National College of Ireland

Configuration Manual

MSc. Practicum Part 2
Cybersecurity (MSCCYB1_A)

Jagadish Babu Sake
Student ID: x23310341

National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Jagadish Babu Sake
Student ID:	X23310341
Programme:	MSc Practicum Part 2 **Year:** 2024-2025
Module:	Research Project
Supervisor:	Vikas Sahni
Submission Due Date:	11th August 2025
Project Title:	Collaborative Detection of SQL Injection Attacks using SIEM,Wazuh Agent and Next Generation Firewalls

Word Count: 2714 **Page Count** 19

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: Jagadish Babu Sake

Date: 10 August 2025

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

Jagadish Babu Sake
Student ID:x2310341

Objectives:

This guide will walk you through installing and configuring the Wazuh SIEM (security information and event management) on an Ubuntu 22.04 server and a Windows 10 system with the Wazuh Agent. The objective is to facilitate researchers the setup of a Wazuh system for detecting and logging a SQLI attack, and the configuration of the OPNsense along with the Zenarmor plugin for the extensive Deep Packet Inspection (DPI). And integration of all the machines Ubuntu, Windows 10 (Victim), Kali Linux (Attacker).
The user will be always able to do:

- How To Install Wazuh Server On Ubuntu 18.04 Introduction Wazuh server is an all-in-one security platform based on OSSEC and EDR.
- Install Wazuh Agent in a Windows 10 for monitoring logs and also the installation and setup of insecure web application DVWA.
- Set up both the components to work with OPNSense and Zenarmor to detect SQL injection.
- The important setup for the log synchronization for initial log generation till the final log detection on SIEM.

This debugging manual provides detailed instructions, step-by-step instructions and screen-shots for users, for the research needs for monitoring SQLi attacks.

1. **System Configuration:** The setup is installed on VirtualBox VMs and following is the configuration details.
    a. *Host Machine:* 16 GB RAM, 512 GB SSD, Intel i7 CPU
    b. *Hypervisor:* VirtualBox Graphical User Interface Version 7.1.0

Table 1: Machines configuration detail

Machines	Memory (RAM)	Storage (HDD)	CPU	Operating System	Version
Wazuh	7 GB	30 GB	10	Ubuntu	Ubuntu Server 22.04 LTS
OPNsense	4 GB	25 GB	8	FreeBSD(64-bit)	OPNsense-25.7
Kali	7 GB	40 GB	10	Debian(64-bit)	Version 2024.3
Windows 10	7 GB	30 GB	10	Windows 10	Windows 10 (64-bit)

Requirement:

- All the virtual networks are routed in a way all the traffic should be passing through the OPNSense.
- All machines have the static IPs and gateway set via OPNsense.

- So that all the traffic can be monitored and to enhance the ability for Deep Packet Inspection (DPI).

2.Installing the Tools

2.1 Installation of Wazuh on Ubuntu:

- Update system packages on Ubuntu

```
sudo apt update && sudo apt upgrade -y
```

- Installing the prerequisite dependencies.

```
sudo apt install gnupg apt-transport
https curl wget lsb-release software-properties-common unzip -y
```

- Import Wazuh GPG key.

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH |
gpg --no-default-keyring
 --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg
--import
sudo chmod 644 /usr/share/keyrings/wazuh.gpg
```

- Install the Wazuh Manager.

```
sudo apt install wazuh-manager -y
```

- Install Filebeat

```
sudo apt install filebeat -y
```

- Download and Configure Filebeat Settings.

```
sudo curl -so /etc/filebeat/filebeat.yml
https://packages.wazuh.com/4.12/tpl/wazuh/filebeat/filebeat.yml
sudo nano /etc/filebeat/filebeat.yml
```

- Create Filebeat Keystore and Add Credentials.

```
sudo filebeat keystore create
echo admin | sudo filebeat keystore add username --stdin --force
echo admin | sudo filebeat keystore add password --stdin --force
```

- Download alerts template and install Filebeat Module.

```
sudo curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/v4.12.0/extensions/elasticsearch/7.x/wazuh-
template.json
sudo chmod go+r /etc/filebeat/wazuh-template.json
curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.4.tar.gz | sudo tar -xvz -C
/usr/share/filebeat/module
```

- Start and enable service.

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-manager
sudo systemctl start wazuh-manager

sudo systemctl enable filebeat
sudo systemctl start filebeat
```

- Check Installation Status

```
sudo systemctl status wazuh-manager
sudo systemctl status filebeat
sudo filebeat test output
```

- Make sure that both the services wazuh manager and filebeat ar active.
- After the successful installing the you can access the wazuh dashboard at http://192.168.30.10 with credentials that been provided during the installation.

Figure 1: Wazuh login page.

2.2 Installation of Wazuh agent on Windows:

- On the Wazuh dashboard navigate to the agent agent tab. Under it you have an option to add multiple agents for different OS like Windows, Linux and Mac OS.
- Choose it Windows option and select the version and provide the IPaddress of the Wazuh manager it will provide you with the installation link.
- This link need to be run on the agent machine with the administration terminal and run the link.This link will take 2 to 3 mintues depending on the internet, by downloading all the necessary repositories and libraries.

