Configuration Manual

MSc Research Project
MSC in Cyber Security

Drisya Mohan Kondhankuzhiyil Radhamohanan
Student ID: 22210504

School of Computing
National College of Ireland

Supervisor: Kamil Mahajan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: DRISYA MOHAN KONDHANKUZHIYIL RADHAMOHANAN

Student ID: 22210504

Programme: MSC CYBER SECURITY **Year:** 2024

Module: INTERNSHIP

Lecturer: KAMIL MAHAJAN

Submission Due Date: 02/09/2024

Project Title: Comparative study of SAST and DAST tools with Manual penetration testing methods for Improving the identification of business logic vulnerabilities of authorization flaws and broken access control and false positive vulnerabilities for enhanced Web application Security

Word Count: 1409 **Page Count:** 11

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.

Signature: DRISYA MOHAN KONDHANKUZHIYIL RADHAMOHANAN

Date: 01/09/2024

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

Drisya Mohan Kondhankuzhiyil Radhamohanan
Student ID: 22210504

1 Introduction

This Configuration manual will be describing the methodology and steps involved in the research work of the Comparative study of SAST and DAST tools with Manual penetration testing methods for Improving the identification of business logic vulnerabilities of authorization flaws and broken access control and false positive vulnerabilities for enhanced Web application Security. It will be providing an insight towards the installation, configuration and execution of the tools which is part of this research work. System configuration will be begun with the installation and configuration of Kali Linux in the virtual box. After completing the system configuration, website hosting and installation and configuration of SAST and DAST tool will be taking place. SonarQube is considered for the SAST tool testing and Burp suite taken for DAST tool testing. Once the tools are up and running perform vulnerability assessment and collect the generated report. In order to perform manual penetration testing burp suite, itself is taken for intercepting traffic and provide attack scenarios. Based on the result analysis the effectiveness of identifying security weaknesses and issues using automated tools and manual pen testing methods explored. Which is the aim of this research project.

2 System Configuration

Host Machine:

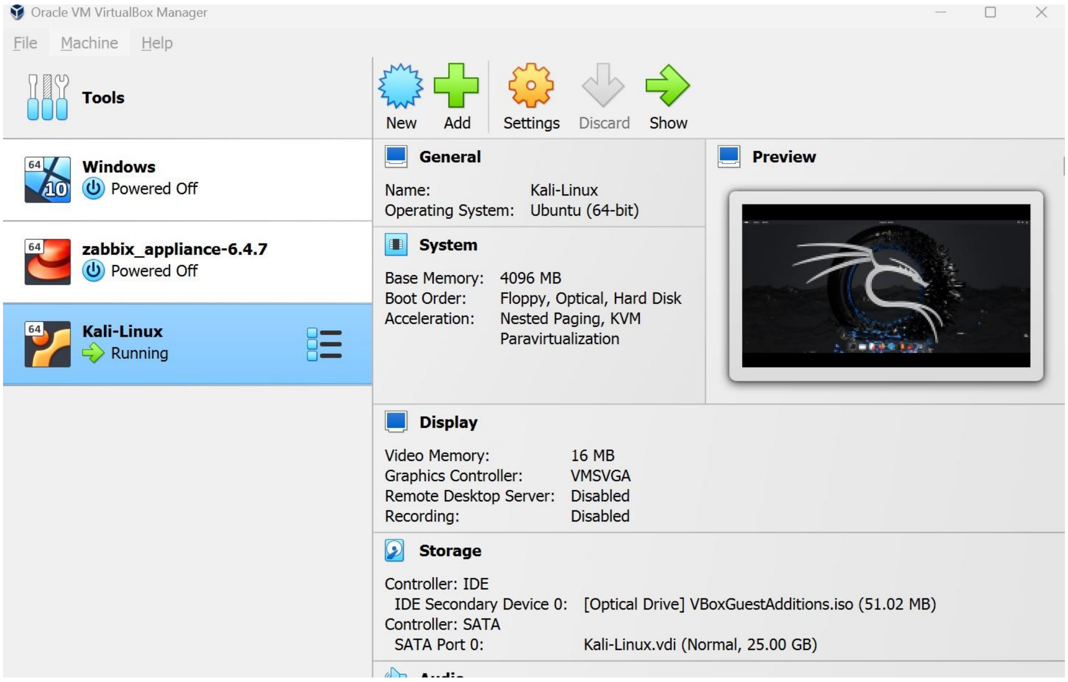
- System Type: X64 Based Processor
- Processor: 12th Gen Intel(R) 1.30 GHz
- Operating system: Microsoft windows 11
- RAM :16.0 GB

Virtual Machine:

- System Type: 64-bit operating system
- Processor: 4 processor cores
- Operating System: Ubuntu 64 bit
- Memory: 4096 MB
- Video Memory: 16MB

2.1 Installation and Configuration of Kali Linux in Virtual Box.

In order to download and install Kali Linux, initially virtual box have to download and setup. From the Oracle VM virtual box website latest version of Virtual box downloaded and installed on the Host machine. Kali Linux iso image also downloaded from website and installed on the virtual machine.[1]



