# Web Apache / WAF

## Installation Modsecurity :

```
apt install apache2 libapache2-mod-security2
```

## Activer le module ModSecurity :

```
a2enmod security2
```

## Modifier le fichier de configuration par défaut :

```
nano /etc/modsecurity/modsecurity.conf
```

> Puis mettre le contenus :

```
SecRuleEngine On
```

## Installer les règles OWASP Core Rule Set (CRS)

> Installe règle inclus dans  modsecurity-crs

```
apt install modsecurity-crs
```

## Activer les règles CRS :

```
ln -s /usr/share/modsecurity-crs/crs-setup.conf.example /etc/modsecurity/crs
ln -s /usr/share/modsecurity-crs/rules /etc/modsecurity/
```

## Redémarrer Apache bash Copy Edit

> Redémarre le service :

```
systemctl restart apache2
```

## Vérifier que ModSecurity est bien chargé :

```
apachectl -M | grep security2
```

## Tester le WAF :

```
curl -v http://localhost/index.html -H "User-Agent: sqlmap"
```

## Obtenir le résultat suivant :

```
root@Serv-Reverse-Proxy-1:~# curl -v http://localhost/index.html -H "User-Agent: sqlmap
"
*   Trying 127.0.0.1:80...
* Connected to localhost (127.0.0.1) port 80 (#0)
> GET /index.html HTTP/1.1
> Host: localhost
> Accept: */*
> User-Agent: sqlmap
>
< HTTP/1.1 403 Forbidden
< Date: Thu, 13 Mar 2025 10:44:18 GMT
< Server: Apache/2.4.62 (Debian)
< Content-Length: 274
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.62 (Debian) Server at localhost Port 80</address>
</body></html>
* Connection #0 to host localhost left intact
root@Serv-Reverse-Proxy-1:~#
```