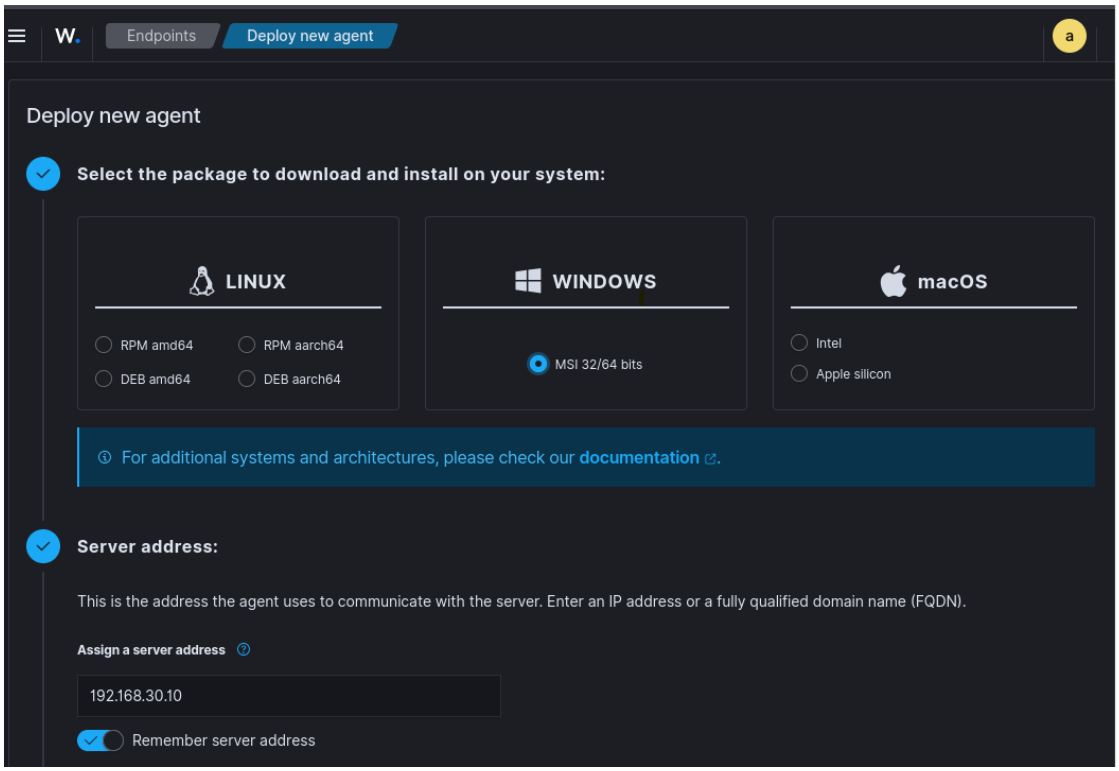

Figure 2: Deploying new agent on Wazuh.

2.3 Configure the Wazuh agent

- After the installation process the agent need to be configured. So as to share the connectivity and forward the logs to the Wazuh manager.
- Navigate to C:\Program Files (x86)\ossec-agent\ossec.conf using Notepad with admin privileges. Need to add the below dependencies to monitor the apache access logs.

```
<localfile>
<log_format>apache</log_format>
<location>C:\xampp\apache\logs\access.log</location>
</localfile>
<localfile>
<log_format>apache</log_format>
<location>C:\xampp\apache\logs\error.log</location>
</localfile>
```

- Crosscheck the Wazuh manager IP on the config file.

```
<client>
  <server>
    <address>192.168.30.10</address>
    <port>1514</port>
    <protocol>tcp</protocol>
  </server>
</client>
```

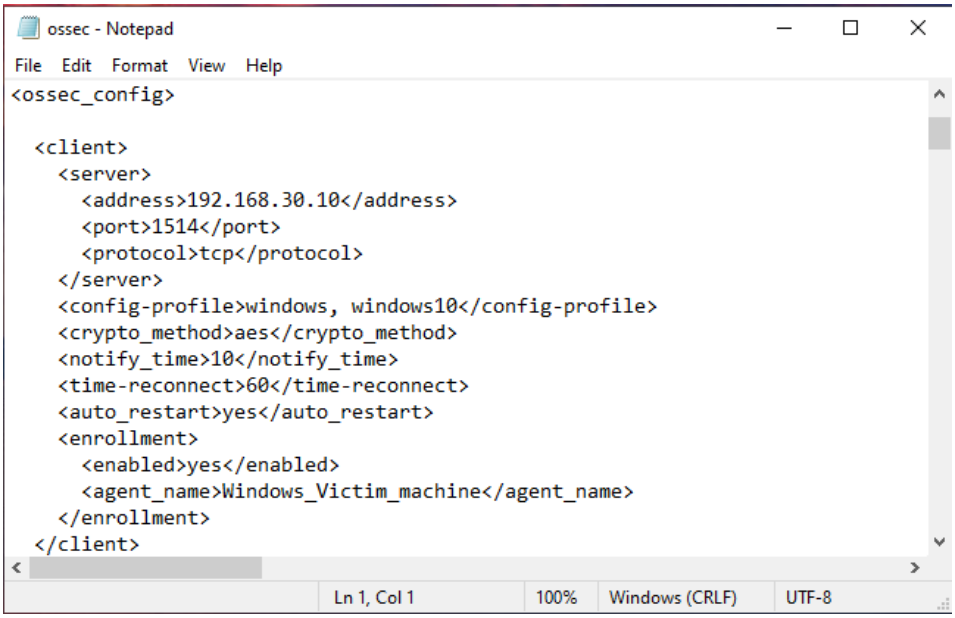

Figure 3: Ossec.config file setup

2.4 Registering the Wazuh agent with the Wazuh manager

- On the Ubuntu server add the windows agent.

```
sudo /var/ossec/bin/manage_agents
```

- Select “A” to add the agent. Enter the agent name and IP address. It will generate the agent ID and the agent KEY.
- On the windows machine import the key and paste from the manger.
- Start the Wazuh agent.

```
net start wazuh
```

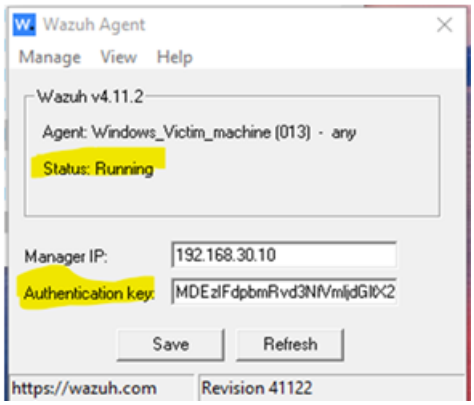

Figure 3: Ossec.config file setup

3.Installing the DVWA server on Windows machine.

3.1 Installing XAMPP.

- Visit the official XAMPP page and select the windows version and download the Installer.
- Run the installer with the **“administrator”.** It will be saved in the default path **C:\xampp.**

- After successful installation you will see a XAMPP control panel. In this panel **“START”** the **Apache** and **MySQL** by click the button next to it.

