📘Wazuh + ModSecurity (WAF) Integration with Apache

---

1. Introduction

🕰️What is Apache?

Apache is an open-source web server software that powers many websites. It serves web content (HTML, PHP, etc.) to clients like browsers.

🕰️What is ModSecurity (ModSec)?

ModSecurity is a Web Application Firewall (WAF) module for Apache. It inspects HTTP requests/responses and blocks malicious traffic (like SQL Injection, XSS, etc.).

🕰️What is WAF?

A **Web Application Firewall (WAF)** protects web applications by filtering and monitoring HTTP/S traffic. It prevents common attacks such as SQL injection, XSS, CSRF, etc.

🕰️What is Wazuh?

Wazuh is an open-source **Security Information and Event Management (SIEM)** platform. It collects logs from agents (like your Kali machine), analyzes them, and shows alerts/dashboards for security events.

---

2. Wazuh Installation (on Ubuntu Manager)

Step 1: Download and run installation script

```
curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh
sudo bash ./wazuh-install.sh -a
```

👉*This installs Wazuh Manager, Wazuh Indexer, and Dashboard automatically.*

Step 2: Verify services

```
sudo systemctl status wazuh-manager
sudo systemctl status wazuh-
dashboard sudo systemctl status
wazuh-indexer
```

👉*Ensures all services are running correctly.*

---

3. Install Wazuh Agent on Kali (Agent Machine)

Step 1: Install agent

```
curl -sO https://packages.wazuh.com/4.12/wazuh-agent-4.12.0.deb
sudo dpkg -i wazuh-agent-4.12.0.deb
```

👉*This installs the Wazuh agent on Kali to forward logs to the manager.*

Step 2: Configure agent

Edit `/var/ossec/etc/ossec.conf`:

```
<server>
  <address>192.168.0.8</address>    <!-- Manager IP -->
  <port>1514</port>
  <protocol>tcp</protocol>
</server>
<client>
  <name>Kali</name>
</client>
```

👉*This tells the agent where the Wazuh Manager is located.*

Step 3: Start and enable agent

```
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

👉*Ensures the agent starts at boot and begins sending logs.*

Step 4: Register agent on Manager

On Ubuntu (Manager):

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

👉*Generates a key.*

On Kali (Agent):

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

👉*Paste the key from Manager → completes registration.*

---

4. Install Apache + ModSecurity on Kali

Step 1: Install Apache + ModSecurity

```
sudo apt update
sudo apt install -y apache2 libapache2-mod-security2 modsecurity-crs
```

👉*Installs Apache web server, ModSecurity WAF, and OWASP CRS rules.*

Step 2: Enable ModSecurity

```
sudo cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/
modsecurity.conf
sudo nano /etc/modsecurity/modsecurity.conf
```

Change:

```
SecRuleEngine On
```

👉*Switches WAF from DetectionOnly to Blocking mode.*

Step 3: Enable module & restart Apache

```
sudo a2enmod security2
sudo systemctl restart apache2
```

👉*Activates ModSecurity with Apache.*

Step 4: Configure ModSecurity logs

Ensure `/etc/modsecurity/modsecurity.conf` has:

```
SecAuditEngine On
SecAuditLogFormat JSON
SecAuditLog /var/log/apache2/modsec_audit.log
```

👉*Sets log format to JSON and defines log file location.*

Create log file:

```
sudo touch /var/log/apache2/modsec_audit.log
sudo chown www-data:adm /var/log/apache2/modsec_audit.log
sudo chmod 640 /var/log/apache2/modsec_audit.log
```

👉*Ensures Apache can write logs properly.*

---

5. Forward ModSecurity Logs to Wazuh

Step 1: Edit Wazuh Agent config (Kali)

```
sudo nano /var/ossec/etc/ossec.conf
```

Add:

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/apache2/modsec_audit.log</location>
</localfile>
```

👉*Tells Wazuh agent to forward ModSecurity audit logs.*

Step 2: Restart Wazuh Agent

```
sudo systemctl restart wazuh-agent
```

👉*Applies new configuration.*

---

6. Test WAF + Wazuh Integration

Step 1: Trigger XSS attack

```
curl "http://localhost/?param=<script>alert(1)</script>"
```

Step 2: Trigger SQL Injection

```
curl "http://localhost/index.php?id=1' OR '1'='1"
```

👉*These should be blocked and logged by ModSecurity.*

Step 3: Check ModSecurity logs

```
sudo tail -f /var/log/apache2/modsec_audit.log
```

