Configuration Manual

MSc Internship
CyberSecurity

Mandar Prashant Shah
Student ID: x18139469

School of Computing
National College of Ireland

Supervisor: Dr. Muhammad Iqbal

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Mandar Prashant Shah

Student ID: X18139469

Programme: MSc Cybersecurity **Year:** 2019

Module: Internship Thesis

Lecturer: Dr. Muhammad Iqbal

Submission Due Date: 8/1/2020

Project Title: Comparative Analysis of the Automated Penetration Testing Tools

Word Count: **1359 Page Count: 8**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: ………..

Date: ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Mandar Prashant Shah
Student ID: x18139469

1 Introduction

To implement and demonstrate the framework presented in the research thesis, we need software and hardware system configurations. We will be discussing this configuration in the following chapters. The system configuration starts with selecting a base machine with adequate resources and installing a VMware player on it. Then the installation of tools such as Burp suite[1], OWASP ZAP[2], Arachni[3] and Nikto2[4]. The Burp suite is installed on Windows machine and other three tools are configured on Kali Linux[5] machine. The benchmark which we are using is OWASP Benchmark Project[6] which we will install on Kali Linux machine [1].

2 System Configuration

System 1:
Base machine: Windows 10
Processor: Quad core processor
Memory: 16 GB
System type: 64 bit operating system
HDD: 10 GB of free space

System 2:
Virtual Machine: Kali Linux
Processor: Two processors
Memory: 4 GB
System type: 64 bit
HDD: 10 GB of free space

3 Tools installation

In this section we will discuss how to install various tools and benchmark required for our experiment.

3.1 OWASP Benchmark Project:

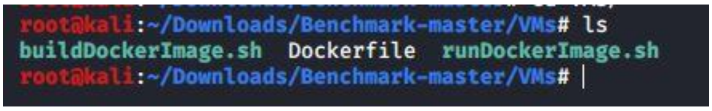
We have installed OWASP Benchmark Project in Kali linux VM. The project is hosted by OWASP.org on their website URL: https://www.owasp.org/index.php/Benchmark

[1] Burp Suite: https://portswigger.net/burp
[2] OWASP ZAP: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project#tab=ZAP_Gear
[3] Arachni: http://arachni-scanner.com/
[4] Nikto 2: http://arachni-scanner.com/
[5] Kali Linux: https://www.kali.org/downloads/
[6] OWASP Benchmark: https://github.com/OWASP/Benchmark

And its source code can be downloaded from URL: https://github.com/OWASP/Benchmark
Step 1: Download the git file, unzip and navigate to the project folder using following command:

- cd /root/Downloads/Benchmark/VMs

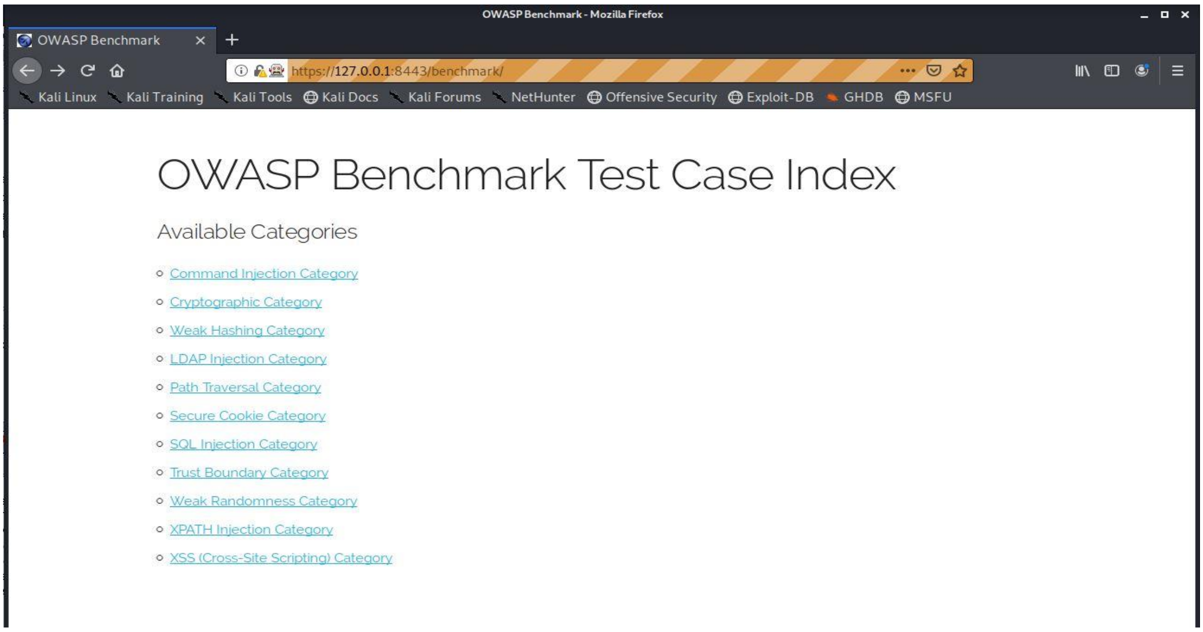
Step 2: In VMs folder run the ‘BuildDockerImage.sh’. Now the docker will be created for the project.



```
root@kali:~/Downloads/Benchmark-master/VMs# ls
buildDockerImage.sh  Dockerfile  runDockerImage.sh
root@kali:~/Downloads/Benchmark-master/VMs# |
```