Windows
Powered Off

zabbix_appliance-6.4.7
Powered Off

Kali-Linux
Running

General

Name: Kali-Linux
Operating System: Ubuntu (64-bit)

System

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Preview

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] VBoxGuestAdditions.iso (51.02 MB)
Controller: SATA
SATA Port 0: Kali-Linux.vdi (Normal, 25.00 GB)

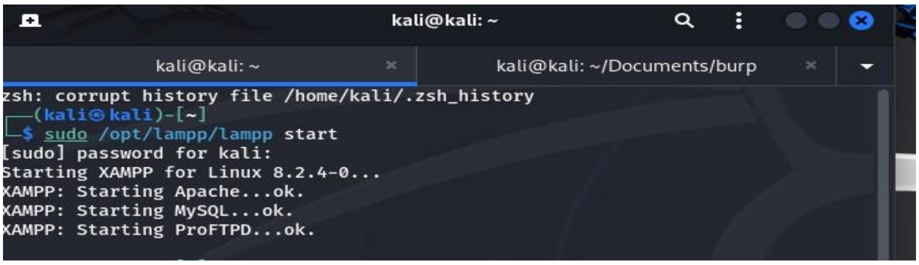
Figure 1: Kali Linux Installed on Oracle VM VirtualBox

3 Environment Setup

After the successful configuration of the virtual environment, in order to test the website interface, it is required to host the website through the local host. An E-commerce PHP website project selected from Code Astro website and for hosting the PHP project LAMP stack will be used. For setting up a local web server XAMPP platform used. It includes the webserver Apache and database MYSQL which is required for this project.

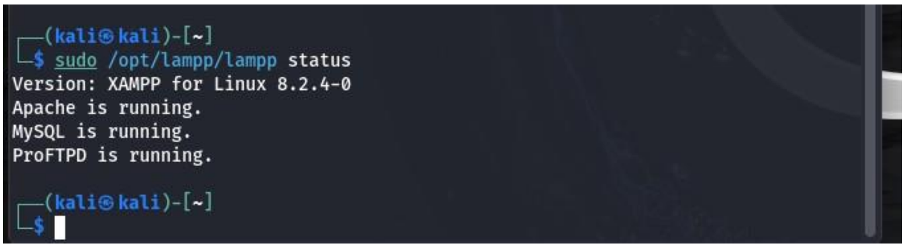
3.1 XAMPP installation:

XAMPP can be downloaded and installed from the Apache website. After the installation procedure XAMPP control panel can be used for starting as well as stopping the services such as Apache, MySQL and others. After setting up the XAMPP services, the web application files can be saved in the htdocs folder in the LAMP directory and access the web browser through local host.



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo /opt/lampp/lampp start
[sudo] password for kali:
Starting XAMPP for Linux 8.2.4-0...
XAMPP: Starting Apache...ok.
XAMPP: Starting MySQL...ok.
XAMPP: Starting ProFTPD...ok.
```

Figure 2. XAMPP Installation and running.



```
┌──(kali㉿kali)-[~]
└─$ sudo /opt/lampp/lampp status
Version: XAMPP for Linux 8.2.4-0
Apache is running.
MySQL is running.
ProFTPD is running.

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 3. XAMPP running status.

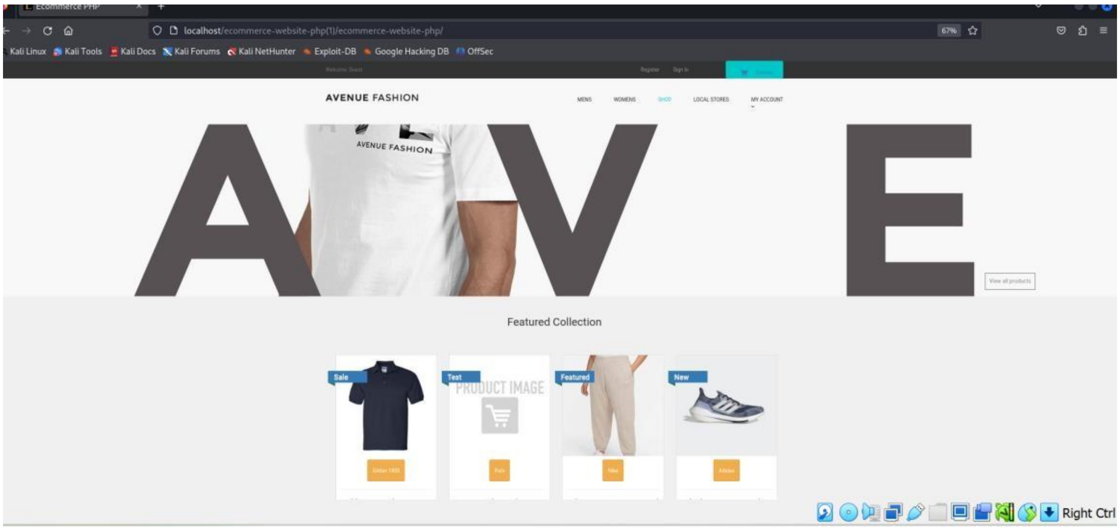
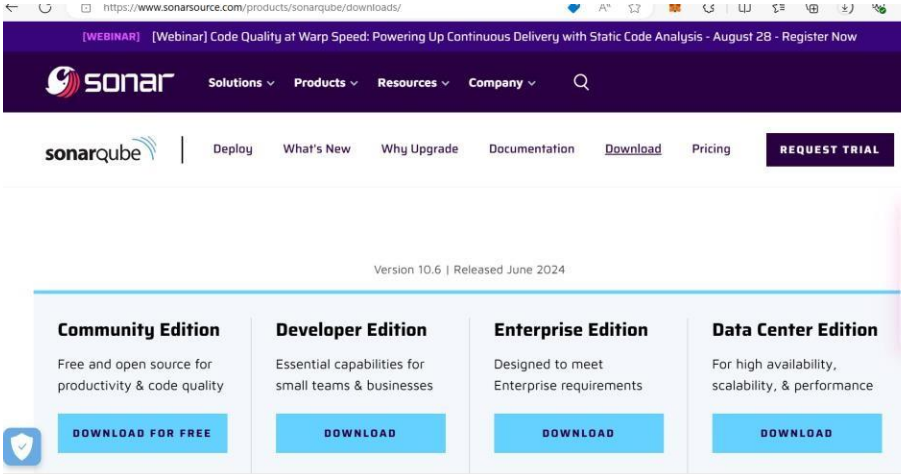