👉*Verify logs are generated.*

Step 4: Check Wazuh Alerts

On Manager:

```
sudo tail -f /var/ossec/logs/alerts/alerts.json
```

👉*Alerts forwarded from Kali should appear.*

📸*[Insert Screenshot: ModSecurity logs in Wazuh Dashboard]*

---

7. Create Wazuh Dashboard for WAF Alerts

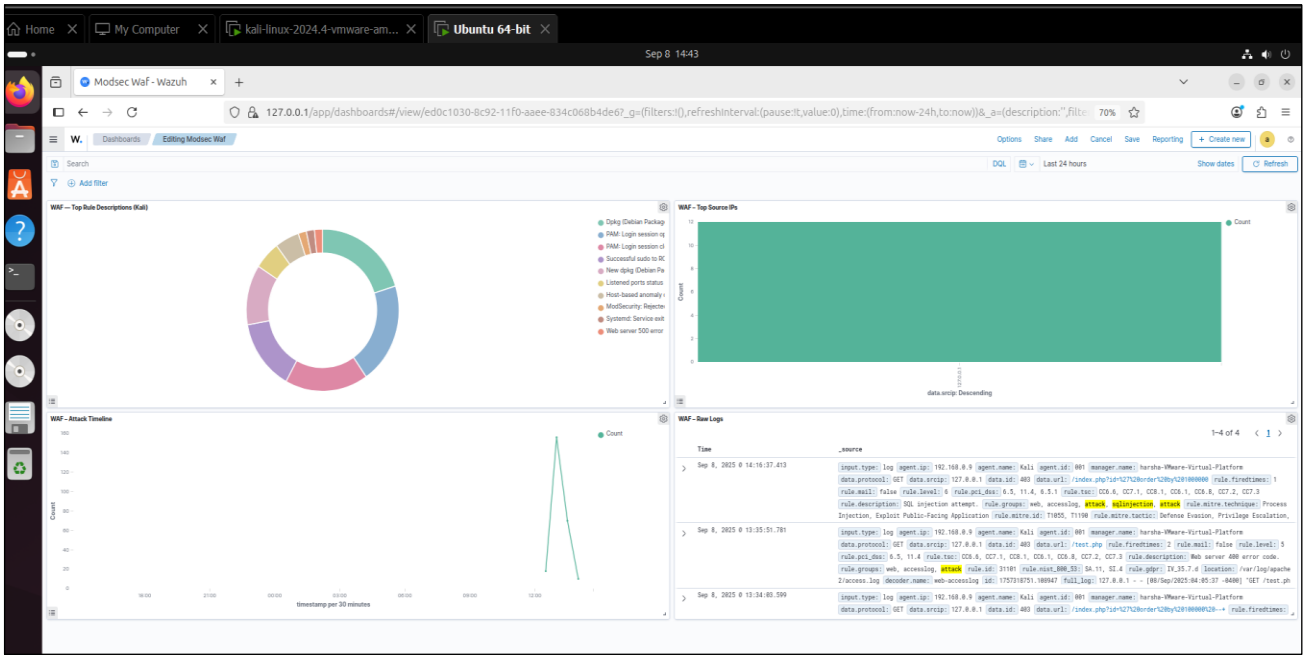
Step 1: Go to Wazuh Dashboard → Discover

- Select index: `wazuh-alerts-*`
- Filter by `agent.name = Kali` 👉*Shows alerts from your Kali machine.*