Figure 3.1: Docker Image scripts

Step 3: Once the docker image is build successfully, run the ‘runDockerImage.sh’ file. This will start the project and host the application.
Step 4: Open web browser and enter following URL to access the Benchmark web application.
URL: https://127.0.0.1:8443/benchmark



OWASP Benchmark Test Case Index

Available Categories

- Command Injection Category
- Cryptographic Category
- Weak Hashing Category
- LDAP Injection Category
- Path Traversal Category
- Secure Cookie Category
- SQL Injection Category
- Trust Boundary Category
- Weak Randomness Category
- XPATH Injection Category
- XSS (Cross-Site Scripting) Category

Figure 3.2: OWASP Benchmark Project

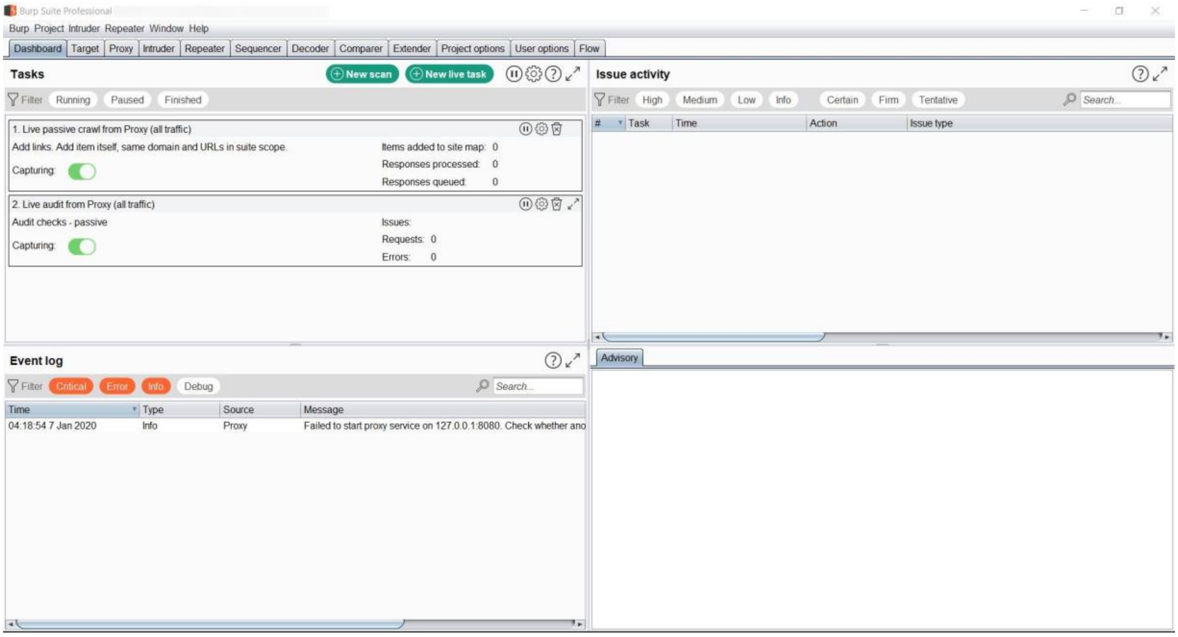
The application is ready for scan.

