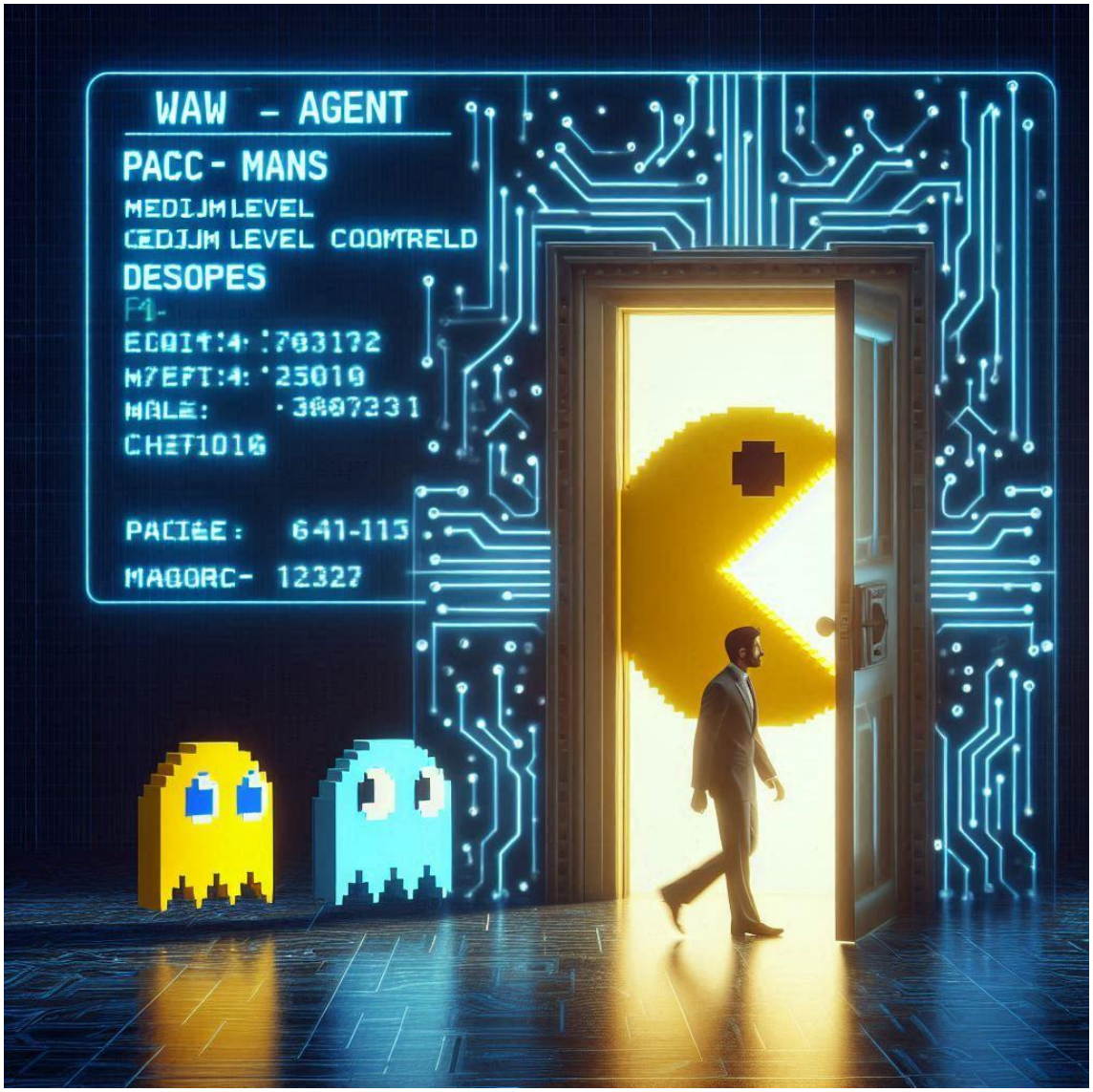


TEAM CHALLENGE - SPRING 9

REGLAS WAF – NIVEL MEDIO DVWA

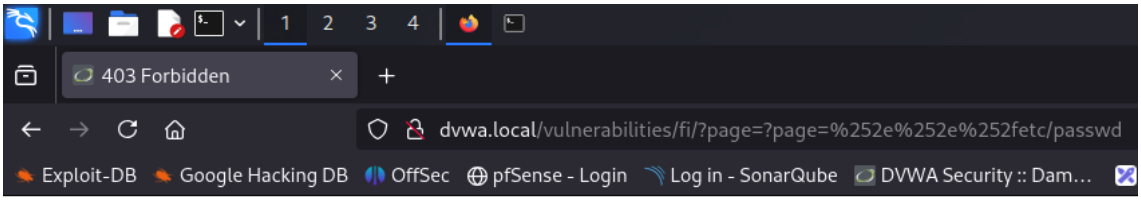
1.- REGLAS WAF USADAS PARA LA REALIZACION DEL TEAM

```
##TEAM CHALLENGE S9

<VirtualHost *:80>
    #DVWA TEAM CHALLENGE NIVEL MEDIO
    ServerName http://10.0.2.6/
    ProxyPreserveHost On

    #proxy inverso
    ProxyPass / http://10.0.2.6/
    ProxyPassReverse / http://10.0.2.6/

    <IfModule security2_module>
        SecRuleEngine On

        # Regla Path Traversal
        SecRule REQUEST_URI|ARGS|REQUEST_BODY "@rx ((\.\./|/\.\.)|(%2e%2e%2f)|(\.\.\\\\\\\\\\\.\.))" "t:none,log,tag:'ATAC_P_TRAV',deny,msg:'PATH TRAVERSAL DETECTADO',id:300001,phase:2"

        # Regla LFI
        SecRule REQUEST_URI|ARGS "@rx (/etc/passwd|/etc/hosts|/etc/shadow|php://filter)" "t:none,log,tag:'ATAC_LFI',deny,msg:'LFI DETECTADO',id:300002,phase:2"

        # Regla RFI
        SecRule REQUEST_URI|ARGS "@rx (http|https|ftp)\:\/\/" "t:none,log,tag:'ATAC_RFI',deny,msg:'RFI DETECTADO',id:300003,phase:2"

        # Regla XSS-reflected
