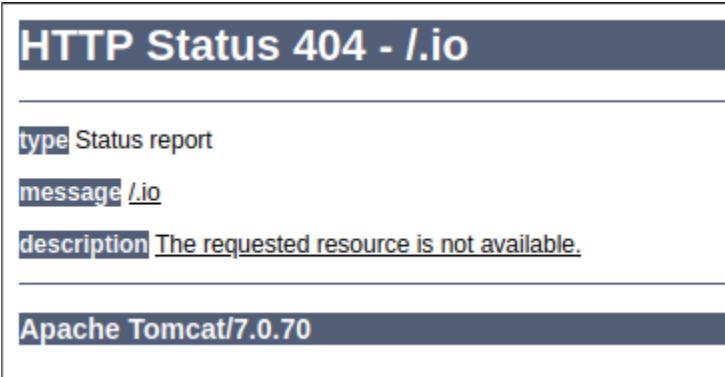
```
Protocol Name HTTP
Protocol Version 1.1
Statuscode 501
Statustext Not Implemented
Banner Apache-Coyote/1.1
X-Powered-By
Header Spaces 1
Capital after Dash 1
Header-Order Full Date,Server,Access-Control-Allow-Origin,Cache-Control,Content-Type,Content-
Language,Content-Length,Connection
Header-Order Limit Date,Server,Access-Control-Allow-Origin,Cache-Control,Content-Type,Content-
Language,Content-Length,Connection
Options-Allowed
Options-Public
Options-Delimiter
ETag
ETag-Length 0
ETag-Quotes
Content-Type text/html;charset=utf-8
Accept-Range
Connection close
Cache-Control no-cache, max-age=0, must-revalidate, no-store
Pragma
Vary-Order
Vary-Capitalized
Vary-Delimiter
htaccess-Realm
```

wrong_version

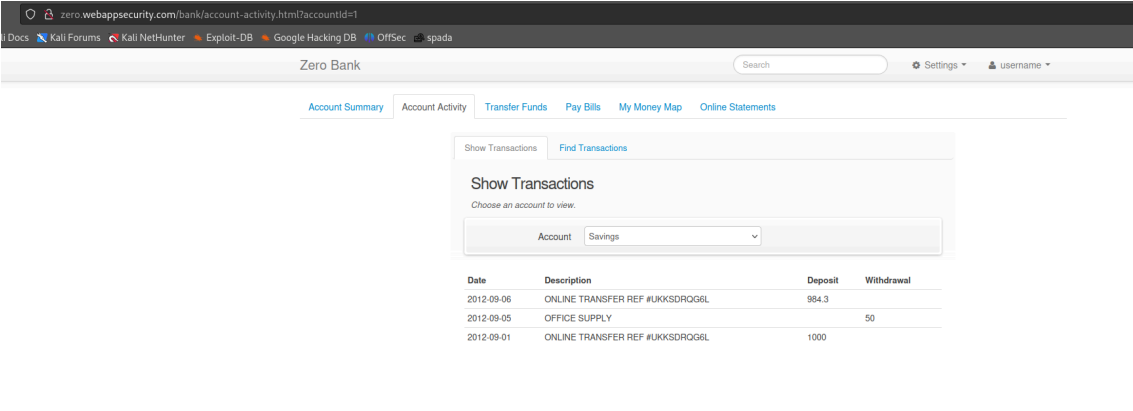
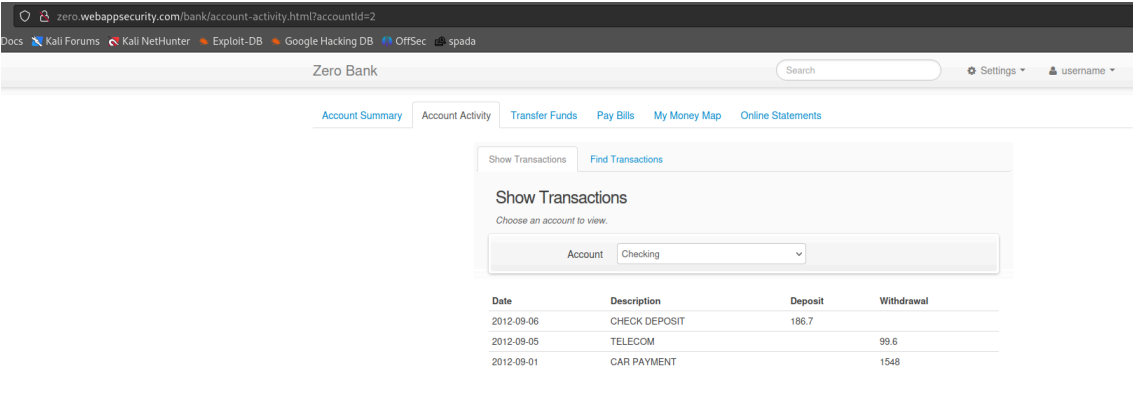
```
Protocol Name HTTP
Protocol Version 1.1
Statuscode 200
Statustext
Banner Apache-Coyote/1.1
X-Powered-By
Header Spaces 1
Capital after Dash 1
Header-Order Full Date,Server,Access-Control-Allow-Origin,Cache-Control,Content-Type,Content-
Language,Keep-Alive,Connection,Transfer-Encoding
Header-Order Limit Date,Server,Access-Control-Allow-Origin,Cache-Control,Content-Type,Content-
Language,Keep-Alive,Connection,Transfer-Encoding
Options-Allowed
Options-Public
Options-Delimiter
ETag
ETag-Length 0
ETag-Quotes
Content-Type text/html;charset=UTF-8
Accept-Range
Connection Keep-Alive
Cache-Control no-cache, max-age=0, must-revalidate, no-store
Pragma
Vary-Order
Vary-Capitalized
Vary-Delimiter
htaccess-Realm
```