3.2 Burp Suite:

The Burp Suite Pro version was used for this test. Download the Burp Suite Pro executable from following URL:
https://portswigger.net/buy/pro
We will install Burp Suite on Windows machine.
Step 1: Navigate to the Downloads folder in C drive.

- Path: C:\Users\<USERNAME>\Downloads

Step 2: Locate the Burp Suite executable file and double click to install.
Step 3: Once the installation process is complete, double click on installed application icon to stat the application.


Burp Suite Professional
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Flow
Tasks
New scan
New live task
Filter Running Paused Finished
Issue activity
Filter High Medium Low Info Certain Firm Tentative
Search...
Event log
Filter Critical Error Info Debug
Search...
Advisory

1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing:
Items added to site map: 0
Responses processed: 0
Responses queued: 0

2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing:
Issues:
Requests: 0
Errors: 0

#	Task	Time	Action	Issue type

Time	Type	Source	Message
04:18:54 7 Jan 2020	Info	Proxy	Failed to start proxy service on 127.0.0.1:8080. Check whether ano

Figure 3.2.1: Burp Proxy interface

3.3 OWASP ZAP:

OWASP ZAP comes pre-installed in KALI Linux machine. But before going forward we will update the ZAP.

Step 1: Use commands shown in the following image to update the ZAP.

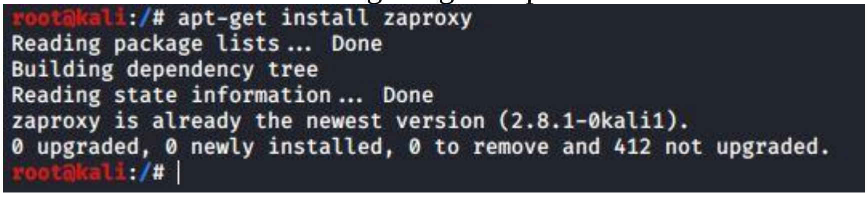
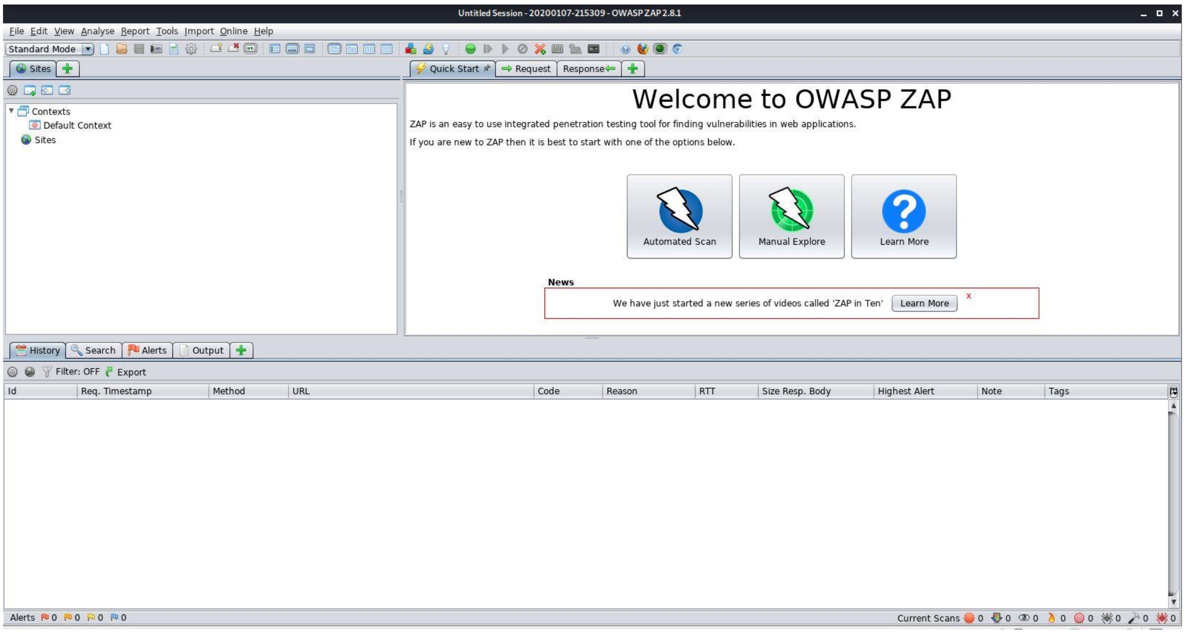

```
root@kali:/# apt-get install zaproxy
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
zaproxy is already the newest version (2.8.1-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 412 not upgraded.
root@kali:/# |
```

Figure 3.3.1: ZAP Update

Step 2: Open a terminal and type command 'zaproxy' and press enter. ZAP will initiate and application UI will be presented on the screen.



