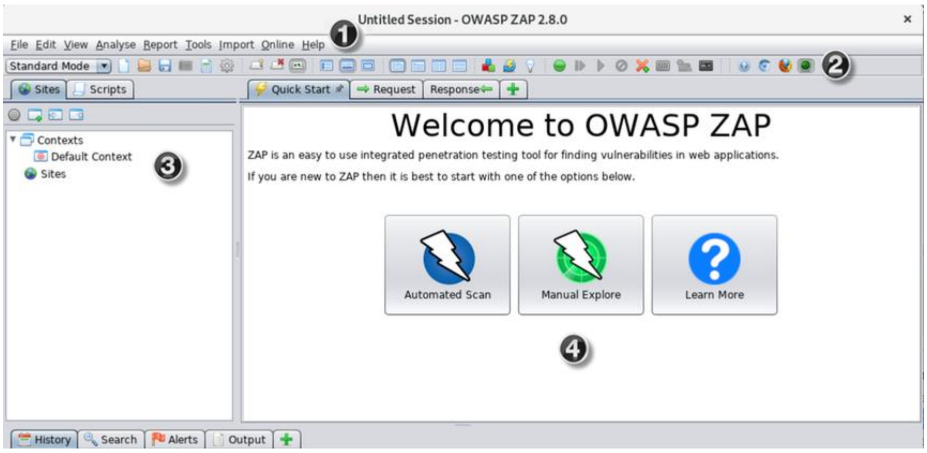
Automated Scanners

Report by Sukhveer singh

Automated Scanners –

1. OWASP ZAP (Zed Attack Proxy): -

OWASP ZAP, developed by the Open Web Application Security Project, stands as a dynamic application security testing (DAST) tool. Designed to uncover vulnerabilities in web applications, ZAP facilitates both active and passive scanning, identifying issues like injection, cross-site scripting, and cross-site request forgery. Its user-friendly interface makes it accessible to users of varying expertise, and with automation capabilities, ZAP seamlessly integrates into development pipelines, ensuring continuous security monitoring.



Untitled Session - OWASP ZAP 2.8.0

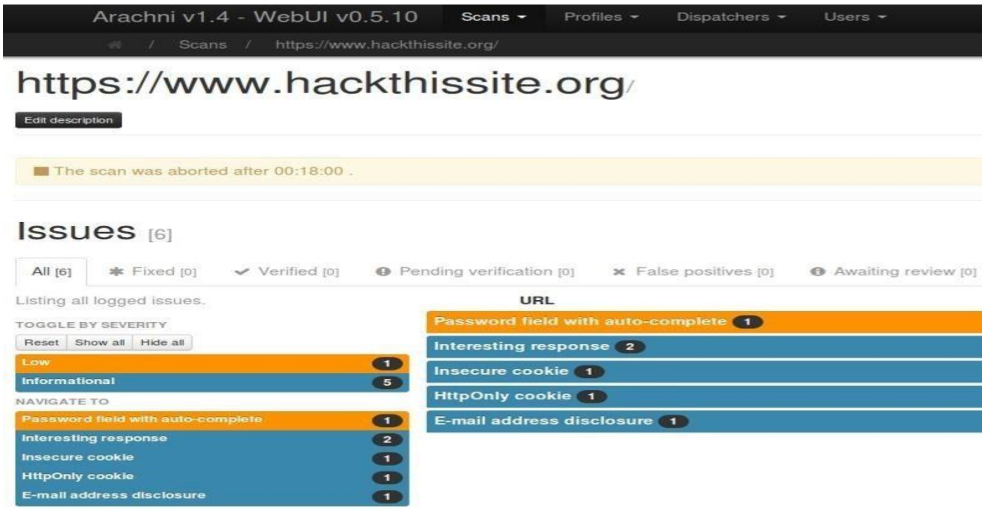
Welcome to OWASP ZAP

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.

2. Arachni: -

Arachni serves as a crawler-based scanner, systematically navigating through web applications to identify security vulnerabilities. Its comprehensive scanning approach ensures the detection of various bugs and security holes, contributing to a robust defense against potential threats. Arachni's efficiency lies in its ability to thoroughly map and analyze web applications, making it a valuable asset in the realm of web security.



https://www.hackthissite.org/

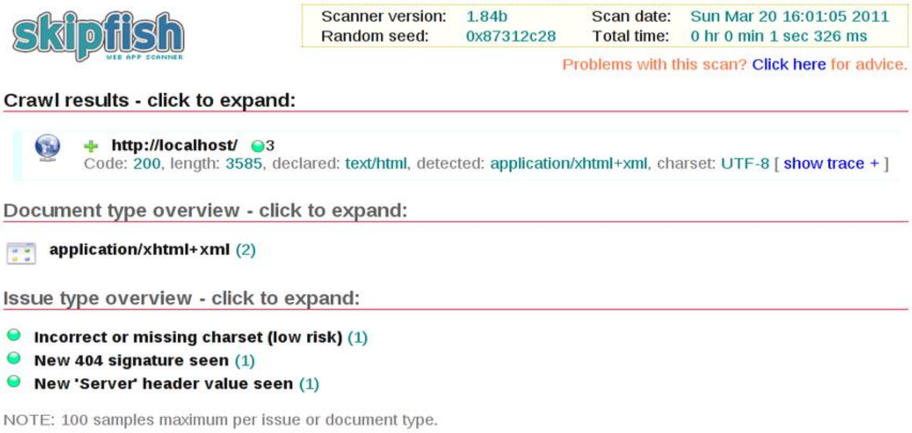
The scan was aborted after 00:18:00 .

Issues [6]

Listing all logged issues.

3. Skipfish: -

Skipfish emerges as a high-speed and reliable web application security scanner. Its key strength lies in quickly mapping and pinpointing vulnerabilities within web applications. By efficiently scanning and analyzing potential risks, Skipfish aids developers and security professionals in fortifying their online assets, ensuring a proactive and effective defense against cyber threats.



Scanner version: 1.84b Scan date: Sun Mar 20 16:01:05 2011
Random seed: 0x87312c28 Total time: 0 hr 0 min 1 sec 326 ms

Problems with this scan? Click here for advice.