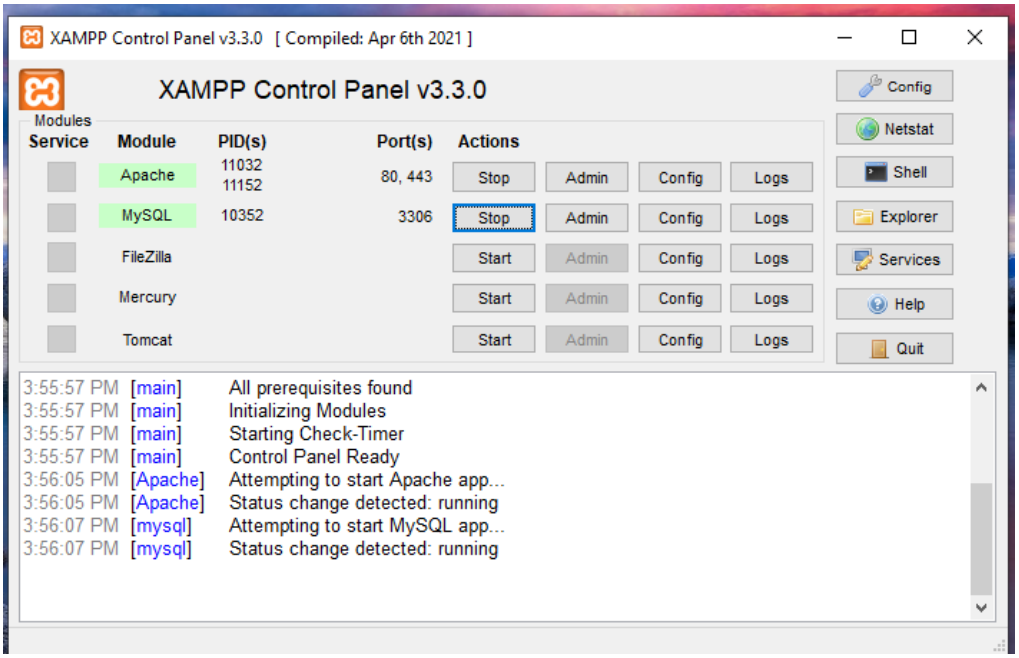

Figure 4: Xampp control panel

3.2 Installing DVWA.

- Navigate to **https://github.com/digininja/DVWA.** Click the code and Download the ZIP file.
- The downloaded the ZIP folder is extract in the location **“C:\xampp\htdocs\dvwa”.**
- Check the file structure and verify folder contains index.php, setup.php, config etc.

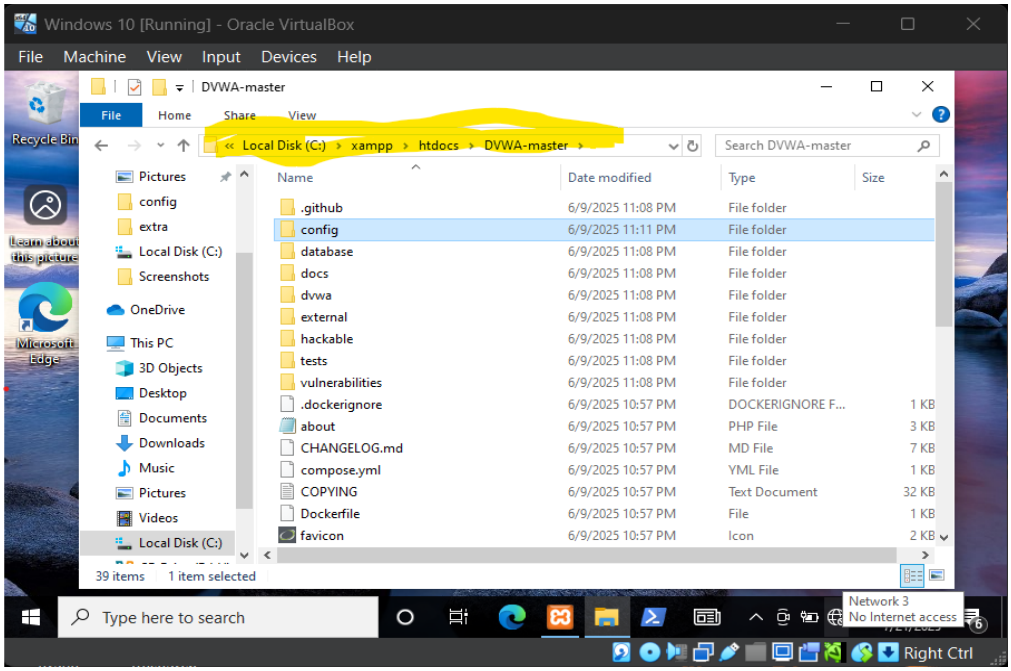

Figure 5: Configuration setup for Xampp

3.3 Configuring DVWA.

- Open the file location **" C:\xampp\htdocs\dvwa\config\config.inc.php"** in notepad with administrator access and update the database settings.

```
$_DVWA['db_server']   = 'localhost';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user']     = 'dvwa';
$_DVWA['db_password'] = 'p@ssw0rd';
```

- For the testing adjust the security level to "LOW".

```
$_DVWA['default_security_level'] = 'low';
```

- Save and exit the file.

3.4 Login and access DVWA.

- Open a browser and navigate to **http://192.168.20.20/dvwa**.
- If redirected to the setup page http://192.168.20.20/dvwa/setup.php. Here click on create and reset database.
- After the setup access http://192.168.20.20/dvwa/login.php.
- For Login use the default credentials username **"admin"** and password **"password".**