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.

News

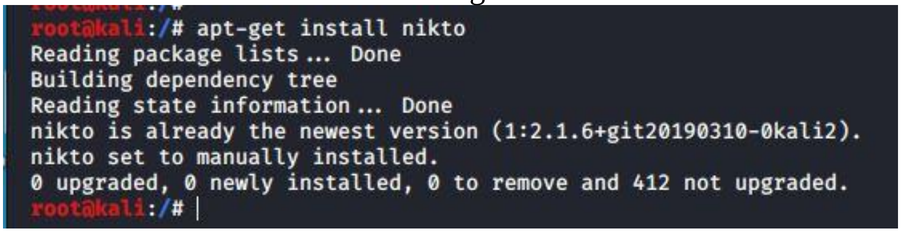
We have just started a new series of videos called 'ZAP in Ten' Learn More

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags

Figure 3.3.2: ZAP Proxy interface

3.4 Nikto 2:

Nikto also comes pre-installed in Kali distribution. We will update the Nikto.
Step 1: Run the command shown in the following screenshot.



```
root@kali:/# apt-get install nikto
Reading package lists... Done
Building dependency tree
Reading state information... Done
nikto is already the newest version (1:2.1.6+git20190310-0kali2).
nikto set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 412 not upgraded.
root@kali:/# |
```

Figure 3.4.1: Nikto update

Step 2: The tool is ready for use. Use command ‘nikto -host <URL>’ to scna the host.

3.5 Arachni:

Arachni does not come preconfigured with the Kali Linux but can be installed using the apt-get command.
Step 1: Open a terminal and type following command.

- Command: apt-get install arachni

Step 2: Once the installation is complete the tool is ready to use. Use the following command to scan the host.

- arachni <URL>

4 Tools configuration

For Point and shoot scan following are the commands used for each scanner

4.1 Arachni

Step 1: Open a new terminal and type following command and press enter.

- arachni https://127.0.0.1:8443/benchmarks

This will load all the profiles in the Arachni and scan the host.
Report will be stored in “/usr/share/arachni/reports/” folder in .afr format.
Step 2: Run the arachni reporter tool to convert the report in .xml format.

- arachni_reporter arachni2.afr --reporter 'xml:outfile=/root/Desktop'

4.2 Nikto 2:

Step 1: Type following command in the terminal to run the scan on a host:

- nikto -host https://127.0.0.1:8443/benchmarks -format xml

step 2: The xml report generated can be copied to Benchmarks results folder using following command:

- cp ./format.xml /root/Downloads/Benchmark/results

For configured scan the tool can be configured in the following way:

4.3 Burp Suite:

Step 1: Configure the Burp to your browser.
Step 2: Open the following URL in the browse with intercept off on the Burp suite.

- URL: https://127.0.0.1:8443/benchmarks

Step 3: Manually crawl through the application. This will create the site map in the Burp suite.

Step 4: Click on the Target tab in the Burp and right click on the scope URL. Select add to scope option.

Step5: Again, right click on the target URL and select scan.

Step 6: A new window will popup. Select crawl and scan profile in this page.

Step 7: The active scan will start and at the end of scan select the issues you wish to report and click on generate report.

Step 8: Select file type as .xml.