attack_request

```
Protocol Name HTTP
Protocol Version 1.1
Statuscode 404
Statustext
Banner Apache-Coyote/1.1
X-Powered-By
Header Spaces 1
Capital after Dash 1
Header-Order Full Date,Server,Access-Control-Allow-Origin,Content-Type,Content-
Language,Content-Length,Keep-Alive,Connection
Header-Order Limit Date,Server,Access-Control-Allow-Origin,Content-Type,Content-
Language,Content-Length,Keep-Alive,Connection
Options-Allowed
Options-Public
Options-Delimiter
ETag
ETag-Length 0
ETag-Quotes
Content-Type text/html;charset=utf-8
Accept-Range
Connection Keep-Alive
Cache-Control
Pragma
Vary-Order
Vary-Capitalized
Vary-Delimiter
htaccess-Realm
```

WSTG-ID	Test Name	Result	Notes
INFO-10	Map Application Architecture		
Screenshot :			
			
Configuration and Deployment Management Testing			
CONF-01	Test Network/Infrastructure Configuration		
Screenshot :			
CONF-02	Test Application Platform Configuration		
Screenshot :			
CONF-03	Test File Extensions Handling for Sensitive Information		
Screenshot :			
CONF-04	Review Old Backup and Unreferenced Files for Sensitive Information		
Screenshot :			
CONF-05	Enumerate Infrastructure and Application Admin Interface		
Screenshot :			
CONF-06	Test HTTP Methods		
Screenshot :			
CONF-07	Test HTTP Strict Transport Security		
Screenshot :			
CONF-08	Test RIA Cross Domain Policy		
Screenshot :			
CONF-09	Test File Permission		
Screenshot :			
CONF-10	Test for Subdomain Takeover		
Screenshot :			
CONF-11	Test Cloud Storage		
Screenshot :			
Identity Management Testing			
IDNT-01	Test Role Definition		