        SecRule ARGS|REQUEST_URI "@rx (<script[^>]*>.*?<\/script>|javascript:|<img[^>]*src=[^>]*>)" "t:none,log,tag:'XSS_REFLECTED',deny,msg:'XSS REFLECTED DETECTADO',id:300004,phase:2>

        # Regla SQLi
        SecRule ARGS|REQUEST_URI "@rx (\bOR\b|\bAND\b|\bUNION\b|=|\bLIKE\b|\bSELECT\b|\bINSERT\b|\bUPDATE\b|\bDELETE\b|\bDROP\b|\bALTER\b|\bFROM\b|\bWHERE\b|\bTABLE\b|\bDATABASE\b|--|#|;)" /
        "t:none,log,tag:'SQLi',deny,msg:'SQL INJECTION DETECTADO',id:300005,phase:2"

        # Regla RCE
        SecRule ARGS "@rx (\b(exec|system|passthru|shell_exec|popen|proc_open|eval|assert)\b|\b(cmd|php(?!:\/\/filter|:\/\/input|:\/\/stdin)|python|perl)\b)" "t:none,log,tag:'RCE',deny,msg:'RCE DETECTADO',id:300006,phase:2>

    </IfModule>
</VirtualHost>
```

Para la configuración del WAF en la maquina REDWEB con IP 10.0.2.4, he configurado la maquina como un proxy inverso, de forma que todo el trafico que envío a la web DVWA, se redirige por el WAF modsecurity instalado en la REDWEB, incluyendo las 5 reglas del ejercicio en el archivo /etc/apache2/sites-enabled/dvwa-proxy.conf.