Figure 4. Website Hosting through local host

3.2 Installation and Configuration of SAST and DAST Tool

- **SonarQube**

Sonarqube is a Static Application Security Testing tool developed for analysing static code and identify the vulnerabilities present in the application. In order to operate the SonarQube it requires the Java 11 or 17. In order to that OpenJDK needs to be installed on the system. After that SonarQube Community edition Downloaded from Sonarqube official Website. Later Sonarqube Server can start by providing the StartSonar.bat. When the instance is up and running, we can login to the path http://localhost:9000 with default user credentials such as username as admin and Password also as admin. After that password can be modified with the user choice. [2] After successful installation of Sonarqube, user needs to install Sonar scanner as well. It is required for integrating the Sonarqube with the php source code. It can also download from the Sonar scanner download page and set the environmental variables. After that user can navigate to the project directory and execute the scanner. Once login to the localhost Sonarqube instance we can create new project and select the php source code for the website. By generating a token, we can run and analyze the project. After completing the source code scan Sonarqube will provide the analysis report explaining the open security issues, reliability security hotspot and all.



[WEBINAR] [Webinar] Code Quality at Warp Speed: Powering Up Continuous Delivery with Static Code Analysis - August 28 - Register Now

Version 10.6 | Released June 2024

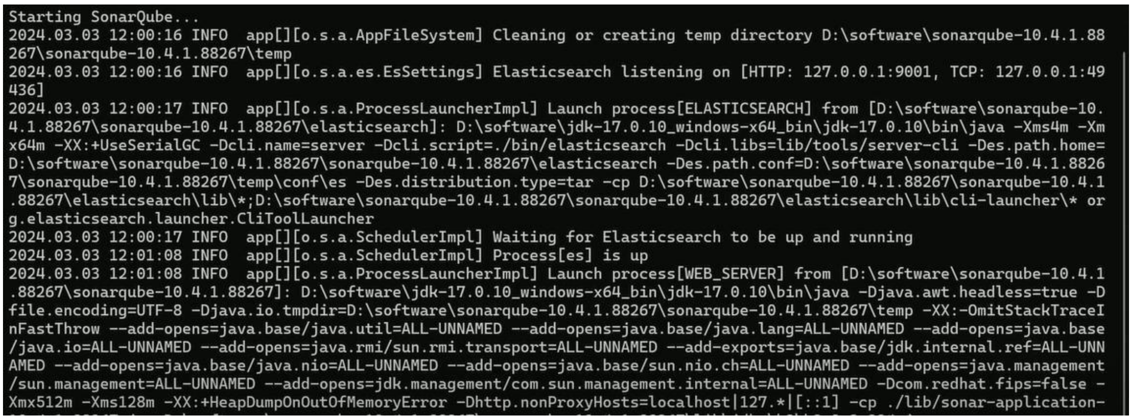
Community Edition
Free and open source for productivity & code quality