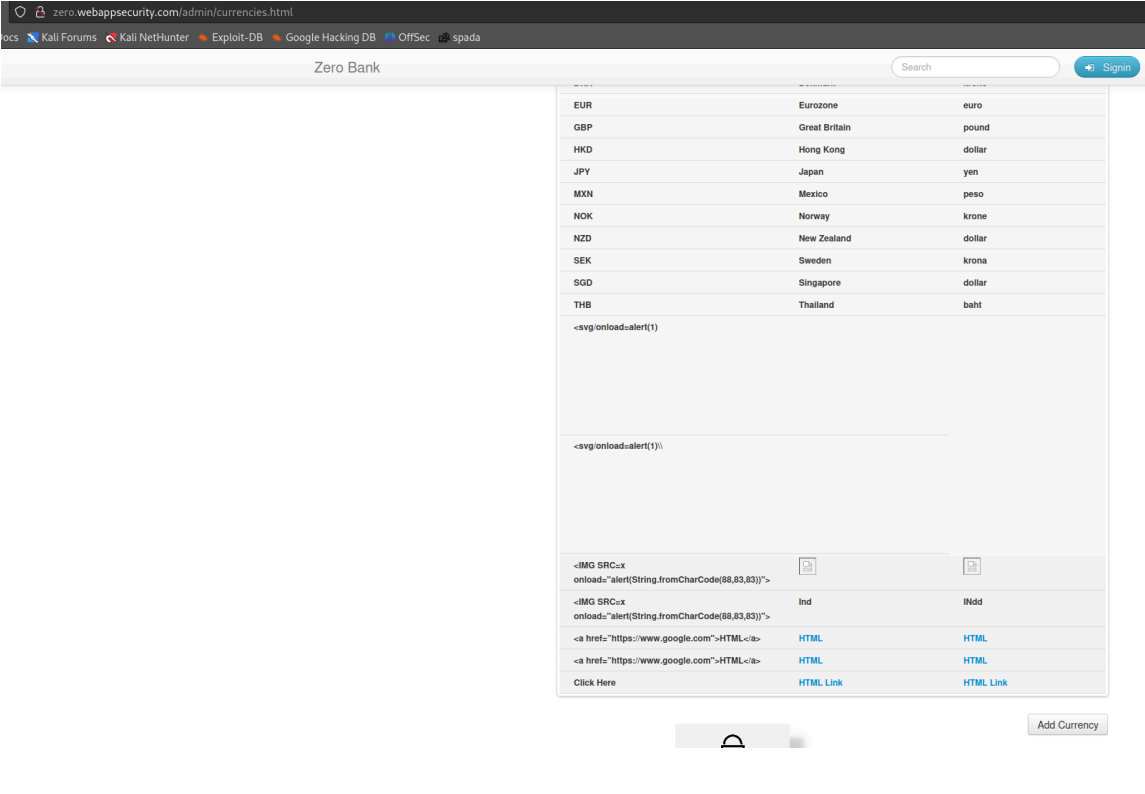
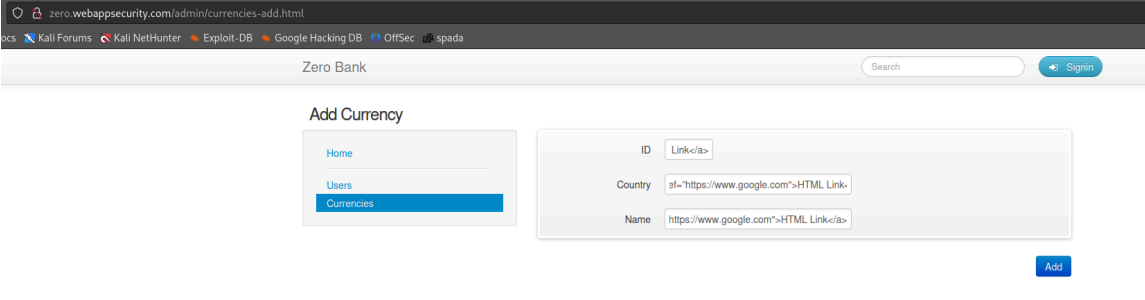
WSTG-ID	Test Name	Result	Notes
Screenshot :			
IDNT-02	Test User Registration Process		
Screenshot :			
IDNT-03	Test Account Provisioning Process		
Screenshot :			
IDNT-04	Testing for Account Enumeration and Guessable User Account		
Screenshot :			
IDNT-05	Testing for Weak or Unenforced Username Policy		
Screenshot :			
Authentication Testing			
ATHN-01	Testing for Credentials Transported over an Encrypted Channel		
Screenshot :			
ATHN-02	Testing for Defaults Credentials		
Screenshot :			
ATHN-03	Testing for Weak Lock Out Mechanism		
Screenshot :			
ATHN-04	Testing for Bypassing Authentication Schema		
Screenshot :			
ATHN-05	Testing for Vulnerable Remember Password		
Screenshot :			
ATHN-06	Testing for Browser Cache Weakness		
Screenshot :			
ATHN-07	Testing for Weak Password Policy		
Screenshot :			
ATHN-08	Testing for Weak Security Question/Answer		
Screenshot :			
ATHN-09	Testing for Weak Password Change or Reset Functionalities		
Screenshot :			
ATHN-10	Testing for Weaker Authentication in Alternative Channel		
Screenshot :			
Authorization Testing			
ATHZ-01	Testing Directory Traversal/File Include		
Screenshot :			
ATHZ-02	Testing for Bypassing Authorization Schema		

