Objective

This lab is about creating and testing a Web Application Firewall (WAF)

The WAF protects web servers by checking incoming requests and blocking dangerous ones

It helps understand how web security tools prevent common attacks.

Implementation Summary

The WAF checks every request using regex rules

If a rule matches a known attack pattern, it blocks the request with a 403 error

If nothing matches, the request is sent to the backend normally.

Inspected Components

- Path → Detects directory traversal or local file inclusion attacks (../, etc/passwd).
- Query Parameters → Identifies SQL injection attempts (UNION SELECT, OR 1=1, --).
- Request Body → Detects XSS or command injection payloads (<script>, ;, &&, |).

```
raghad@raghad-VMware-Virtual-Platform:~$ curl -i "http://127.0.0.1:8080/?id=1"
HTTP/1.1 200 OK
Server: Werkzeug/3.1.3 Python/3.12.3
Date: Mon, 03 Nov 2025 20:39:14 GMT
Server: SimpleHTTP/0.6 Python/3.12.3
Date: Mon, 03 Nov 2025 20:39:14 GMT
Content-type: text/html
Last-Modified: Mon, 03 Nov 2025 20:23:25 GMT
Content-Length: 3
Connection: close

OK
```

```
raghad@raghad-VMware-Virtual-Platform:~$ curl -i "http://127.0.0.1:8080/?id=1%20UNION%20SELE
CT%20%2A%20FROM%20users"
HTTP/1.1 403 FORBIDDEN
Server: Werkzeug/3.1.3 Python/3.12.3
Date: Mon, 03 Nov 2025 20:43:43 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 22
Connection: close
Show Apps
Request blocked by WAFraghad@raghad-VMware-Virtual-Platform:~$
```

```
raghad@raghad-VMware-Virtual-Platform:~$ curl -i -X POST "http://127.0.0.1:8080/comment" -d
"<script>alert(1)</script>"
HTTP/1.1 403 FORBIDDEN
Server: Werkzeug/3.1.3 Python/3.12.3
Date: Mon, 03 Nov 2025 21:02:35 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 22
Connection: close

Request blocked by WAFraghad@raghad-VMware-Virtual-Platform:~$
```

```
raghad@raghad-VMware-Virtual-Platform:~$ curl -i "http://127.0.0.1:8080/%2e%2e/%2e%2e/%2e%2e
/etc/passwd"
HTTP/1.1 403 FORBIDDEN
Server: Werkzeug/3.1.3 Python/3.12.3
Date: Mon, 03 Nov 2025 21:05:44 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 22
Connection: close

Request blocked by WAFraghad@raghad-VMware-Virtual-Platform:~$
```

```
raghad@raghad-VMware-Virtual-Platform:~$ curl -i --get --data-urlencode "cmd=who; cat /etc/p
asswd" "http://127.0.0.1:8080/"ttp://127.0.0.1:8080/"
HTTP/1.1 403 FORBIDDEN
Server: Werkzeug/3.1.3 Python/3.12.3
Date: Mon, 03 Nov 2025 21:08:38 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 22
Connection: close

Request blocked by WAFraghad@raghad-VMware-Virtual-Platform:~$
```

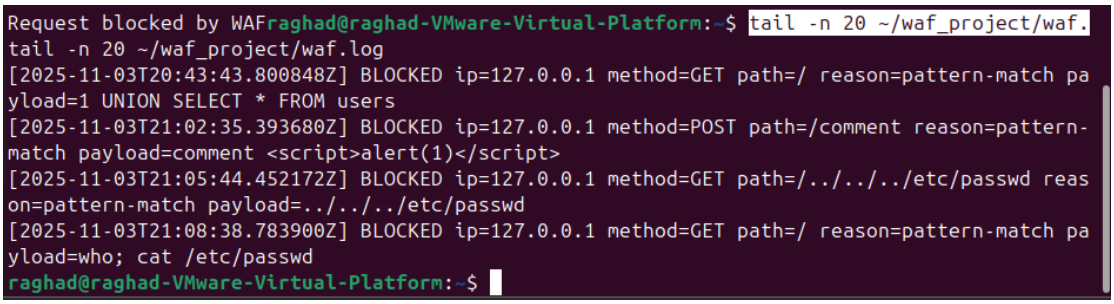
Logging & Evidence

Every event (blocked or allowed) is recorded in:

- waf.log → Human-readable text logs.
- waf.jsonl → JSON lines for structured analysis.

Each log entry includes:

- Timestamp
- Client IP
- Path
- Action (allowed/blocked)
- Reason and matching rule



Conclusion

The WAF effectively detects and blocks common attacks using regex-based rules while logging detailed events. It provides a simple yet practical layer of protection for web applications