Developer Edition
Essential capabilities for small teams & businesses

Enterprise Edition
Designed to meet Enterprise requirements

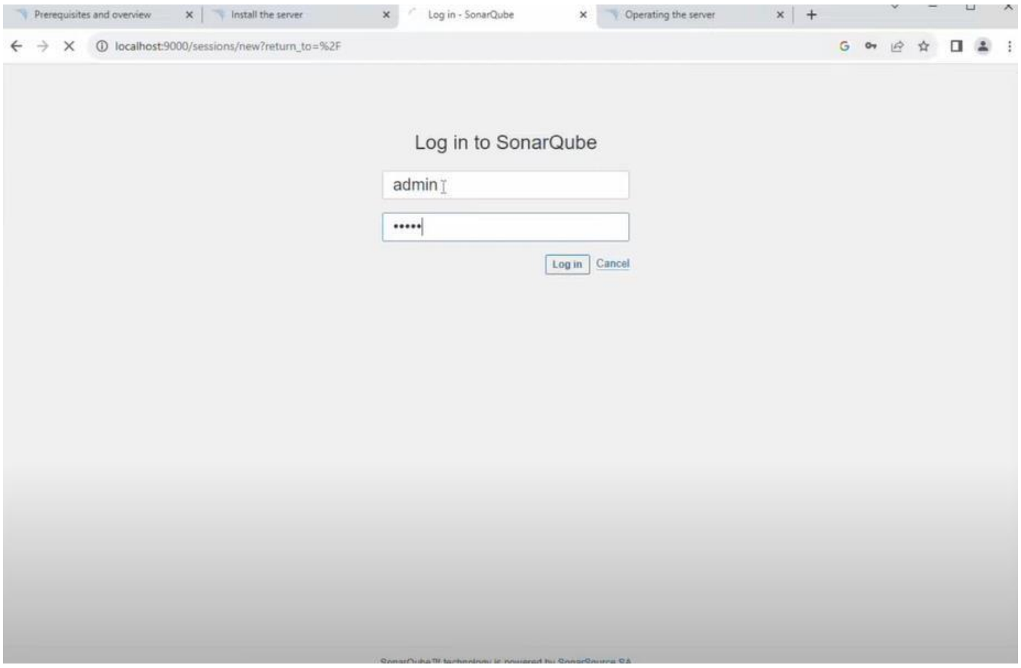
Data Center Edition
For high availability, scalability, & performance

Figure 5. Downloading Sonarqube



```
Starting SonarQube...
2024.03.03 12:00:16 INFO  app[][o.s.a.AppFileSystem] Cleaning or creating temp directory D:\software\sonarqube-10.4.1.88
267\sonarqube-10.4.1.88267\temp
2024.03.03 12:00:16 INFO  app[][o.s.a.es.EsSettings] Elasticsearch listening on [HTTP: 127.0.0.1:9001, TCP: 127.0.0.1:49
436]
2024.03.03 12:00:17 INFO  app[][o.s.a.ProcessLauncherImpl] Launch process[ELASTICSEARCH] from [D:\software\sonarqube-10.
4.1.88267\sonarqube-10.4.1.88267\elasticsearch]: D:\software\jdk-17.0.10_windows-x64_bin\jdk-17.0.10\bin\java -Xms4m -Xm
x64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=./bin/elasticsearch -Dcli.libs=lib/tools/server-cli -Des.path.home=
D:\software\sonarqube-10.4.1.88267\sonarqube-10.4.1.88267\elasticsearch -Des.path.conf=D:\software\sonarqube-10.4.1.8826
7\sonarqube-10.4.1.88267\temp\conf\es -Des.distribution.type=tar -cp D:\software\sonarqube-10.4.1.88267\sonarqube-10.4.1
.88267\elasticsearch\lib\*;D:\software\sonarqube-10.4.1.88267\sonarqube-10.4.1.88267\elasticsearch\lib\cli-launcher\* or
g.elasticsearch.launcher.CliToolLauncher
2024.03.03 12:00:17 INFO  app[][o.s.a.SchedulerImpl] Waiting for Elasticsearch to be up and running
2024.03.03 12:01:08 INFO  app[][o.s.a.SchedulerImpl] Process[es] is up
2024.03.03 12:01:08 INFO  app[][o.s.a.ProcessLauncherImpl] Launch process[WEB_SERVER] from [D:\software\sonarqube-10.4.1
.88267\sonarqube-10.4.1.88267]: D:\software\jdk-17.0.10_windows-x64_bin\jdk-17.0.10\bin\java -Djava.awt.headless=true -D
file.encoding=UTF-8 -Djava.io.tmpdir=D:\software\sonarqube-10.4.1.88267\sonarqube-10.4.1.88267\temp -XX:-OmitStackTraceI
nFastThrow --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base
/java.io=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED --add-exports=java.base/jdk.internal.ref=ALL-UNN
AMED --add-opens=java.base/java.nio=ALL-UNNAMED --add-opens=java.base/sun.nio.ch=ALL-UNNAMED --add-opens=java.management
/sun.management=ALL-UNNAMED --add-opens=jdk.management/com.sun.management.internal=ALL-UNNAMED -Dcom.redhat.fips=false -
Xmx512m -Xms128m -XX:+HeapDumpOnOutOfMemoryError -Dhttp.nonProxyHosts=localhost|127.*|[::1] -cp ./lib/sonar-application-
```