WSTG-ID	Test Name	Result	Notes
Screenshot :			
ATHZ-03	Testing for Privilege Escalation		
Screenshot :			
ATHZ-04	Testing for Insecure Direct Object References		
Screenshot :			
IDOR with query parameter			
			
			
Session Management Testing			
SESS-01	Testing for Session Management Schema		
Screenshot :			
SESS-02	Testing for Cookies Attributes		
Screenshot :			
SESS-03	Testing for Session Fixation		
Screenshot :			
Static Session ID			
Attempt 1			

WSTG-ID	Test Name	Result	Notes
<div> <div>Request</div> <div> <div>Pretty</div> <div>Raw</div> <div>Hex</div> </div> <div> <div>1</div> <div>2</div> <div>3</div> <div>4</div> <div>5</div> <div>6</div> <div>7</div> <div>8</div> <div>9</div> <div>10</div> <div>11</div> <div>12</div> <div>13</div> </div> <div> <pre> GET /login.html?login_error=true HTTP/1.1 Host: zero.webappsecurity.com Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/av if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange ;v=b3;q=0.7 Referer: http://zero.webappsecurity.com/login.html?login_error=true Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: JSESSIONID=DD47FFFE Connection: close </pre> </div> </div>			
<div> <div>Attempt 2</div> <div> <div>Pretty</div> <div>Raw</div> <div>Hex</div> </div> <div> <div>1</div> <div>2</div> <div>3</div> <div>4</div> <div>5</div> <div>6</div> <div>7</div> <div>8</div> <div>9</div> <div>10</div> <div>11</div> <div>12</div> <div>13</div> <div>14</div> <div>15</div> </div> <div> <pre> POST /signin.html HTTP/1.1 Host: zero.webappsecurity.com Content-Length: 105 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: http://zero.webappsecurity.com Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://zero.webappsecurity.com/login.html?login_error=true Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: JSESSIONID=DD47FFFE Connection: close user_login=username&user_password=password&submit=Sign+in&user_token=e9ec03c2-47fa-49ab-a81a-cb22a13c198b </pre> </div> </div>			
SESS-04	Testing for Exposed Session Variables		
Screenshot :			
SESS-05	Testing for Cross Site Request Forgery		
Screenshot :			
SESS-06	Testing for Logout Functionality		
Screenshot :			
SESS-07	Testing Session Timeout		
Screenshot :			
SESS-08	Testing for Session Puzzling		
Screenshot :			
SESS-09	Testing for Session Hijacking		
Screenshot :			