Crawl results - click to expand:

http://localhost/ 3
Code: 200, length: 3585, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]

Document type overview - click to expand:

application/xhtml+xml (2)

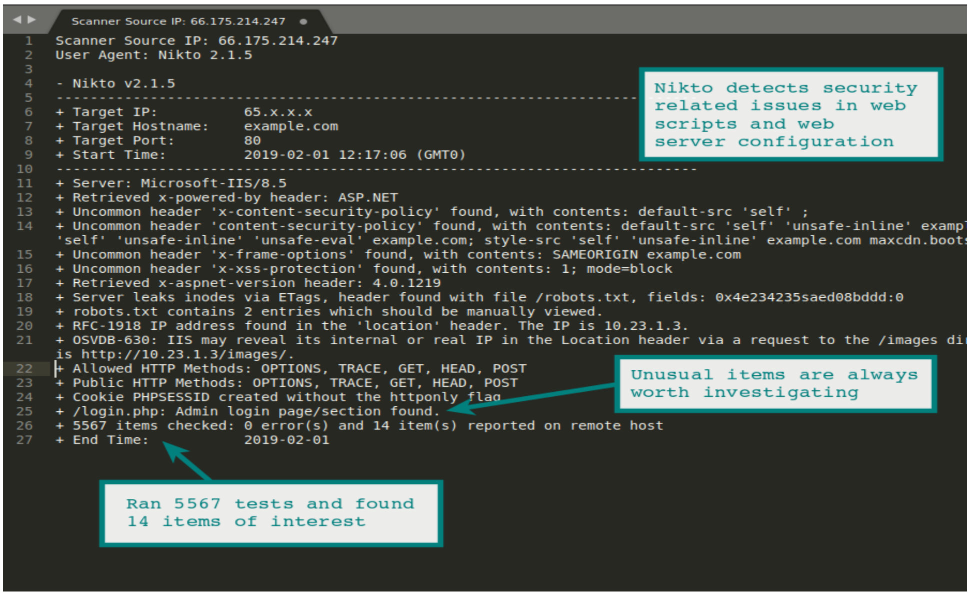
Issue type overview - click to expand:

- Incorrect or missing charset (low risk) (1)
- New 404 signature seen (1)
- New 'Server' header value seen (1)

NOTE: 100 samples maximum per issue or document type.

4. Nikto: -

Nikto stands out as a steadfast web server scanner, diligently searching for potential security issues and vulnerabilities. Its versatility allows it to uncover a range of risks, providing a comprehensive assessment of a web server's security posture. Nikto's systematic approach makes it an essential tool for ensuring the robustness of web applications in the face of evolving cyber threats.



```
Scanner Source IP: 66.175.214.247
User Agent: Nikto 2.1.5

- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          65.x.x.x
+ Target Hostname:    example.com
+ Target Port:        80
+ Start Time:         2019-02-01 12:17:06 (GMT0)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.5
+ Retrieved x-powered-by header: ASP.NET
+ Uncommon header 'x-content-security-policy' found, with contents: default-src 'self' ;
+ Uncommon header 'content-security-policy' found, with contents: default-src 'self' 'unsafe-inline' exampl
'self' 'unsafe-inline' 'unsafe-eval' example.com; style-src 'self' 'unsafe-inline' example.com maxcdn.boots
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN example.com
+ Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
+ Retrieved x-aspnet-version header: 4.0.1219
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x4e234235saed08bddd:0
+ robots.txt contains 2 entries which should be manually viewed.
+ RFC-1918 IP address found in the 'location' header. The IP is 10.23.1.3.
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images di
is http://10.23.1.3/images/.
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Cookie PHPSESSID created without the httponly flag
+ /login.php: Admin login page/section found.
+ 5567 items checked: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2019-02-01
```

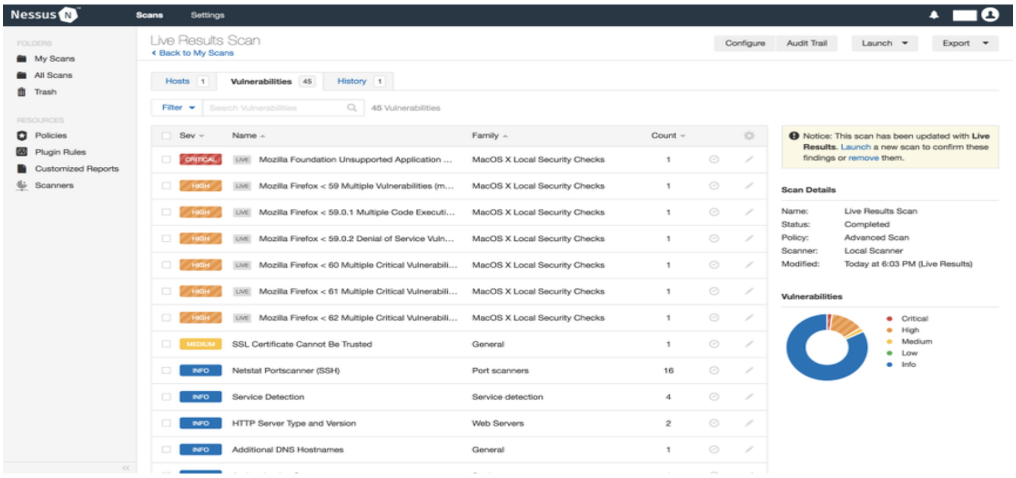
Nikto detects security related issues in web scripts and web server configuration

Unusual items are always worth investigating

Ran 5567 tests and found 14 items of interest

5. Nessus: -

Nessus, often considered the Sherlock Holmes of cybersecurity, is a comprehensive vulnerability scanner. Known for its accuracy and efficiency, Nessus digs deep into systems to identify weaknesses and potential threats. Its proactive approach to vulnerability management makes Nessus a go-to choice for security professionals aiming to maintain a secure digital environment.