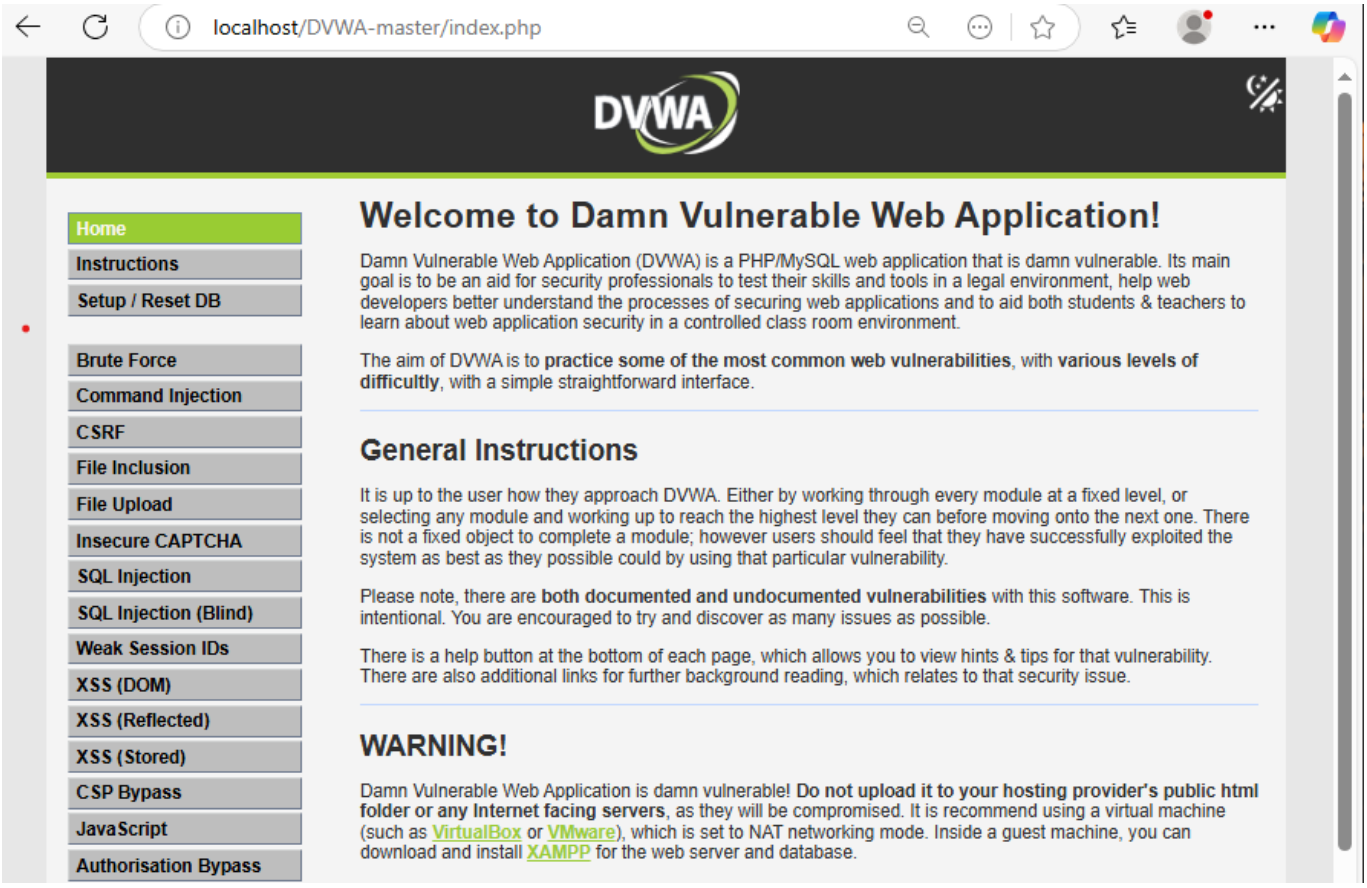

Figure 6: DVWA GUI page

4.Installing the OPNsense and Zenarmor.

4.1 Download the OPNsense software

- Download the ISO file for the official website **https://opnsense.org/download/.**
- Choose the architecture amd64 and image type DVD.

4.2 Create OPNsense on the Virtual machine.

- Create a new machine provide a name, type and version.
- Allocate the memory 4Gb and disk space 25Gb.
- **Network**

    - Adapter 1 → **Bridged Adapter** (testing in isolated lab)
    - Adapter 2 → **Internal Network** (intnet_opnsense for LAN)

- Mount ISO file. Go to **Settings > Storage** > Mount the downloaded .iso file in the optical drive.

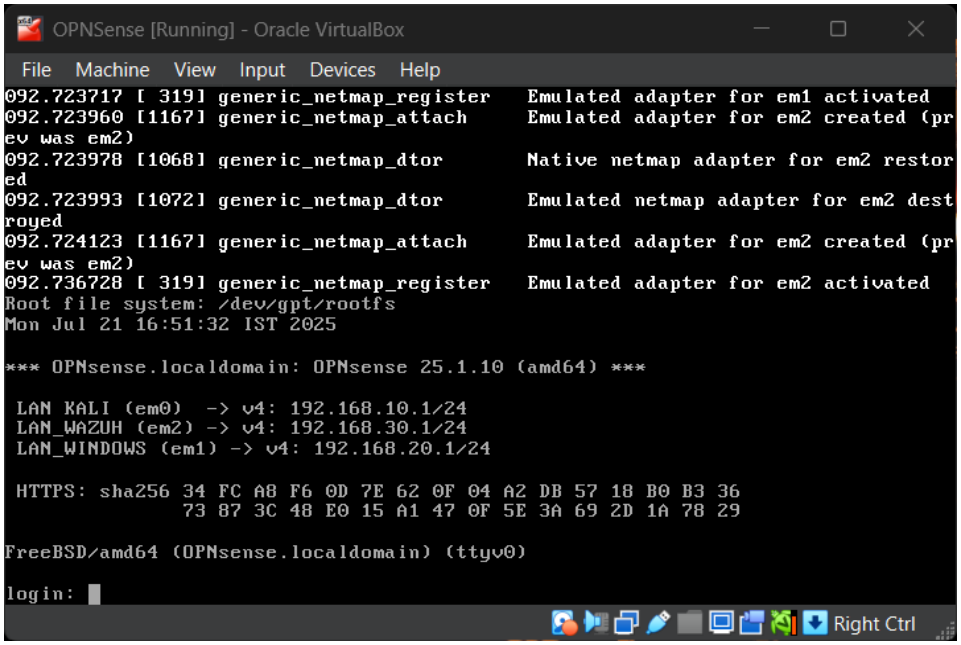

Figure 6: OPNsense assigning the interfaces

4.3 Assign the interfaces on OPNsense.

- From the opnsense CLI choose the option 1 for assign interface. It will automatically detect the locally available network like em0,em1and em2 for the LAN, WAN.
- Now choose the option 2 for the assigning the IP manually or we can use the DHCP, but for this experiment I choose manual IP assignment.
- Now save and exit. It will general the LAN link and can access the web interface from your host browser at http://<LAN_IP_ADDRESS> (default: http://192.168.30.1)
- Using the default login Username: **“root”** and Password: **“opnsense”**