WSTG-ID	Test Name	Result	Notes
Input Validation Testing			
INPV-01	Testing for Reflected Cross Site Scripting		
Screenshot :			
INPV-02	Testing for Stored Cross Site Scripting		
Screenshot :			
INPV-03	Testing for HTTP Verb Tampering		
Screenshot :			
INPV-04	Testing for HTTP Parameter pollution		
Screenshot :			
INPV-05	Testing for SQL Injection		
Screenshot :			
INPV-06	Testing for LDAP Injection		
Screenshot :			
INPV-07	Testing for XML Injection		
Screenshot :			
INPV-08	Testing for SSI Injection		
Screenshot :			
INPV-09	Testing for XPath Injection		
Screenshot :			
INPV-10	Testing for IMAP/SMTP Injection		
Screenshot :			
INPV-11	Testing for Code Injection		
INPV-12	Testing for Command Injection		
Screenshot :			
INPV-13	Testing for Format String Injection		
Screenshot :			
INPV-14	Testing for Incubated Vulnerabilities		
Screenshot :			
INPV-15	Testing for HTTP Splitting/Smuggling		
Screenshot :			
INPV-16	Testing for HTTP Incoming Requests		
Screenshot :			
INPV-17	Testing for Host Header Injection		
Screenshot :			
INPV-18	Testing for Server-side Template Injection		
Screenshot :			
INPV-19	Testing for Server-side Request Forgery		
Screenshot :			

WSTG-ID	Test Name	Result	Notes
Testing for Error Handling			
ERRH-01	Testing for Improper Error Handling		
Screenshot :			
ERRH-02	Testing for Stack Traces		
Screenshot :			
Testing for Weak Cryptography			
CRYP-01	Testing for Weak Transport Layer Security		
Screenshot :			
CRYP-02	Testing for Padding Oracle		
Screenshot :			
CRYP-03	Testing for Sensitive Information Sent via Unencrypted Channels		
Screenshot :			
CRYP-04	Testing for Weak Encryption		
Screenshot :			
Business Logic Testing			
BUSL-01	Test Business Logic Data Validation		
Screenshot :			
BUSL-02	Test Ability to Forge Requests		
Screenshot :			
BUSL-03	Test Integrity Checks		
Screenshot :			
BUSL-04	Test for Process Timing		
Screenshot :			
BUSL-05	Test Number of Times a Function Can be Used Limits		
Screenshot :			
BUSL-06	Testing for the Circumvention of Work Flows		
Screenshot :			
BUSL-07	Test Defenses Against Application Misuse		
Screenshot :			
BUSL-08	Test Upload of Unexpected File Types		
Screenshot :			
BUSL-09	Test Upload of Malicious Files		
Screenshot :			
Client Side Testing			
CLNT-01	Testing for DOM-Based Cross Site Scripting		
Screenshot :			
CLNT-02	Testing for JavaScript Execution		
Screenshot :			

WSTG-ID	Test Name	Result	Notes
CLNT-03	Testing for HTML Injection		
Screenshot : Payload: HTML Link			
			
			
CLNT-04	Testing for Client-side URL Redirect		
Screenshot :			
CLNT-05	Testing for CSS Injection		
Screenshot :			
CLNT-06	Testing for Client Side Resource Manipulation		
Screenshot :			
CLNT-07	Testing Cross Origin Resource Sharing		
Screenshot :			
CLNT-08	Testing for Cross Site Flashing		

WSTG-ID	Test Name	Result	Notes
Screenshot :			
CLNT-09	Testing for Clickjacking		
Screenshot :			
CLNT-10	Testing WebSockets		
Screenshot :			
CLNT-11	Testing Web Messaging		
Screenshot :			
CLNT-12	Testing Browser Storage		
Screenshot :			
CLNT-13	Testing for Cross Site Script Inclusion		
Screenshot :			
API Testing			
APIT-01	Testing GraphQL		
Screenshot :			