Figure 6. Starting Sonarqube

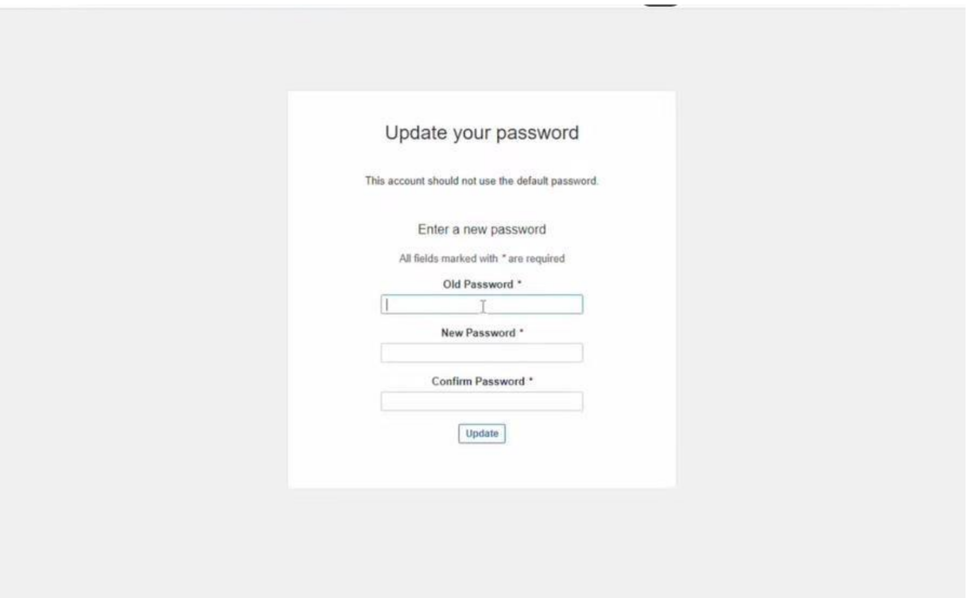


Log in to SonarQube

admin

•••••

Figure 7 .Login to Sonar Qube as Admin



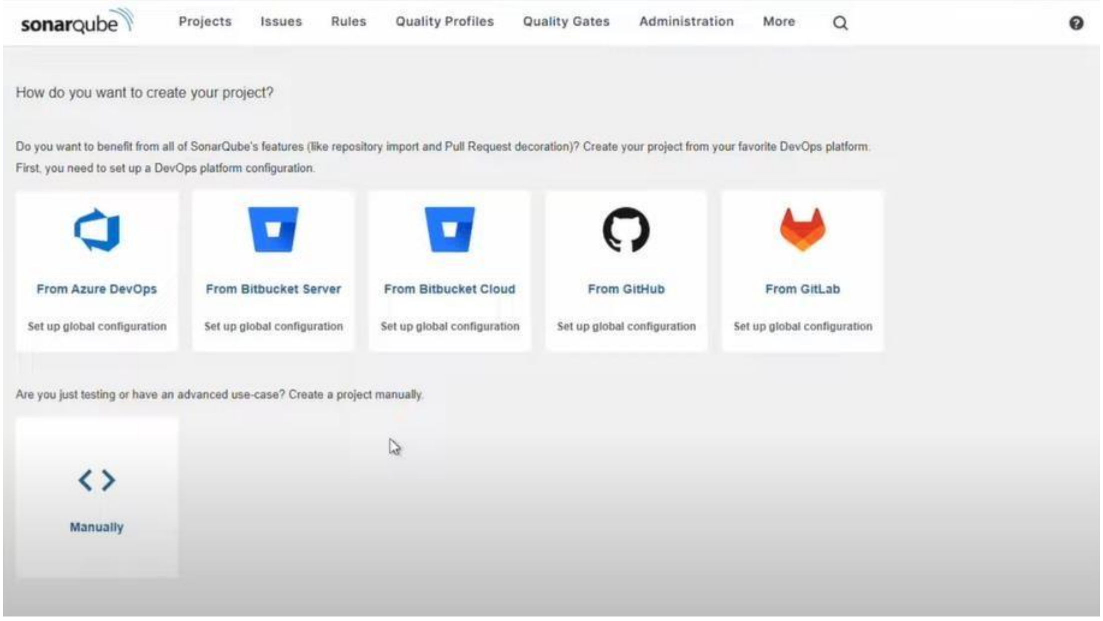
Update your password

This account should not use the default password.

Enter a new password

All fields marked with * are required

Figure 8 .Updating login credentials



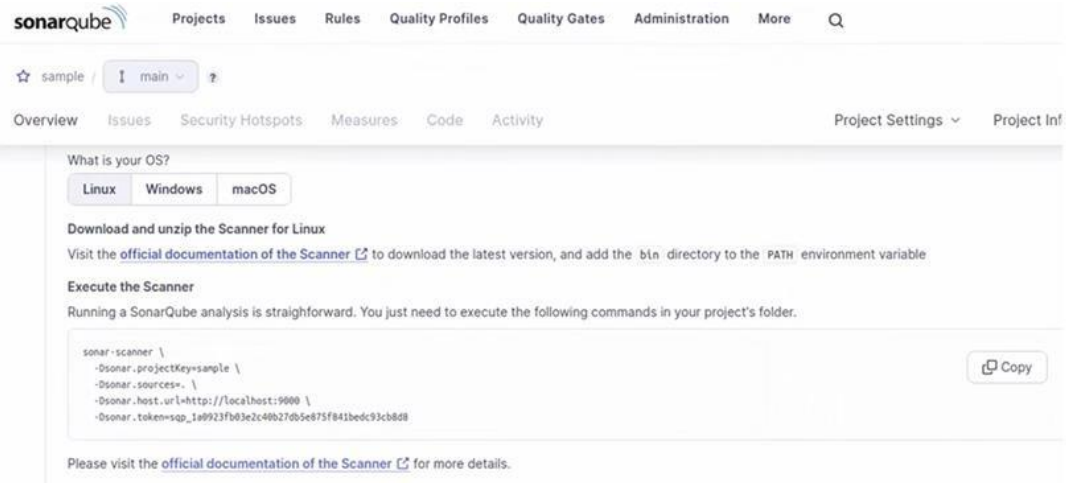
How do you want to create your project?