4.4 OWASP ZAP:

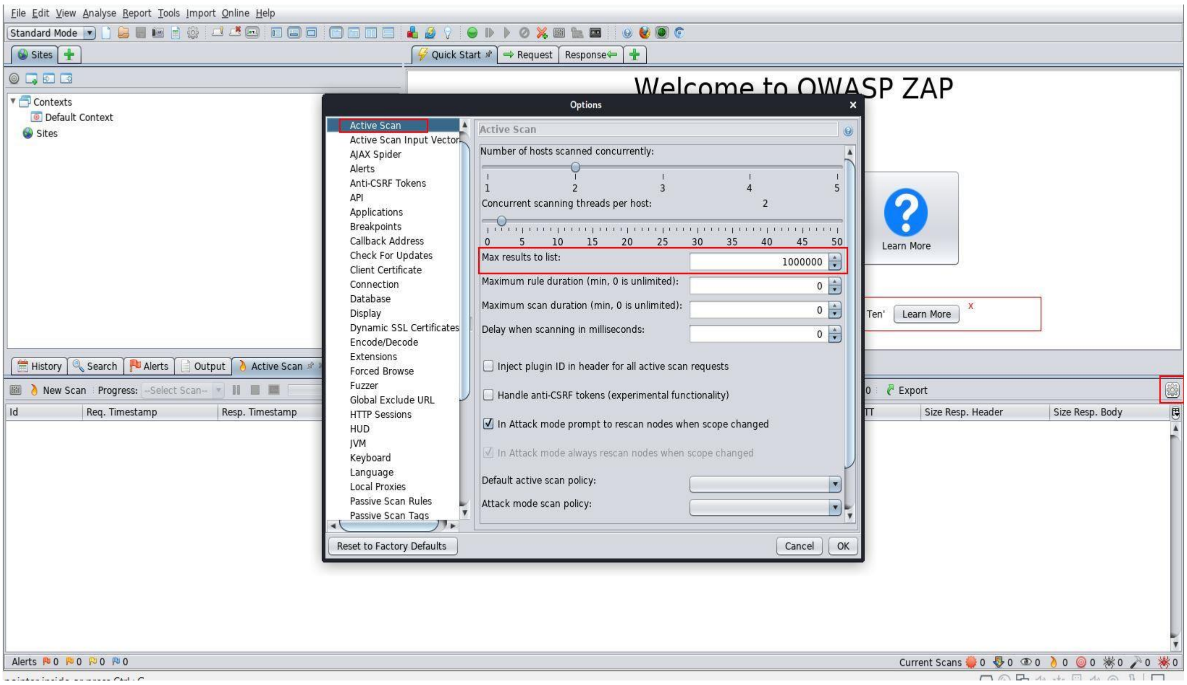
Step 1: Turn on ZAP and select the browser icon in the tool to start a proxy browser.

Step 2: Enter the target URL in the browser and navigate through the pages.

- URL: https://127.0.0.1:8443/benchmarks

Step 3: Click on 'View>show tab> Active Scan tab' to get the active scan tab on the screen.

Step 4: To increase the default logging of request from 1000 to 100000, select the wheel icon on the right hand side of the screen and adjust the value under 'Active Scan' option. As shown in the following figure.



Active Scan

Number of hosts scanned concurrently: 2

Concurrent scanning threads per host: 2

Max results to list: 1000000

Maximum rule duration (min, 0 is unlimited): 0

Maximum scan duration (min, 0 is unlimited): 0

Delay when scanning in milliseconds: 0

☐ Inject plugin ID in header for all active scan requests

☐ Handle anti-CSRF tokens (experimental functionality)