Figure 7: OPNsense Login Page

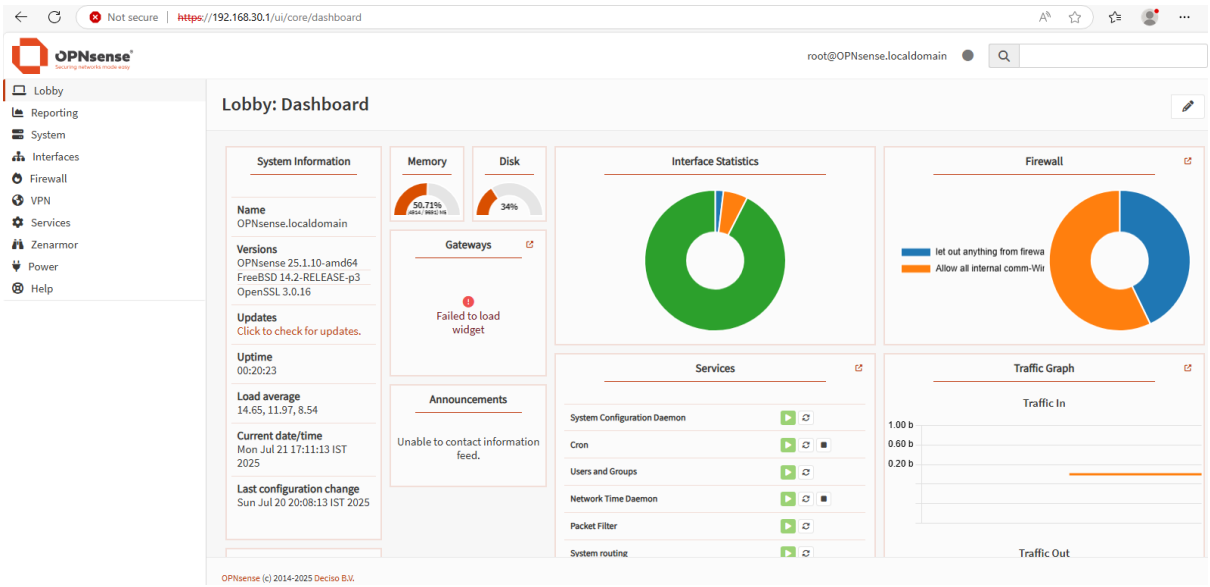

Figure 8: OPNsense Dashboard

4.4 Installing the Zenarmor plugin.

- Login to the OPNsense Web UI using the default credentials. Now navigate to **System →Firmware→Plugins.**
- In the plugin tab search for
    - For **Vendor Repository**: **os-sunnyvalley**
      Click the + icon to install.
    - For **Zenarmor/Sensei**: **os-sensei**
      Click the + icon to install. Confirm installation when prompted.
- After installing plugin now refresh the page. The **"Zenarmor"** will be added to the menu on the side bar on the left. Now you can access it.

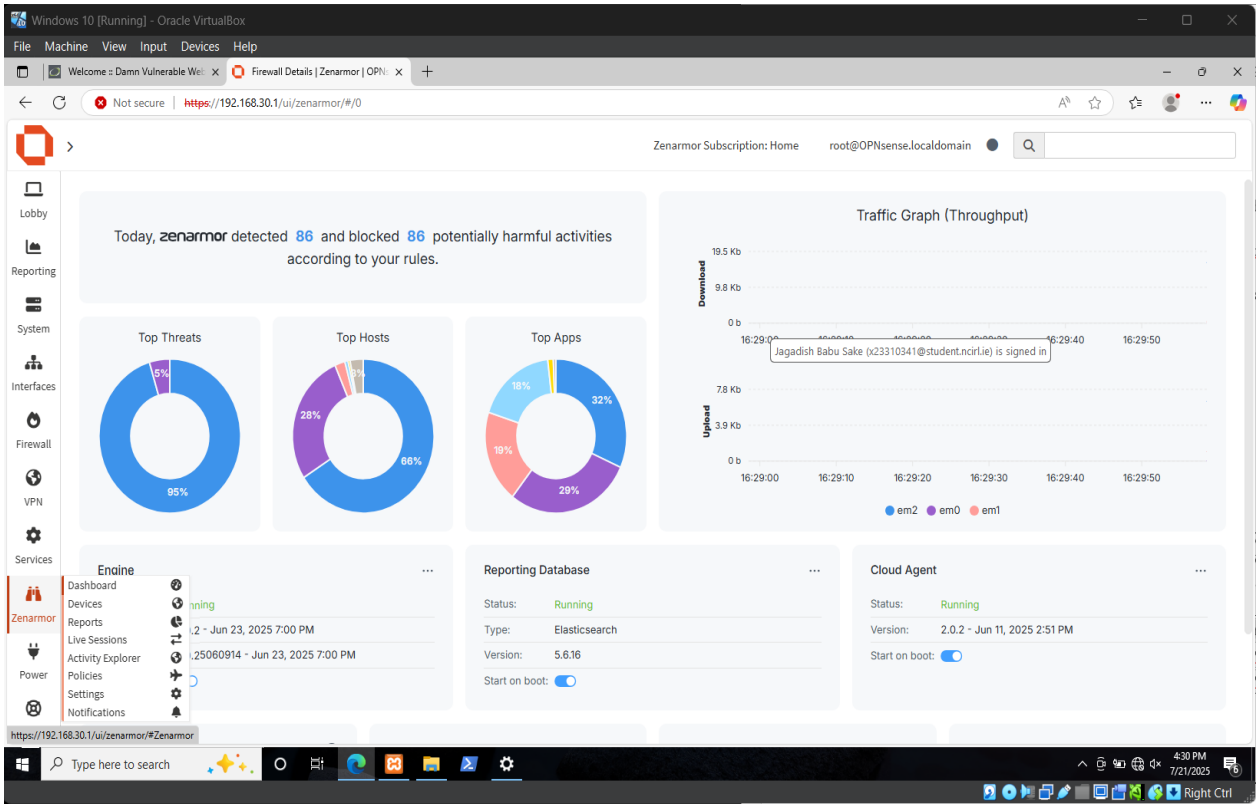

Figure 8: Zenarmor Dashboard

- Zenarmor policies tab. We can create our own customized policies for the sql injection attack scenarios.