2 – APLICACIÓN DE LA REGLAS WAF EN DVWA – NIVEL MEDIO EN MAQUINA KALI

✓ PATH TRAVERSAL:



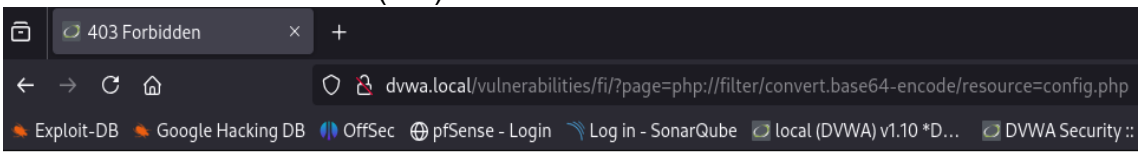
Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at dvwa.local Port 80

```
[Thu Aug 15 21:01:38.625660 2024] [:error] [pid 4332] [client 10.0.2.19:51264] [client 10.0.2.19] ModSecurity: Access denied with code 403 (phase 2). Pattern match "((\\\\.\\\\./|/\\\\.\\\\.)|(%2e%2e%2f)|(\\\\.\\\\.\\\\\\\\\\\\\\\\\\\\\\\\\\\\.\\\\.))" at ARGS:page. [file "/etc/apache2/sites-enabled/dvwa-proxy.conf"] [line "16"] [id "300001"] [msg "PATH TRAVERSAL DETECTADO"] [tag "ATAC_P_TRAV"] [hostname "dvwa.local"] [uri "/vulnerabilities/fi/"] [unique_id "Zr5QksOc7ojPkc4ErmjakwAAAAc"]
```

✓ LOCAL FILE INCLUSION (LFI)



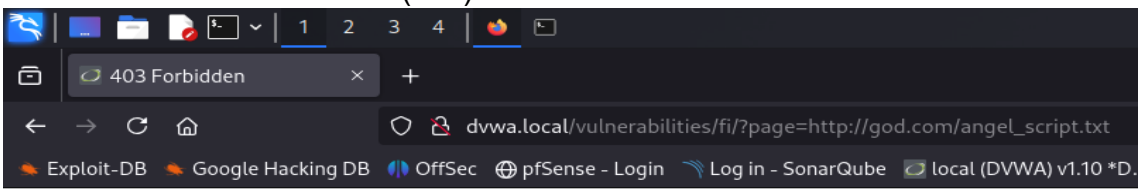
Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at dvwa.local Port 80

```
[Thu Aug 15 21:45:59.820860 2024] [:error] [pid 4738] [client 10.0.2.19:47152] [client 10.0.2.19] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(/etc/passwd|/etc/hosts|/etc/shadow|php://filter)" at REQUEST_URI. [file "/etc/apache2/sites-enabled/dvwa-proxy.conf"] [line "19"] [id "300002"] [msg "LFI DETECTADO"] [tag "ATAC_LFI"] [hostname "dvwa.local"] [uri "/vulnerabilities/fi/"] [unique_id "Zr5a96WNmhcA9Ty2s8kbJQAAAAE"]
```

✓ REMOTE FILE INCLUSION(RFI)



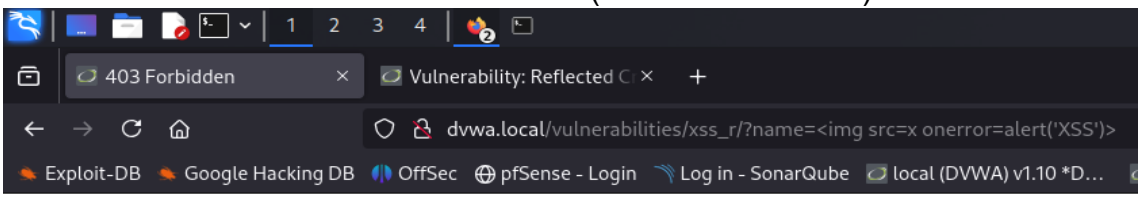
Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at dvwa.local Port 80

```
[Thu Aug 15 21:50:31.642670 2024] [:error] [pid 4740] [client 10.0.2.19:44440] [client 10.0.2.19] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(http|https|ftp)\\\\:\\\\/\\\\/" at REQUEST_URI. [file "/etc/apache2/sites-enabled/dvwa-proxy.conf"] [line "22"] [id "300003"] [msg "RFI DETECTADO"] [tag "ATAC_RFI"] [hostname "dvwa.local"] [uri "/vulnerabilities/fi/"] [unique_id "Zr5cB7Arw1GoLoUPJ875EwAAAAM"]
```

✓ CROSS SITE SCRIPTING REFLECTED (XSS REFLEJADO)