Do you want to benefit from all of SonarQube's features (like repository import and Pull Request decoration)? Create your project from your favorite DevOps platform.
First, you need to set up a DevOps platform configuration.

From Azure DevOps
Set up global configuration
From Bitbucket Server
Set up global configuration
From Bitbucket Cloud
Set up global configuration
From GitHub
Set up global configuration
From GitLab
Set up global configuration

Are you just testing or have an advanced use-case? Create a project manually.

Figure 9. Create new project Manually



What is your OS?

Download and unzip the Scanner for Linux

Visit the official documentation of the Scanner to download the latest version, and add the `bin` directory to the `PATH` environment variable

Execute the Scanner

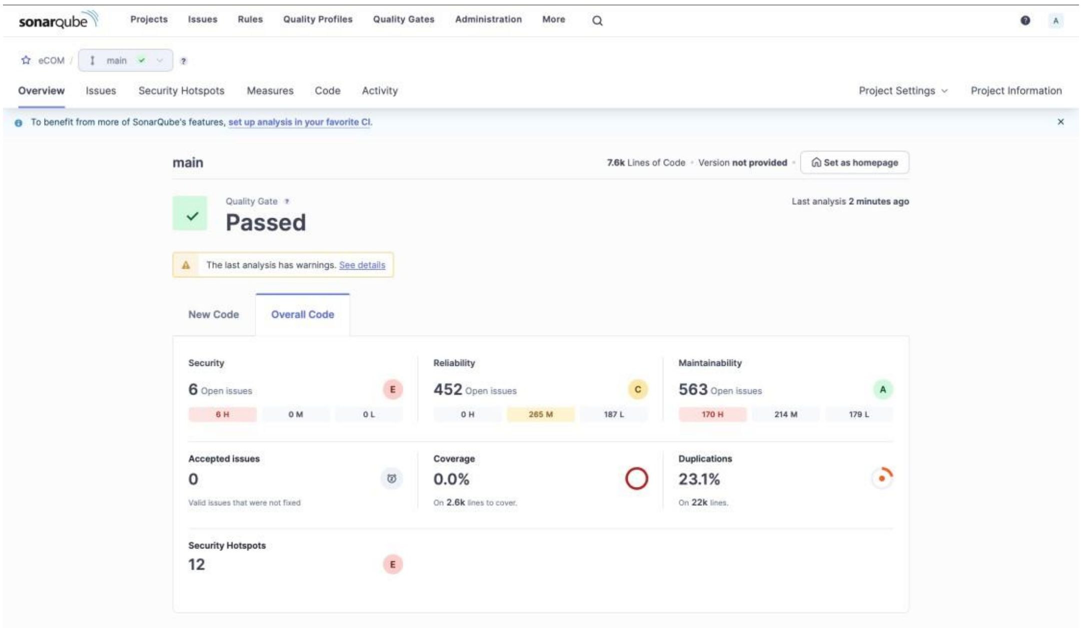
Running a SonarQube analysis is straighforward. You just need to execute the following commands in your project's folder.

```
sonar-scanner \
  -Dsonar.projectKey=sample \
  -Dsonar.sources=. \
  -Dsonar.host.url=http://localhost:9000 \
  -Dsonar.token=sqp_1a0923fb03e2c40b27db5e875f841bedc93cb8d8
```

Please visit the official documentation of the Scanner for more details.

Figure 10. Generating token for

authenticationAfter complete the scan generates report.



To benefit from more of SonarQube's features, set up analysis in your favorite CI.

main

7.6k Lines of Code · Version not provided

Quality Gate

Passed

Last analysis 2 minutes ago

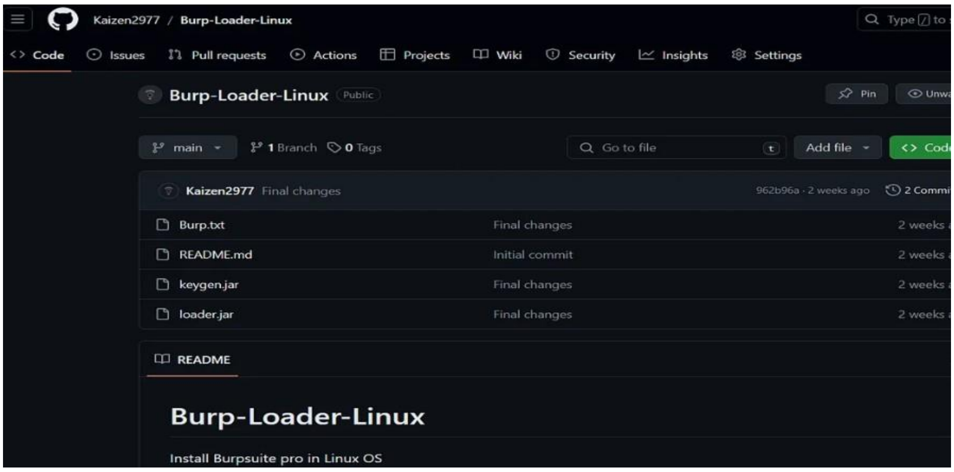
The last analysis has warnings. See details