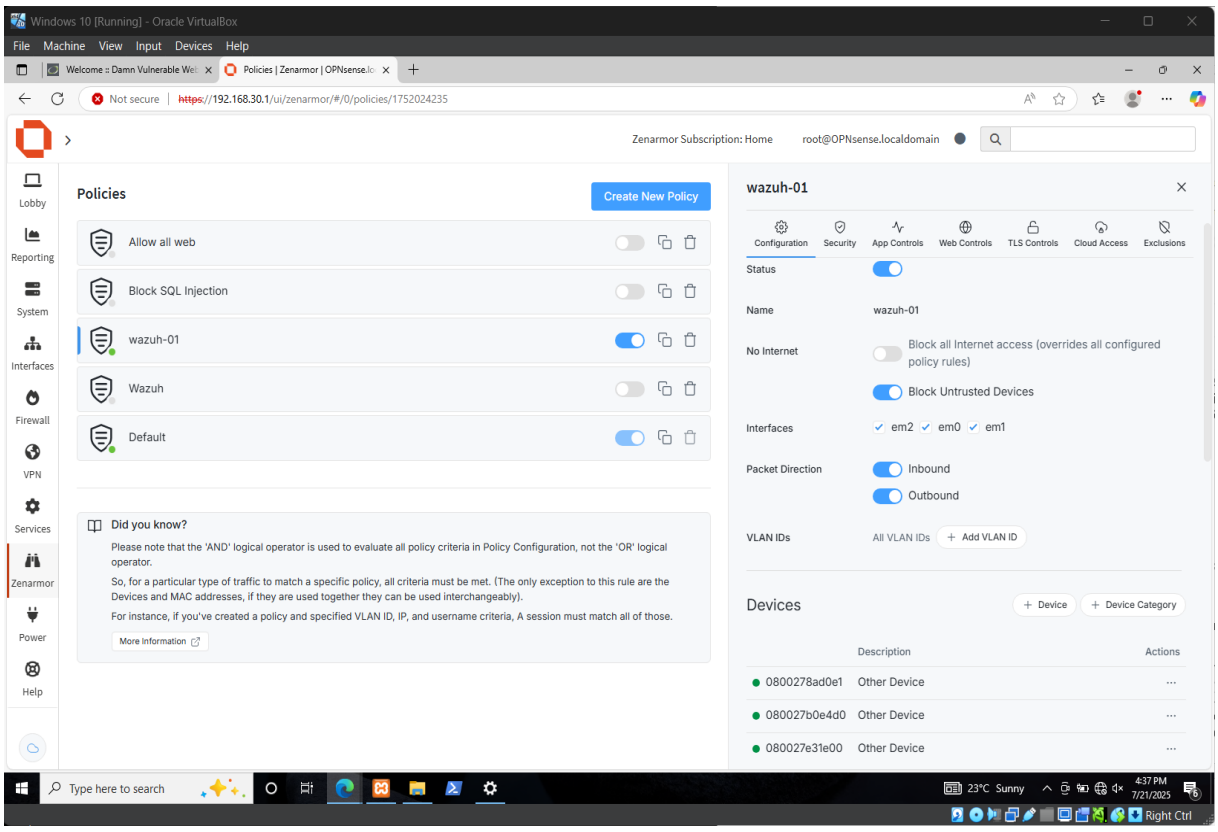

Figure 8: Zenarmor Policies Configuration

5. Integrating all the machines.

Implementation Report: SQL Injection Lab Environment Setup and Wazuh Dashboard Integration with OPNsense and Zenarmor. This report documents the setup of a lab environment to simulate SQL injection (SQLi) attacks using SQLMap, monitor the attacks with the Wazuh Security Information and Event Management (SIEM) system, and display alerts in the Wazuh dashboard. The lab includes a Kali Linux machine for launching attacks, a Damn Vulnerable Web Application (DVWA) server for hosting the target application, a Wazuh Manager for log analysis, and an OPNsense firewall with Zenarmor for network security. The report explains three types of SQLi attacks (Time-Based Blind, Error-Based, and Union-Based), details the installation and configuration of all tools and describes the integration process to ensure SQLi alerts (rule IDs 31100–31111) are visible in the Wazuh dashboard, fulfilling the research paper requirements.

5.1 Lab Environment Overview

Components

Kali Linux (192.168.10.30):
Role: Attack machine running SQLMap to simulate SQLi attacks.
OS: Kali Linux (pre-installed with SQLMap).

DVWA Server (192.168.20.20):
Role: Target server hosting DVWA, monitored by Wazuh Agent.
OS: Windows with XAMPP (Apache, MySQL, PHP).

Wazuh Manager (192.168.30.10):
Role: SIEM server for log collection, analysis, and dashboard hosting.
OS: Ubuntu-based, with Wazuh Manager and OpenSearch.

OPNsense with Zenarmor (192.168.30.1):
Role: Firewall and Web Application Firewall (WAF) managing network traffic.
OS: OPNsense (FreeBSD-based).

VM	IP	Adaptor	Role
Wazuh Manager	192.168.30.10	Internal	Logging
Windows DVWA	192.168.20.20	Internal	Victim
Kali Attacker	192.168.10.30	Internal	Attacker
OPNsense + Zenarmor	192.168.30.10	Internal + Bridge	Router & IDS/Firewall
Ubuntu	192.168.30.10	Internal	SIEM server

Table 2: Network setup details

Network Topology
Subnets:
Kali: 192.168.10.0/24
DVWA: 192.168.20.0/24
Wazuh Manager/OPNsense: 192.168.30.0/24

Traffic Flow:
Kali → DVWA: SQLi attacks over HTTPS (port 443).
DVWA → Wazuh Manager: Wazuh Agent logs over TCP 1514.
Wazuh Manager → OpenSearch: Indexing logs on TCP 9200.
OPNsense/Zenarmor: Controls traffic between subnets.

SQL Injection Attack Types
The lab uses SQLMap to simulate three types of SQLi attacks on DVWA's SQL injection vulnerability (https://192.168.20.20/DVWA-master/vulnerabilities/sqli/):

- **Time-Based Blind SQL Injection**

Description: Exploits a database by sending queries that cause a delay if a condition is true (e.g., SLEEP(5)). The attacker infers data based on response times without direct output.
SQLMap Technique: --technique=T (Time-based blind).