☑ In Attack mode prompt to rescan nodes when scope changed

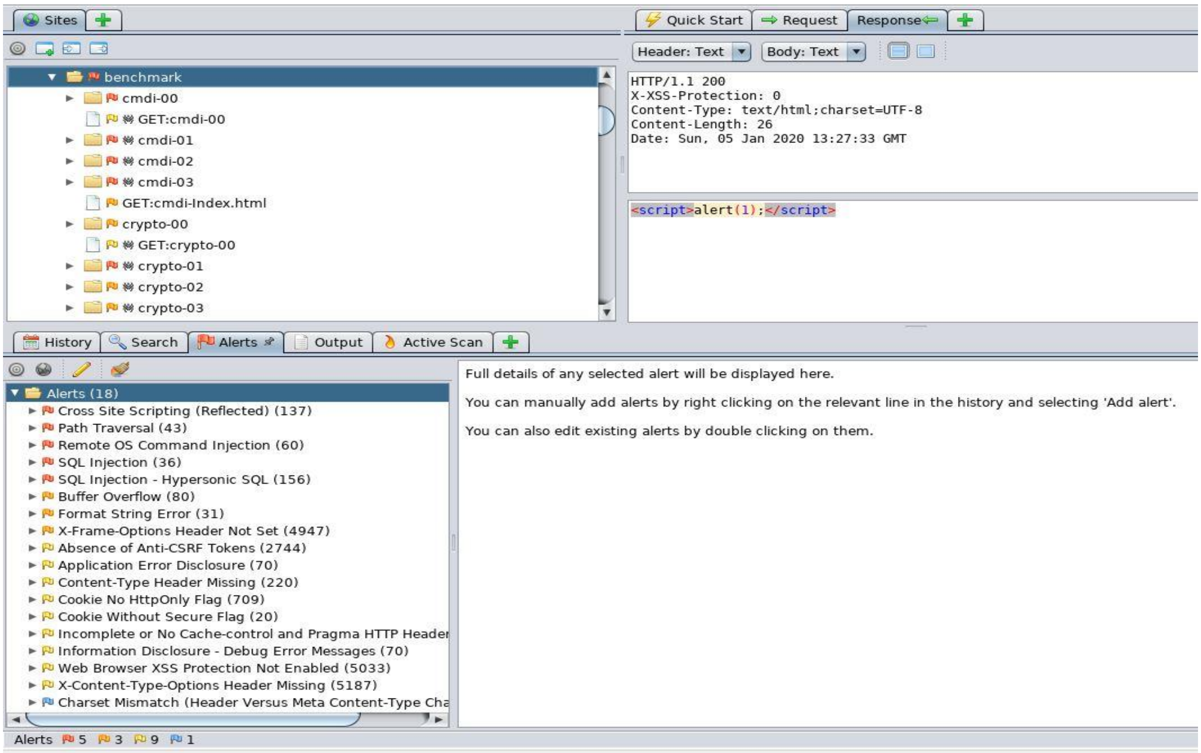
☑ In Attack mode always rescan nodes when scope changed

Default active scan policy:

Attack mode scan policy:

Figure 4.4.1: ZAP configuration

Step 5: Now right click on the target URL in site map and click on 'Active scan'. This will actively crawl the URL and then perform scan as well. As shown in the following figure.



- benchmark
  - cmdi-00
    - GET:cmdi-00
  - cmdi-01
  - cmdi-02
  - cmdi-03
  - GET:cmdi-Index.html
  - crypto-00
    - GET:crypto-00
  - crypto-01
  - crypto-02
  - crypto-03

```
HTTP/1.1 200
X-XSS-Protection: 0
Content-Type: text/html;charset=UTF-8
Content-Length: 26
Date: Sun, 05 Jan 2020 13:27:33 GMT
```

```
<script>alert(1);</script>
```

- Alerts (18)
  - Cross Site Scripting (Reflected) (137)
  - Path Traversal (43)
  - Remote OS Command Injection (60)
  - SQL Injection (36)
  - SQL Injection - Hypersonic SQL (156)
  - Buffer Overflow (80)
  - Format String Error (31)
  - X-Frame-Options Header Not Set (4947)
  - Absence of Anti-CSRF Tokens (2744)
  - Application Error Disclosure (70)
  - Content-Type Header Missing (220)
  - Cookie No HttpOnly Flag (709)
  - Cookie Without Secure Flag (20)
  - Incomplete or No Cache-control and Pragma HTTP Header
  - Information Disclosure - Debug Error Messages (70)
  - Web Browser XSS Protection Not Enabled (5033)
  - X-Content-Type-Options Header Missing (5187)
  - Charset Mismatch (Header Versus Meta Content-Type Cha

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

Figure 4.4.2: ZAP in active scan

Step 6: The scan is in progress and once the scan is completed export the result in .xml format.

4.5 OWASP Benchmark -Report generating tool

Step 1: Collect all the scan outputs in .xml format and copy them to benchmark results folder.

- Results folder: ./Downloads/Benchmark/results

Step 2: Run the ‘createScorecard.sh’ file in the Benchmark folder.

- ./createScorecard.sh

This will generate benchmark score and graphical representation for all the reports in the ‘reports’ folder and store them in ‘scorecard’ folder.

Then we take these results and interpret them as per our framework and evaluate the scanner.

5 References

[1] B. Mburano and W. Si, "Evaluation of Web Vulnerability Scanners Based on OWASP Benchmark," in *26th International Conference on Systems Engineering (ICSEng)*, Sydney, Australia, Australia, 2018.