Sev	Name	Family	Count
CRITICAL	LIVE Mozilla Foundation Unsupported Application ...	MacOS X Local Security Checks	1
HIGH	LIVE Mozilla Firefox < 59 Multiple Vulnerabilities (m...	MacOS X Local Security Checks	1
HIGH	LIVE Mozilla Firefox < 59.0.1 Multiple Code Executi...	MacOS X Local Security Checks	1
HIGH	LIVE Mozilla Firefox < 59.0.2 Denial of Service Vuln...	MacOS X Local Security Checks	1
HIGH	LIVE Mozilla Firefox < 60 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
HIGH	LIVE Mozilla Firefox < 61 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
HIGH	LIVE Mozilla Firefox < 62 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
INFO	Netstat Portscanner (SSH)	Port scanners	16
INFO	Service Detection	Service detection	4
INFO	HTTP Server Type and Version	Web Servers	2
INFO	Additional DNS Hostnames	General	1

Notice: This scan has been updated with **Live Results**. Launch a new scan to confirm these findings or remove them.

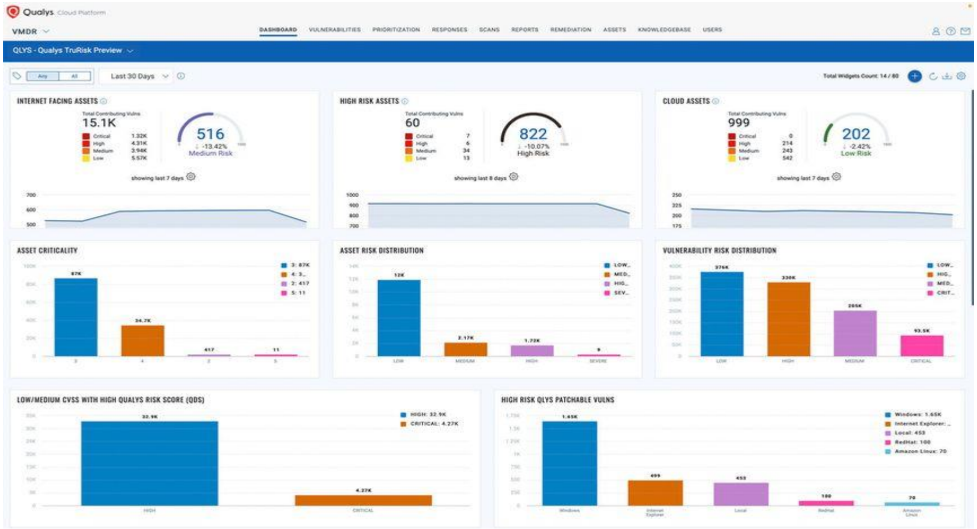
Scan Details

Name:	Live Results Scan
Status:	Completed
Policy:	Advanced Scan
Scanner:	Local Scanner
Modified:	Today at 6:03 PM (Live Results)

Vulnerabilities

6. Qualys: -

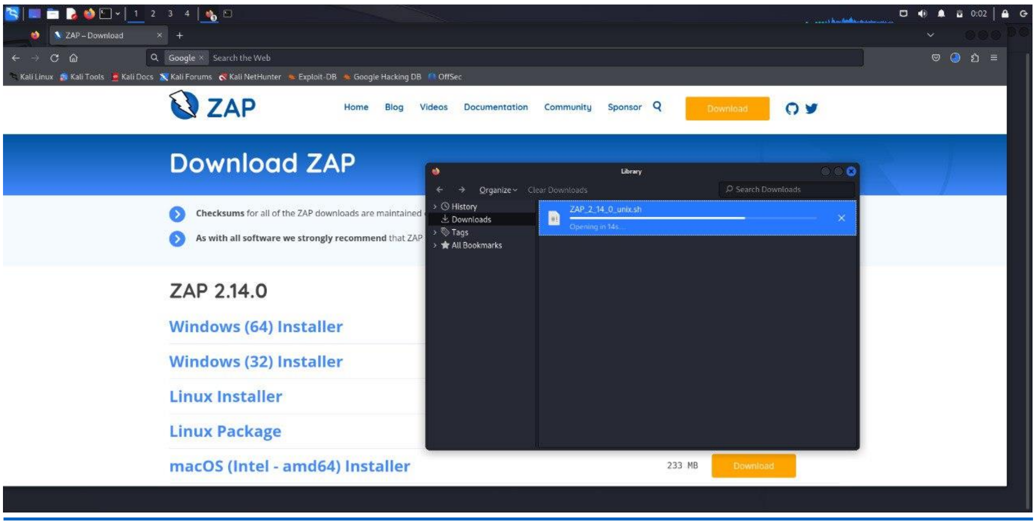
Qualys emerges as a proactive cloud-based security platform, covering everything from vulnerability management to web application security. With continuous monitoring and a comprehensive suite of security tools, Qualys enables users to stay ahead of potential threats. Its cloud-based nature facilitates easy integration and scalability, making Qualys a valuable ally in maintaining the security of online assets.