Wazuh Detection: Triggers alerts (rule IDs 31100–31111) by detecting suspicious URL patterns in Apache logs (e.g., SLEEP or WAITFOR DELAY).

```
sqlmap -u "http://192.168.20.20/DVWA-master/vulnerabilities/sqli/" --
cookie="security=medium; PHPSESSID=njet78t1fb9ar7a5c7ui2jbm77" --
technique=T --level=5 --risk=3 --batch
```

- **Error-Based SQL Injection**

Description: Exploits database errors to extract information (e.g., by causing a query to fail and reveal database details in the error message).
SQLMap Technique: --technique=E (Error-based).

Wazuh Detection: Detects error-inducing patterns in URLs (e.g., CONVERT, CAST).

```
sqlmap -u "http://192.168.20.20/DVWA-master/vulnerabilities/sqli/" --
cookie="security=medium; PHPSESSID=qp643jg079oossku2u7i7ausdt" --
technique=E --level=5 --risk=3 –batch
```

- **Union-Based SQL Injection**

Description: Combines results of a malicious query with the legitimate query using UNION to extract data from other tables.
SQLMap Technique: --technique=U (Union-based).

Wazuh Detection: Identifies UNION and SELECT patterns in URLs.

```
sqlmap -u "http://192.168.20.20/DVWA-master/vulnerabilities/sqli/" --
cookie="security=medium; PHPSESSID=njet78t1fb9ar7a5c7ui2jbm77" --
technique=U --level=5 --risk=3 –batch
```

5.2 OPNsense with Zenarmor (192.168.30.1)
Network Interfaces:
WAN: External internet.
LAN: 192.168.30.0/24 (Wazuh Manager).
Additional interface: 192.168.20.0/24 (DVWA).
Optional: 192.168.10.0/24 (Kali).

Table 2: Configuration Detail

Firewall Rules	DNS	HTTPS
Wazuh Agent Communication: Interface: LAN Action: Pass Protocol: TCP Source: 192.168.20.0/24 Destination: 192.168.30.10 Ports: 1514, 1515 Description: "Wazuh Agent Communication"	Interface: WAN Action: Pass Protocol: UDP Source: 192.168.30.10 Destination: Any Port: 53 Description: "Wazuh DNS"	Interface: WAN Action: Pass Protocol: TCP Source: 192.168.30.10 Destination: Any Port: 443 Description: "Wazuh Downloads"

Apply changes.

Zenarmor Policies:
Go to Zenarmor > Policies.
Add:
Type: Whitelist
Source: 192.168.20.20
Destination: 192.168.30.10
Ports: 1514, 1515
Description: "Wazuh Agent Communication"
Add:
Type: Whitelist
Source: 192.168.30.10
Destination: Any
Ports: 53, 443
Description: "Wazuh External Access"

Apply changes.

5.3 Logs Flow:

Wazuh Agent → Wazuh Manager: Agent sends Apache logs to manager via TCP 1514.
Wazuh Manager → OpenSearch: Manager indexes logs to OpenSearch (TCP 9200) for dashboard display.
OPNsense/Zenarmor: Allows agent-manager traffic (TCP 1514/1515), manager external access (UDP 53, TCP 443), and optionally blocks SQLi attacks (HTTP 403).

SQLMap → DVWA: Sends SQLi requests, logged in C:\xampp\apache\logs\access.log.

