**Task 1: Web Application Firewall (WAF) Implementation Report**

# Objective

To install, configure, and test a Web Application Firewall (WAF) using ModSecurity with the OWASP Core Rule Set (CRS) to protect a web server against common web attacks like SQL Injection, Cross-Site Scripting (XSS), and CSRF, and to demonstrate adding a custom security policy.

# Environment Setup

- Server: Kali Linux VM running Apache2 + ModSecurity + OWASP CRS  
- Attacker: Kali Linux VM for penetration testing  
- Network: Both VMs on the same virtual network (Bridged/NAT)

# Tools Used

- Apache2 — Web server  
- ModSecurity — WAF module for Apache  
- OWASP CRS — Predefined ruleset for common exploits  
- curl — For sending test payloads  
- modsec\_audit.log — For verifying detection and blocking

# Installation Steps

1. Installed Apache2 web server:  
 sudo apt update  
 sudo apt install apache2 -y  
  
2. Installed ModSecurity module for Apache2:  
 sudo apt install libapache2-mod-security2 -y  
 sudo a2enmod security2  
  
3. Switched ModSecurity to blocking mode by editing modsecurity.conf:  
 SecRuleEngine On  
  
4. Cloned the OWASP CRS:  
 cd /etc/modsecurity/  
 sudo git clone https://github.com/coreruleset/coreruleset.git  
 sudo mv coreruleset owasp-crs  
 cd owasp-crs  
 sudo cp crs-setup.conf.example crs-setup.conf  
  
5. Linked CRS to Apache by editing security2.conf:  
 IncludeOptional /etc/modsecurity/owasp-crs/crs-setup.conf  
 IncludeOptional /etc/modsecurity/owasp-crs/rules/\*.conf  
  
6. Restarted Apache:  
 sudo systemctl restart apache2

# Custom Rule

Added a custom rule in modsecurity.conf to block any request containing /secret:  
 SecRule REQUEST\_URI "@contains /secret" "id:999999,phase:1,deny,status:403,msg:'Blocked access to secret area'"

# Test Cases

Normal Request  
 curl -I http://<Server-IP>/  
 Result: HTTP/1.1 200 OK  
  
XSS Attack:  
 curl -I "http://<Server-IP>/?param=%3Cscript%3Ealert(1)%3C%2Fscript%3E"  
 Result: HTTP/1.1 403 Forbidden  
 Log: id "941100" msg "XSS Attack Detected"  
  
SQL Injection Attack:  
 curl -I "http://<Server-IP>/?id=1' OR '1'='1"  
 Result: HTTP/1.1 403 Forbidden  
 Log: id "942100" ms "SQL Injection Attack Detected"  
  
Local File Inclusion:  
 curl -I "http://<Server-IP>/?file=../../../../etc/passwd"  
 Result: HTTP/1.1 403 Forbidden  
  
Custom Rule `/secret`:  
 curl -I "http://<Server-IP>/secret"  
 Result: HTTP/1.1 403 Forbidden  
 Log: id "999999" msg "Blocked access to secret area"

# Evidence

Attached screenshots:  
- Apache default page (200 OK)  
- Terminal showing curl commands returning 403  
- modsec\_audit.log showing rule matches

# Conclusion

The WAF was successfully installed and configured using ModSecurity and the OWASP CRS. Attacks like XSS, SQL Injection, and Local File Inclusion were blocked. A custom security rule was created and verified. This demonstrates effective protection for the web server.