Practical report

1. Installation process of zap proxy in kali –

Step 1 – install zap from https://www.zaproxy.org/



Download ZAP

Checksums for all of the ZAP downloads are maintained

As with all software we strongly recommend that ZAP

ZAP 2.14.0

Windows (64) Installer

Windows (32) Installer

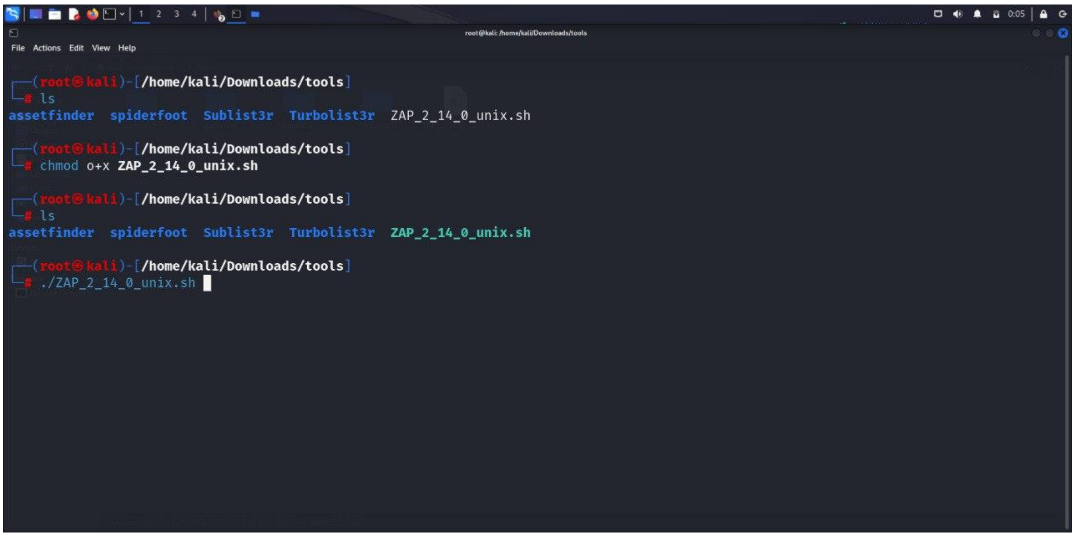
Linux Installer

Linux Package

macOS (Intel - amd64) Installer 233 MB

Step 2 – open file location in terminal and make sure you have root permission

Then give permission to zap file name in order to execute



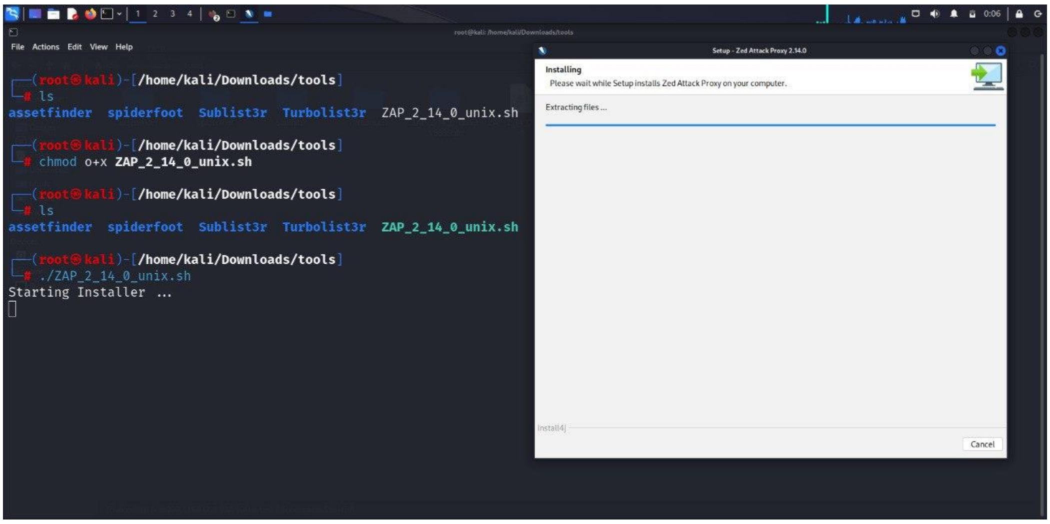
```
┌──(root㉿kali)-[/home/kali/Downloads/tools]
└─# ls
assetfinder  spiderfoot  Sublist3r  Turbolist3r  ZAP_2_14_0_unix.sh

┌──(root㉿kali)-[/home/kali/Downloads/tools]
└─# chmod o+x ZAP_2_14_0_unix.sh

┌──(root㉿kali)-[/home/kali/Downloads/tools]
└─# ls
assetfinder  spiderfoot  Sublist3r  Turbolist3r  ZAP_2_14_0_unix.sh

┌──(root㉿kali)-[/home/kali/Downloads/tools]
└─# ./ZAP_2_14_0_unix.sh
```

Step 3 – run zap using (./filename) in my case - ./ZAP_2_14_0_unix.sh



```
┌──(root㉿kali)-[/home/kali/Downloads/tools]
└─# ls
assetfinder  spiderfoot  Sublist3r  Turbolist3r  ZAP_2_14_0_unix.sh

┌──(root㉿kali)-[/home/kali/Downloads/tools]
└─# chmod o+x ZAP_2_14_0_unix.sh

┌──(root㉿kali)-[/home/kali/Downloads/tools]
└─# ls
assetfinder  spiderfoot  Sublist3r  Turbolist3r  ZAP_2_14_0_unix.sh

┌──(root㉿kali)-[/home/kali/Downloads/tools]
└─# ./ZAP_2_14_0_unix.sh
Starting Installer ...
```

Setup - Zed Attack Proxy 2.14.0

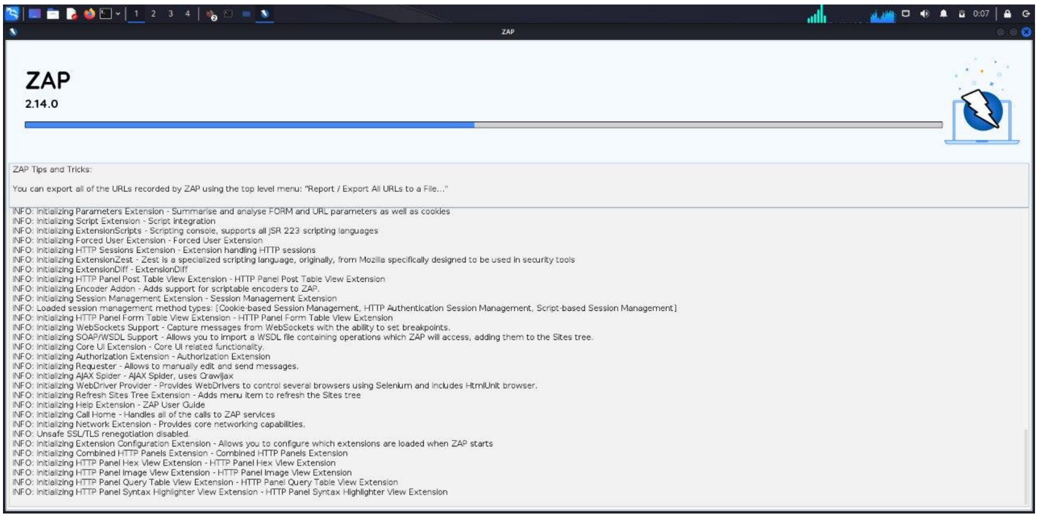
Installing

Please wait while Setup installs Zed Attack Proxy on your computer.