Security	Reliability	Maintainability
6 Open issues E	452 Open issues C	563 Open issues A
6 H · 0 M · 0 L	0 H · 265 M · 187 L	170 H · 214 M · 179 L
Accepted issues	**Coverage**	**Duplications**
0	0.0%	23.1%
Valid issues that were not fixed	On 2.6k lines to cover.	On 22k lines.
Security Hotspots		
12 E		

Figure 11. SonarQube scan generated results

- **Burpsuite**

Burp Suite is a powerful web vulnerability scanner which can be useful for identifying the vulnerabilities present in the web application. In the Kali Linux Burp Suite community edition is pre-installed. In order to perform automated scanning in this research project , Cracked version of Burp suite enterprise edition is used. Initially Burpsuite professional JAR file is downloaded from the portswigger releases page. Further the Burp Loader files downloaded from Github.[3]



Kaizen2977 / Burp-Loader-Linux

Burp-Loader-Linux Public

main · 1 Branch · 0 Tags

Kaizen2977 Final changes 962b96a · 2 weeks ago

```
Burp.txt        Final changes    2 weeks
README.md       Initial commit   2 weeks
keygen.jar      Final changes    2 weeks
loader.jar      Final changes    2 weeks
```

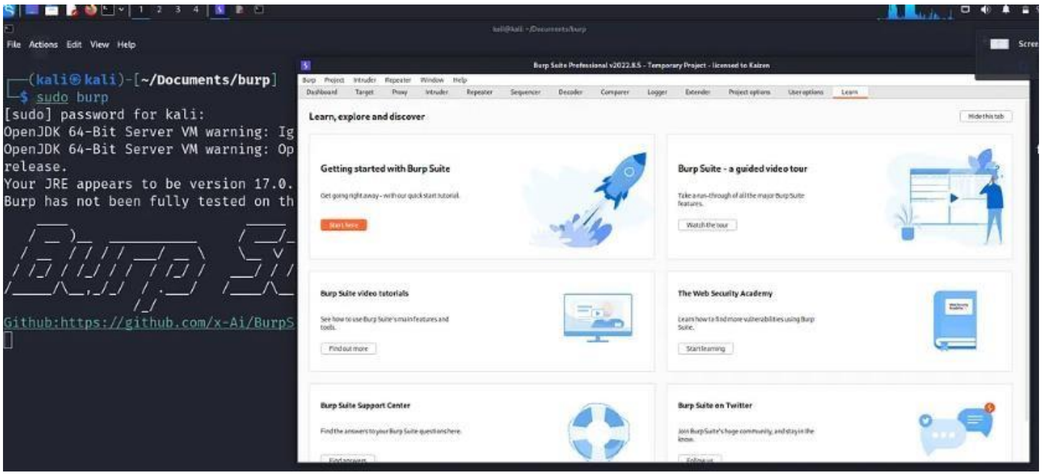
README

Burp-Loader-Linux

Install Burpsuite pro in Linux OS

Figure 12.Downloading Burp Loader files from Github

After providing the execution permission to the keygen.jar and loader.jar file access permitted to the burp suite pro version.

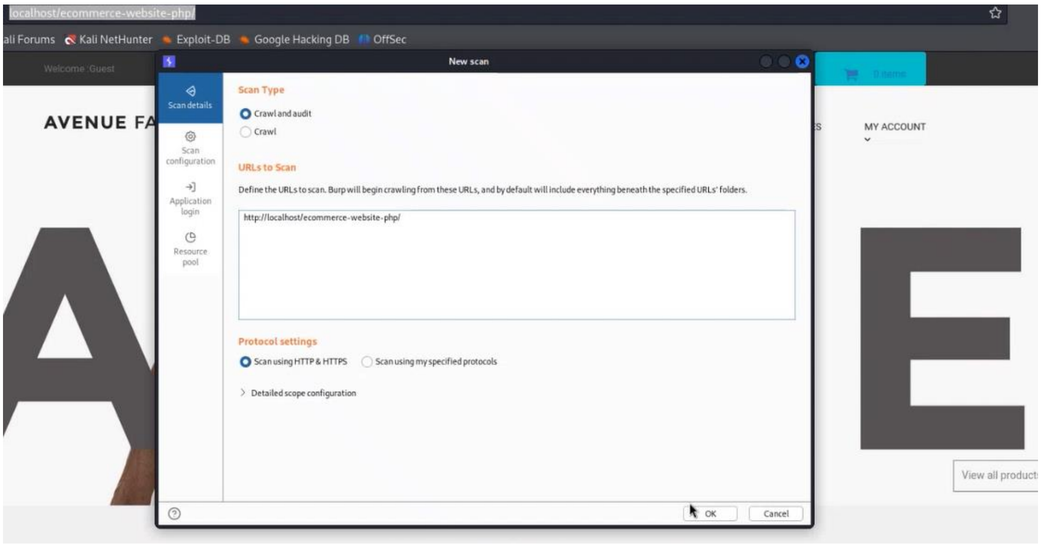


```
┌──(kali㉿kali)-[~/Documents/burp]
└─$ sudo burp
[sudo] password for kali:
OpenJDK 64-Bit Server VM warning: Ig
OpenJDK 64-Bit Server VM warning: Op
release.
Your JRE appears to be version 17.0.
Burp has not been fully tested on th

Github:https://github.com/x-Ai/BurpS
```