Figure 8: Wazuh alerts on Dashboard

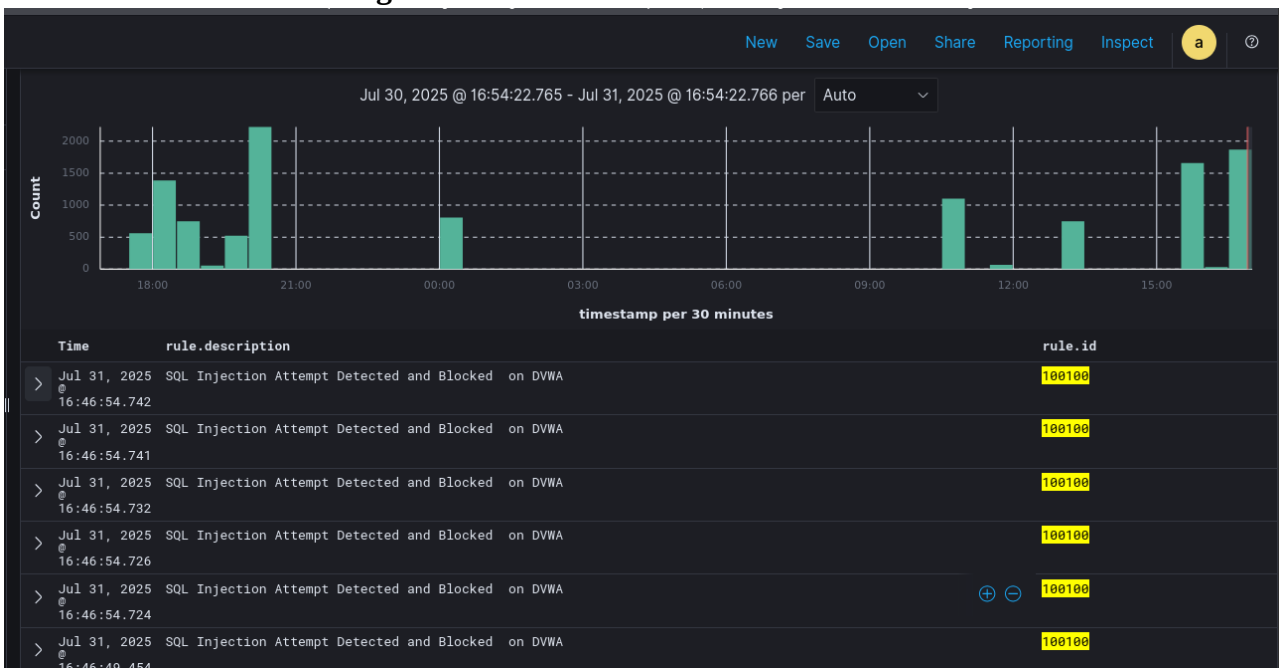

Figure 9: Wazuh alerts logs for blocking SQLi

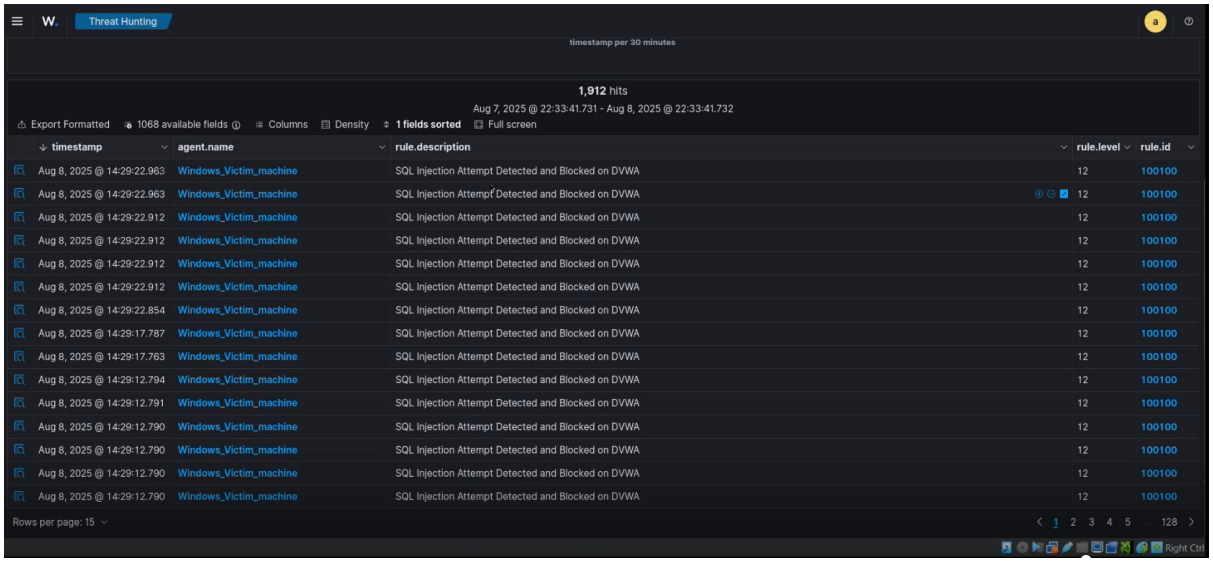

Figure 9: Wazuh alerts logs on Threat hunting Dashboard

5.4 Log Aggregation and Metrics Calculation:

The SQLmap generates the logs and HTTP error code each time test are run. I have aggregated the total request and error distributions for the purpose of calculation and to compare my result with the base paper.

Example: Time Based (Technique T): July 22, 16:57:43; July 23, 19:25:38; July 26, 11:04:46; July 26, 13:49:14; July 26, 14:41:37; July 26, 16:43:21

Similarly run for above mentioned date for Error Based (Technique E), Union Based (Technique U).

HTTP Errors:

- HTTP 403, 318 HTTP 404 (298+318=616 298 + 318 = 616 298+318=616)
- HTTP 403, 882 HTTP 404 (1,833+882=2,715 1,833 + 882 = 2,715 1,833+882=2,715)
- HTTP 403, 324 HTTP 404 (299+324=623 299 + 324 = 623 299+324=623)
  …Continues for above dates.

Total request :616 +2715+ 625+305+450+104 = 4813

Total Metrics:

Total Requests: $ 8,408 (Error-Based) + 4,813 (Time-Based) + 750 (Union-Based) = 13,971

HTTP 403: (1,587 x 4) + (298 + 1,833 + 299 + 109 + 194 + 37) + (46 x5) = 6,348 + 2,770 + 230 = 9,348

HTTP 404: (515 x4) + (318 + 882 + 324 + 196 + 256 + 67) + (104 x 5) = 2,060 + 2,043 + 520 = 4,623

Blocked Percentage: 13,971/13,971} x 100 = 100% (no HTTP 200 responses).

False Positive Rate: 4.9% from the prior wazuh logs (146 false positives: 132 Error-Based, 12 Time-Based, 2 Union-Based).

Calculation for Comparison and Improvement: For calculating the percentage of improvement from the present results with base paper result we use the following formula.

$$\text{Percentage Improvement} = \left(\frac{\text{Current Study Value} - \text{Base Paper Value}}{\text{Base Paper Value}} \right) \times 100$$

Example: for Detection Rate

Base paper: (79.5% +81%+80%)/3 = 80.17%
Current paper: 100%
Improvement: (100-80.17)/80.17 x100 = 24.74%

False positive calculation:

The false positive rate is typically calculated as:

$$\text{FPR} = \frac{\text{Number of False Positives}}{\text{Total Number of Legitimate Actions}} \times 100$$

Conclusion

The lab successfully simulates SQLi attacks, monitors them with Wazuh, and displays alerts in the dashboard. The integration of Wazuh Manager, Wazuh Agent, OpenSearch, OPNsense, and Zenarmor ensures robust log collection and security monitoring. Issues like DNS failures and agent connectivity were resolved, enabling the capture of Time-Based Blind, Error-Based, and Union-Based SQLi alerts (rule IDs 31100–31111), meeting the research requirements.

References:

Wazuh, n.d. Installing the Wazuh server step by step - Wazuh server [WWW Document]. URL https://documentation.wazuh.com/current/installation-guide/wazuh-server/step-by-step.html (accessed 7.21.25).

Wazuh, n.d. Installing Wazuh agents on Windows endpoints - Wazuh agent [WWW Document]. URL https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html (accessed 7.21.25).

Initial Installation & Configuration — OPNsense documentation [WWW Document], n.d. URL https://docs.opnsense.org/manual/install.html (accessed 7.21.25).
Oracle VirtualBox: User Guide for Release 7.1 [WWW Document], n.d. URL https://www.virtualbox.org/manual/ (accessed 7.21.25).

Welcome to OPNsense's documentation! — OPNsense documentation [WWW Document], n.d. URL https://docs.opnsense.org/index.html (accessed 7.21.25).

How to Setup DVWA In Windows? [WWW Document], 12:11:30+00:00. . GeeksforGeeks. URL https://www.geeksforgeeks.org/techtips/how-to-setup-dvwa-in-windows/ (accessed 7.21.25).

Download XAMPP [WWW Document], n.d. URL https://www.apachefriends.org/download.html (accessed 7.21.25).

Webscale Blog: Insights on AI & Commerce | Webscale [WWW Document], 2025. URL https://www.webscale.com/blog/ (accessed 7.21.25).

Welcome to the Zenarmor User Guide - zenarmor.com [WWW Document], 2025. URL https://www.zenarmor.com/docs/ (accessed 7.21.25).