Extracting files ...

File Actions Edit View Help
root@kali: /home/kali/Downloads/tools
Install4j
Cancel
0:06

Install manually by clicking next-next



ZAP

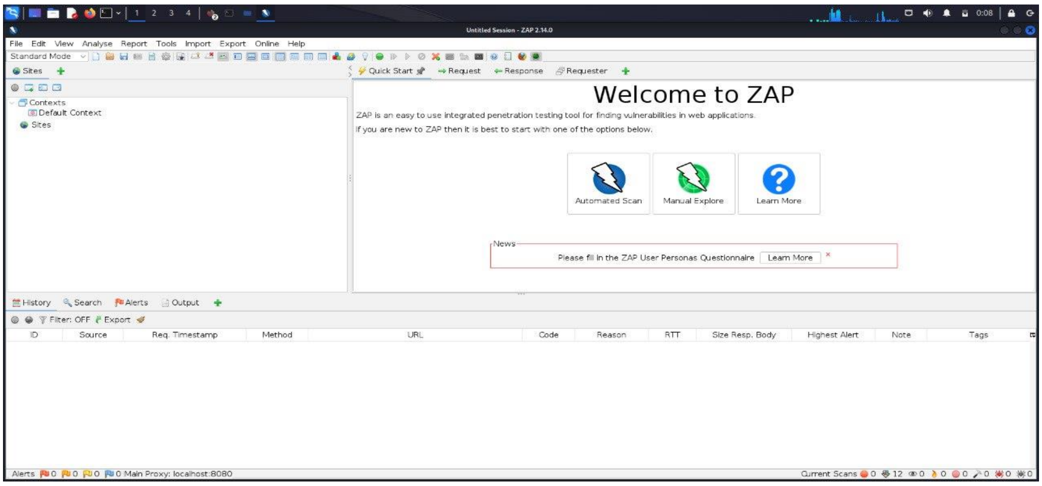
2.14.0

ZAP Tips and Tricks:

You can export all of the URLs recorded by ZAP using the top level menu: "Report / Export All URLs to a File..."

```
INFO: Initializing Parameters Extension - Summarise and analyse FORM and URL parameters as well as cookies
INFO: Initializing Script Extension - Script integration
INFO: Initializing ExtensionScripts - Scripting console, supports all JSR 223 scripting languages
INFO: Initializing Forced User Extension - Forced User Extension
INFO: Initializing HTTP Sessions Extension - Extension handling HTTP sessions
INFO: Initializing ExtensionZest - Zest is a specialized scripting language, originally, from Mozilla specifically designed to be used in security tools
INFO: Initializing ExtensionDiff - ExtensionDiff
INFO: Initializing HTTP Panel Post Table View Extension - HTTP Panel Post Table View Extension
INFO: Initializing Encoder Addon - Adds support for scriptable encoders to ZAP.
INFO: Initializing Session Management Extension - Session Management Extension
INFO: Loaded session management method types: [Cookie-based Session Management, HTTP Authentication Session Management, Script-based Session Management]
INFO: Initializing HTTP Panel Form Table View Extension - HTTP Panel Form Table View Extension
INFO: Initializing WebSockets Support - Capture messages from WebSockets with the ability to set breakpoints.
INFO: Initializing SOAP/WSDL Support - Allows you to import a WSDL file containing operations which ZAP will access, adding them to the Sites tree.
INFO: Initializing Core UI Extension - Core UI related functionality.
INFO: Initializing Authorization Extension - Authorization Extension
INFO: Initializing Requester - Allows to manually edit and send messages.
INFO: Initializing AJAX Spider - AJAX Spider, uses Crawljax
INFO: Initializing WebDriver Provider - Provides WebDrivers to control several browsers using Selenium and includes HtmlUnit browser.
INFO: Initializing Refresh Sites Tree Extension - Adds menu item to refresh the Sites tree
INFO: Initializing Help Extension - ZAP User Guide
INFO: Initializing Call Home - Handles all of the calls to ZAP services
INFO: Initializing Network Extension - Provides core networking capabilities.
INFO: Unsafe SSL/TLS renegotiation disabled.
INFO: Initializing Extension Configuration Extension - Allows you to configure which extensions are loaded when ZAP starts
INFO: Initializing Combined HTTP Panels Extension - Combined HTTP Panels Extension
INFO: Initializing HTTP Panel Hex View Extension - HTTP Panel Hex View Extension
INFO: Initializing HTTP Panel Image View Extension - HTTP Panel Image View Extension
INFO: Initializing HTTP Panel Query Table View Extension - HTTP Panel Query Table View Extension
INFO: Initializing HTTP Panel Syntax Highlighter View Extension - HTTP Panel Syntax Highlighter View Extension
```

Step 4 - your all set now open zap in order to scan a target



Untitled Session - ZAP 2.14.0

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.