File Actions Edit View Help
Burp Suite Professional v2022.8.5 - Temporary Project - licensed to Kaizen
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Learn, explore and discover
Getting started with Burp Suite
Get going right away - with our quick start tutorial.
Start here
Burp Suite - a guided video tour
Watch the tour
Burp Suite video tutorials
See how to use Burp Suite's main features and tools.
Find out more
The Web Security Academy
Start learning
Burp Suite Support Center
Find the answers to your Burp Suite questions here.
Burp Suite on Twitter

Figure 13. Starting Burpsuite



New scan

Scan Type

● Crawl and audit
○ Crawl

URLs to Scan

Define the URLs to scan. Burp will begin crawling from these URLs, and by default will include everything beneath the specified URLs' folders.

http://localhost/ecommerce-website-php/

Protocol settings

● Scan using HTTP & HTTPS ○ Scan using my specified protocols

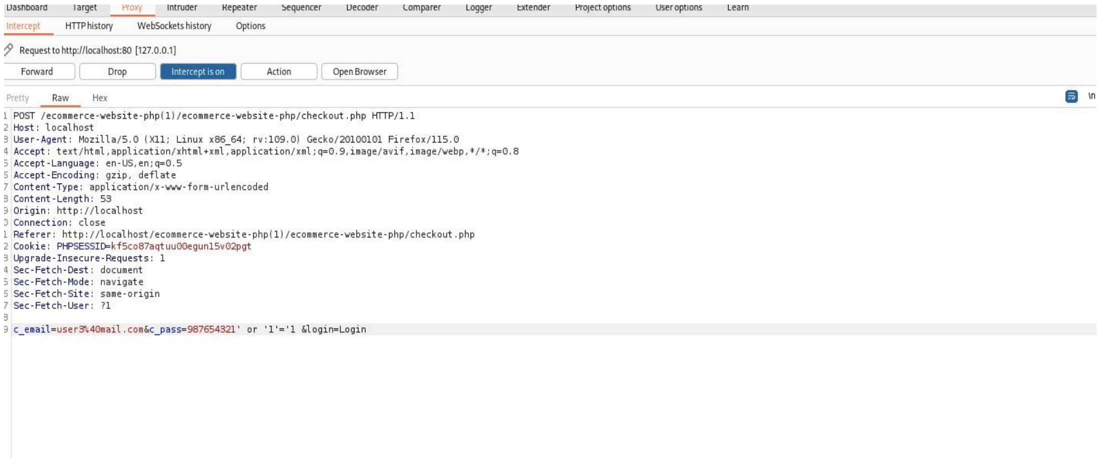
> Detailed scope configuration

Figure 14. Configuration in Burpsuite

After starting the burp suite start a temporary project will get started . From the dashboard select the New scan tab and provide the necessary configurations. Scan type will be selected as crawl and audit, then provides the website URL to scan while forwarding select lightweight after that scan gets started.

- Manual Penetration testing

Manual penetration testing approaches will be helpful for identifying the security issues automated tools might miss. In order to perform manual testing, the community edition of Burp suite present in the kali Linux used in this project. In order to intercept and analyse the traffic burp suite proxy configured in the web browser. After providing the proxy settings and installing the Burp suite certificate, open a new project in the burp suite tool. After that the user can visit the website by turning on the interception. From the intercept tab in the tool the user can view, modify and forward the requests. Repeater tool in the burp suite will be helpful for sending requests multiple times and modify each time.



Request to http://localhost:80 [127.0.0.1]

```
POST /ecommerce-website-php(1)/ecommerce-website-php/checkout.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin: http://localhost
Connection: close
Referer: http://localhost/ecommerce-website-php(1)/ecommerce-website-php/checkout.php
Cookie: PHPSESSID=kf5co87aqtuu00egun15v02pgt
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

c_email=user3%40mail.com&c_pass=987654321' or '1'='1 &login=Login
```

Figure 15. Intercept traffic for manual testing

References

References should be formatted using APA or Harvard style as detailed in NCI Library Referencing Guide available at https://libguides.ncirl.ie/referencing
You can use a reference management system such as Zotero or Mendeley to cite in MS Word.

Phoenixnap. (2024).' How to Install Kali Linux on VirtualBox'[Online] Available at: https://phoenixnap.com/kb/how-to-install-kali-linux-on-virtualbox

SonarSource. 'Install the server'. *SonarQube Docs*. [Online] Available at:https://docs.sonarsource.com/sonarqube/9.9/setup-and-upgrade/install-the-server/

C. Kapil,(2024),'Install Burp Suite Pro Free on Linux'[Online],Available at:Install Burp Suite Pro Free on Linux | by Kapil Chotalia | Medium