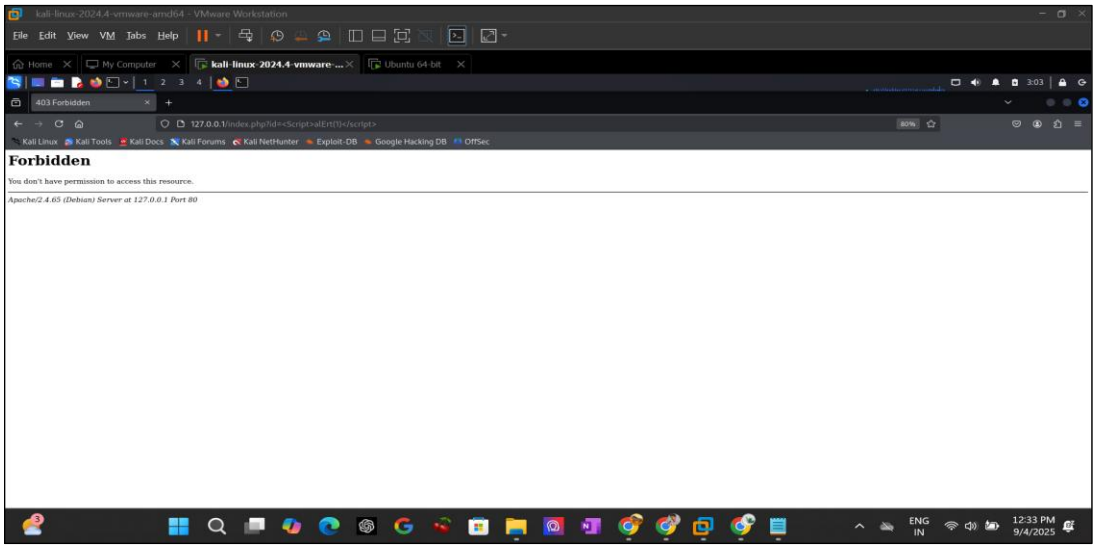
Step 2: Create Visualizations

1. Count of attacks by `rule.description`
2. Attacks by `agent.name`
3. Top source IPs (`data.srcip`)
4. Top URLs attacked (`data.url`)

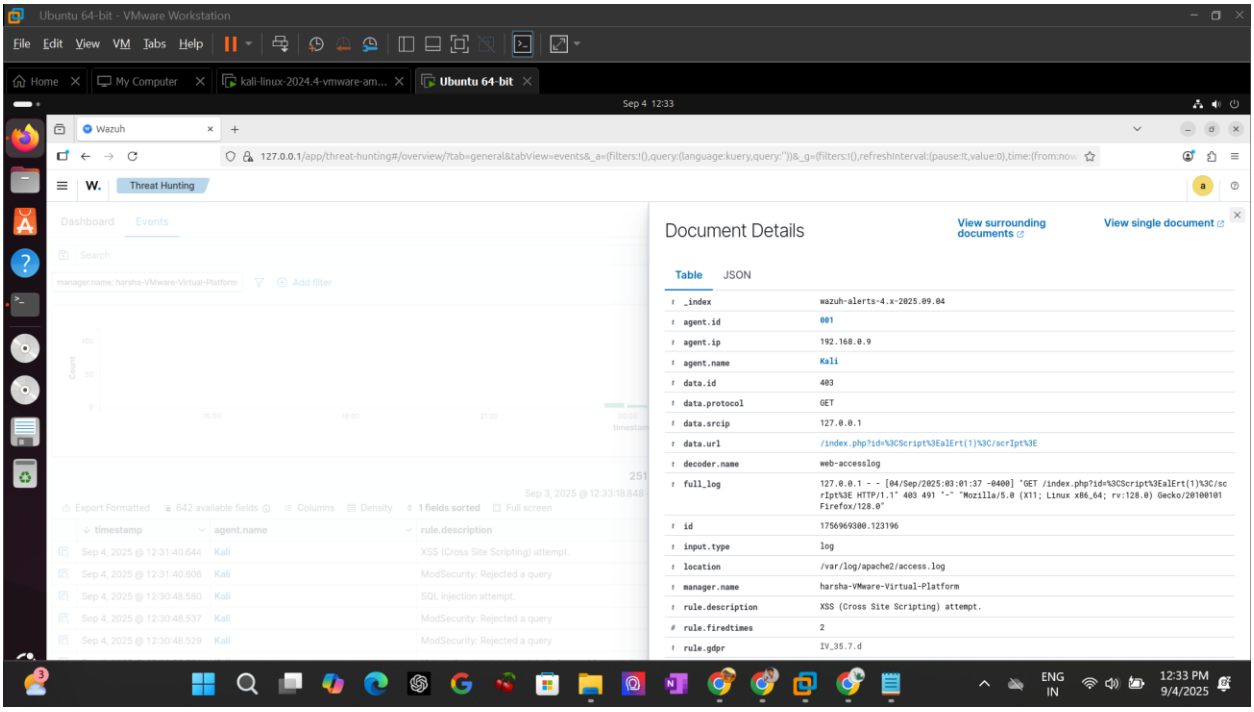
wazuh Dashboard for Modsec Waf Log



Tested Output



OutPut:-



Step 3: Build Dashboard

- Go to **Dashboard** → **Create new dashboard**
- Add the saved visualizations.
- Arrange panels as needed.

[Insert Screenshot: Final WAF Dashboard]

---

8. Conclusion

- **Apache** serves web content.
- **ModSecurity** (WAF) protects against attacks.
- **Wazuh** collects and analyzes security logs.
- Together, they provide **detection + visibility**.

This setup lets you monitor attacks like SQL Injection & XSS in real-time through Wazuh Dashboard.