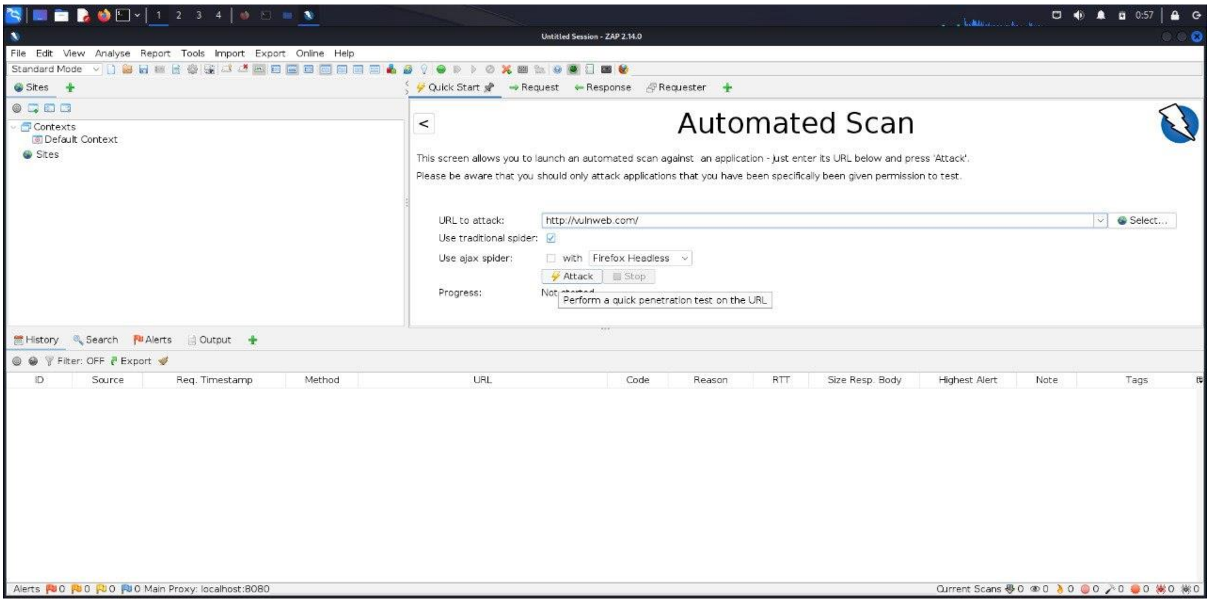
News

Please fill in the ZAP User Personas Questionnaire

How to scan –

Step 1 – open zap and click on automated scan

Step 2 – Enter your target url in my case http://vulnweb.com


Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
History
Search
Alerts
Output
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
Attack
Stop
Select...
Alerts 0 0 0 0 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

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 given permission to test.

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

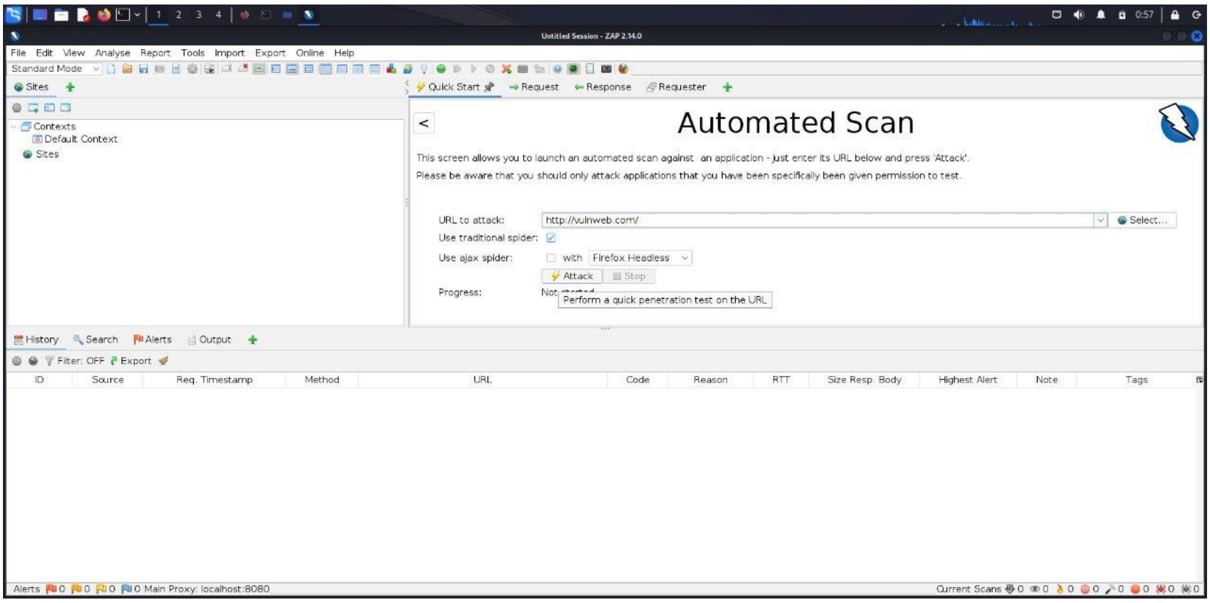
Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Progress: Not started

Perform a quick penetration test on the URL

Step 3 – click on Attack button to run a scan


Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
History
Search
Alerts
Output
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
Attack
Stop
Select...
Alerts 0 0 0 0 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

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 given permission to test.

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

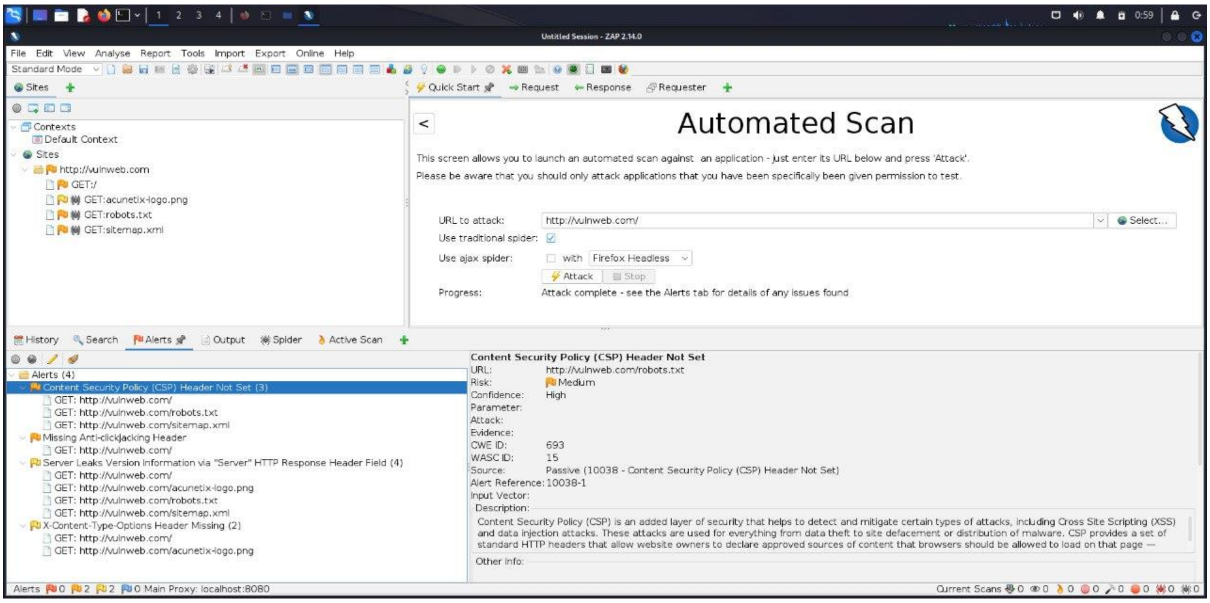
Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Progress: Not started