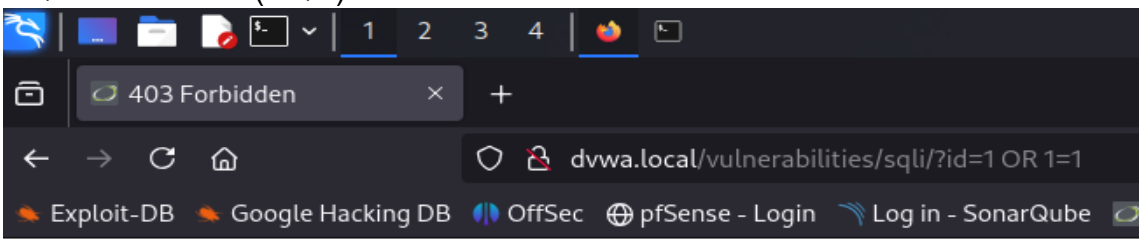
Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at dvwa.local Port 80

```
[Thu Aug 15 22:25:28.685291 2024] [:error] [pid 4786] [client 10.0.2.19:49548] [client 10.0.2.19] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(<script[^>]*>.*?<\\\\/script>|javascript:|<img[^>]*src=[^>]*>)" at ARGS:name. [file "/etc/apache2/sites-enabled/dvwa-proxy.conf"] [line "25"] [id "300004"] [msg "XSS REFLECTED DETECTADO"] [tag "XSS_REFLECTED"] [hostname "dvwa.local"] [uri "/vulnerabilities/xss_r/"] [unique_id "Zr5kOHl4XwS1uPdATTGcEAAAAAE"]
```

✓ SQL INJECTION (SQLi)



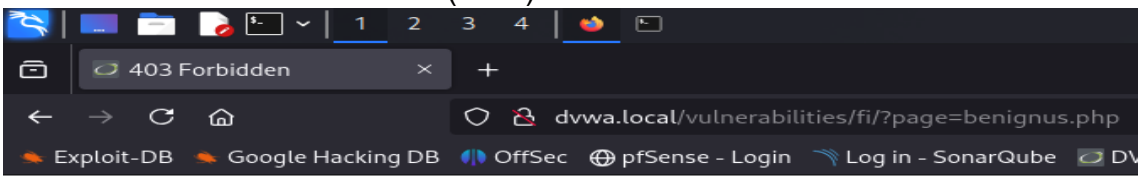
Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at dvwa.local Port 80

```
[Thu Aug 15 22:15:54.935907 2024] [:error] [pid 4915] [client 10.0.2.19:38256] [client 10.0.2.19] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(\\\\bOR\\\\b|\\\\bAND\\\\b|\\\\bUNION\\\\b|=|\\\\bLIKE\\\\b|\\\\bSELECT\\\\b|\\\\bINSERT\\\\b|\\\\bUPDATE\\\\b|\\\\bDELETE\\\\b|\\\\bDROP\\\\b|\\\\bALTER\\\\b|\\\\bFROM\\\\b|\\\\bWHERE\\\\b|\\\\bTABLE\\\\b|\\\\bDATABASE\\\\b|--|#|;)" at ARGS:id. [file "/etc/apache2/sites-enabled/dvwa-proxy.conf"] [line "28"] [id "300005"] [msg "SQL INJECTION DETECTADO"] [tag "SQLI"] [hostname "dvwa.local"] [uri "/vulnerabilities/sqli/"] [unique_id "Zr5h-rYjAFUU_4PWbWXmwQAAAAU"]
```

✓ REMOTE CODE EXECUTION (RCE)



Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at dvwa.local Port 80

```
[Thu Aug 15 21:05:40.396951 2024] [:error] [pid 4290] [client 10.0.2.19:47316] [client 10.0.2.19] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(\\\\b(exec|system|passthru|shell_exec|popen|proc_open|eval|assert|base64_decode)\\\\b|\\\\b(cmd|php|python|perl)\\\\b)" at ARGS:page. [file "/etc/apache2/sites-enabled/dvwa-proxy.conf"] [line "32"] [id "300006"] [msg "RCE DETECTADO"] [tag "RCE"] [hostname "dvwa.local"] [uri "/vulnerabilities/fi/"] [unique_id "Zr5RhI0wxHv7GdHWs0jxCwAAAAE"]
```