Perform a quick penetration test on the URL

Here you can see all output after done 100% scan by clicking various options like alerts, outputs, spider, active scan etc.



Untitled Session - ZAP 2.14.0

File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
History Search Alerts Output Spider Active Scan

Contexts
Default Context
Sites
http://vulnweb.com
GET:/
GET:acunetix-logo.png
GET:robots.txt
GET:sitemap.xml

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.

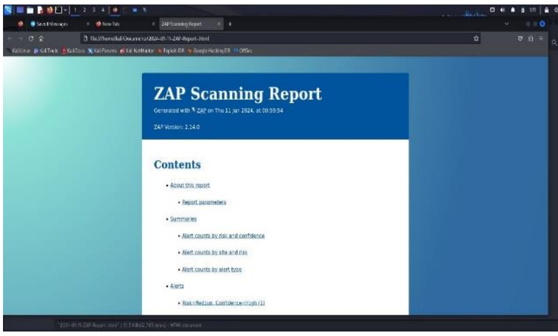
URL to attack: http://vulnweb.com/ Select...
Use traditional spider: ☑
Use ajax spider: □ with Firefox Headless
Attack Stop
Progress: Attack complete - see the Alerts tab for details of any issues found

Alerts (4)
- Content Security Policy (CSP) Header Not Set (3)
  - GET: http://vulnweb.com/
  - GET: http://vulnweb.com/robots.txt
  - GET: http://vulnweb.com/sitemap.xml
- Missing Anti-clickjacking Header
  - GET: http://vulnweb.com/
- Server Leaks Version Information via "Server" HTTP Response Header Field (4)
  - GET: http://vulnweb.com/
  - GET: http://vulnweb.com/acunetix-logo.png
  - GET: http://vulnweb.com/robots.txt
  - GET: http://vulnweb.com/sitemap.xml
- X-Content-Type-Options Header Missing (2)
  - GET: http://vulnweb.com/
  - GET: http://vulnweb.com/acunetix-logo.png

Content Security Policy (CSP) Header Not Set
URL: http://vulnweb.com/robots.txt
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference: 10038-1
Input Vector:
Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page —
Other Info:

Alerts 0 2 2 0 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

The generated report images



file:///home/kali/Documents/2024-01-11-ZAP-Report-.html

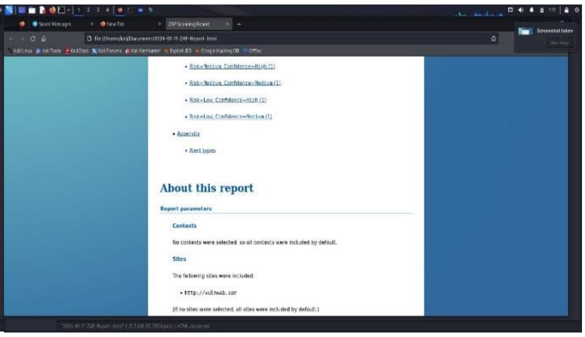
ZAP Scanning Report

Generated with ZAP on Thu 11 Jan 2024, at 00:59:54

ZAP Version: 2.14.0

Contents

- About this report
  - Report parameters
- Summaries
  - Alert counts by risk and confidence
  - Alert counts by site and risk
  - Alert counts by alert type
- Alerts
  - Risk=Medium, Confidence=High (1)



- Risk=Medium, Confidence=High (1)
- Risk=Medium, Confidence=Medium (1)
- Risk=Low, Confidence=High (1)
- Risk=Low, Confidence=Medium (1)
- Appendix
  - Alert types

About this report

Report parameters

Contexts

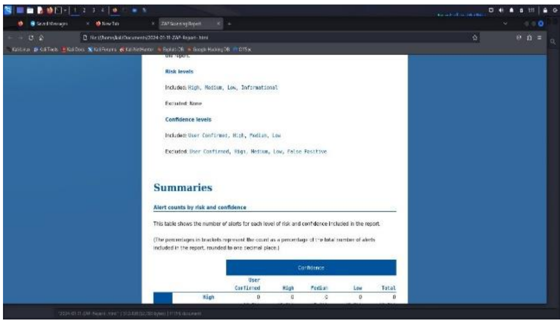
No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- http://vulnweb.com

(If no sites were selected, all sites were included by default.)



Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

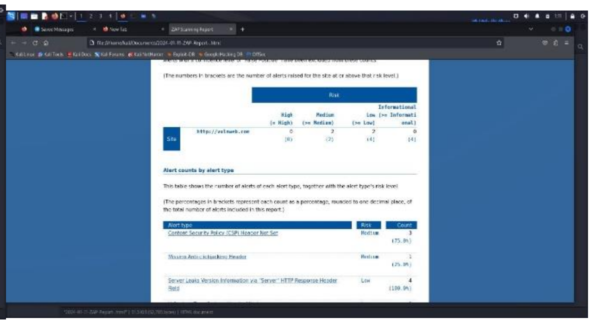
Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
	High	0	0	0	0	0



(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

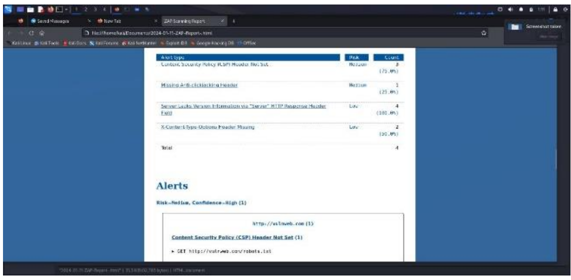
		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://vulnweb.com	0 (0)	2 (2)	2 (4)	0 (4)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	3 (75.0%)
Missing Anti-clickjacking Header	Medium	1 (25.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	4 (100.0%)



Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	3 (75.0%)
Missing Anti-clickjacking Header	Medium	1 (25.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	4 (100.0%)
X-Content-Type-Options Header Missing	Low	2 (50.0%)
Total		4

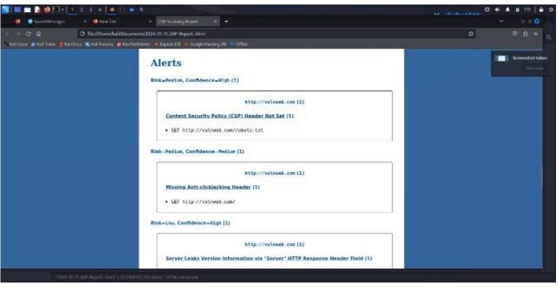
Alerts

Risk=Medium, Confidence=High (1)

http://vulnweb.com (1)

Content Security Policy (CSP) Header Not Set (1)

- GET http://vulnweb.com/robots.txt



Alerts

Risk=Medium, Confidence=High (1)

http://vulnweb.com (1)

Content Security Policy (CSP) Header Not Set (1)

- GET http://vulnweb.com/robots.txt

Risk=Medium, Confidence=Medium (1)

http://vulnweb.com (1)

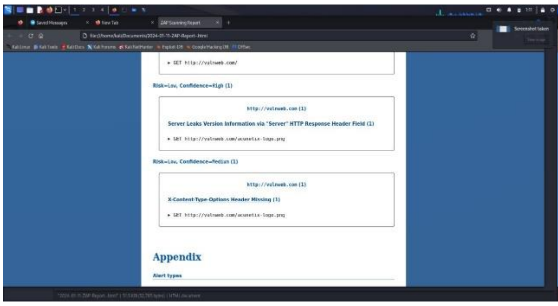
Missing Anti-clickjacking Header (1)

- GET http://vulnweb.com/

Risk=Low, Confidence=High (1)

http://vulnweb.com (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)



- GET http://valnweb.com/

Risk=Low, Confidence=High (1)

http://valnweb.com (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

- GET http://valnweb.com/acunetix-logo.png

Risk=Low, Confidence=Medium (1)

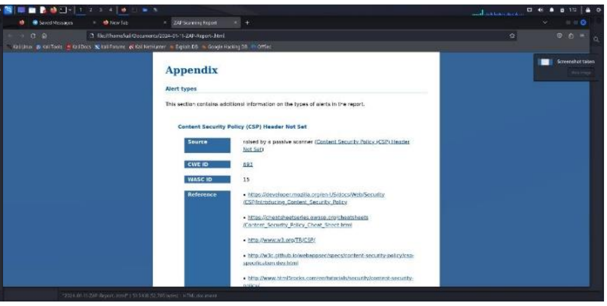
http://valnweb.com (1)

X-Content-Type-Options Header Missing (1)

- GET http://valnweb.com/acunetix-logo.png

Appendix

Alert types



Appendix

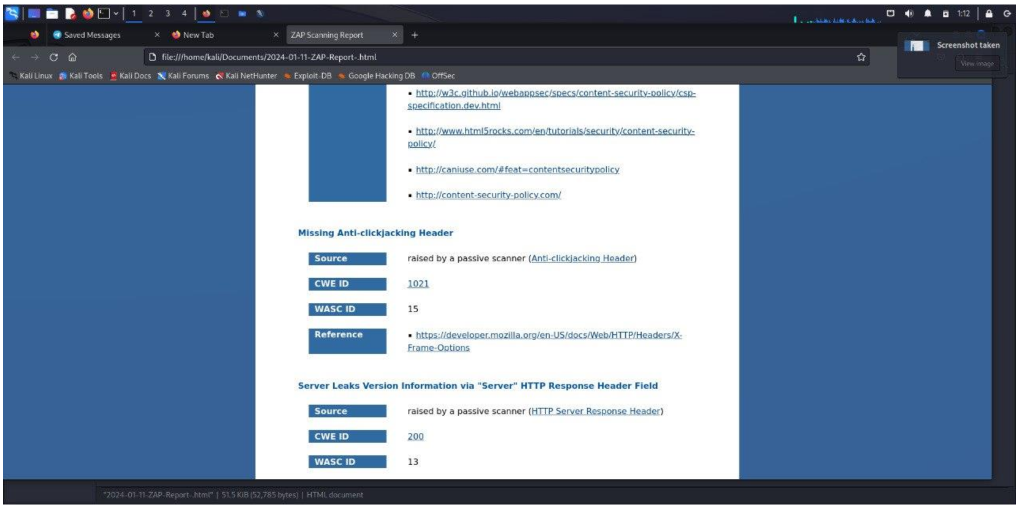
Alert types

This section contains additional information on the types of alerts in the report.

Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	• https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy • https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html • http://www.w3.org/TR/CSP/ • http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html • http://www.html5rocks.com/en/tutorials/security/content-security-policy/

"2024-01-11-ZAP-Report-.html" | 51.5 KiB (52,785 bytes) | HTML document



- http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
- http://www.html5rocks.com/en/tutorials/security/content-security-policy/
- http://caniuse.com/#feat=contentsecuritypolicy
- http://content-security-policy.com/

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	• https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200
WASC ID	13

"2024-01-11-ZAP-Report-.html" | 51.5 KiB (52,785 bytes) | HTML document

References –

https://geekflare.com/open-source-web-security-scanner/

https://www.getastra.com/blog/security-audit/web-application-vulnerability-scanner/

https://www.zaproxy.org/