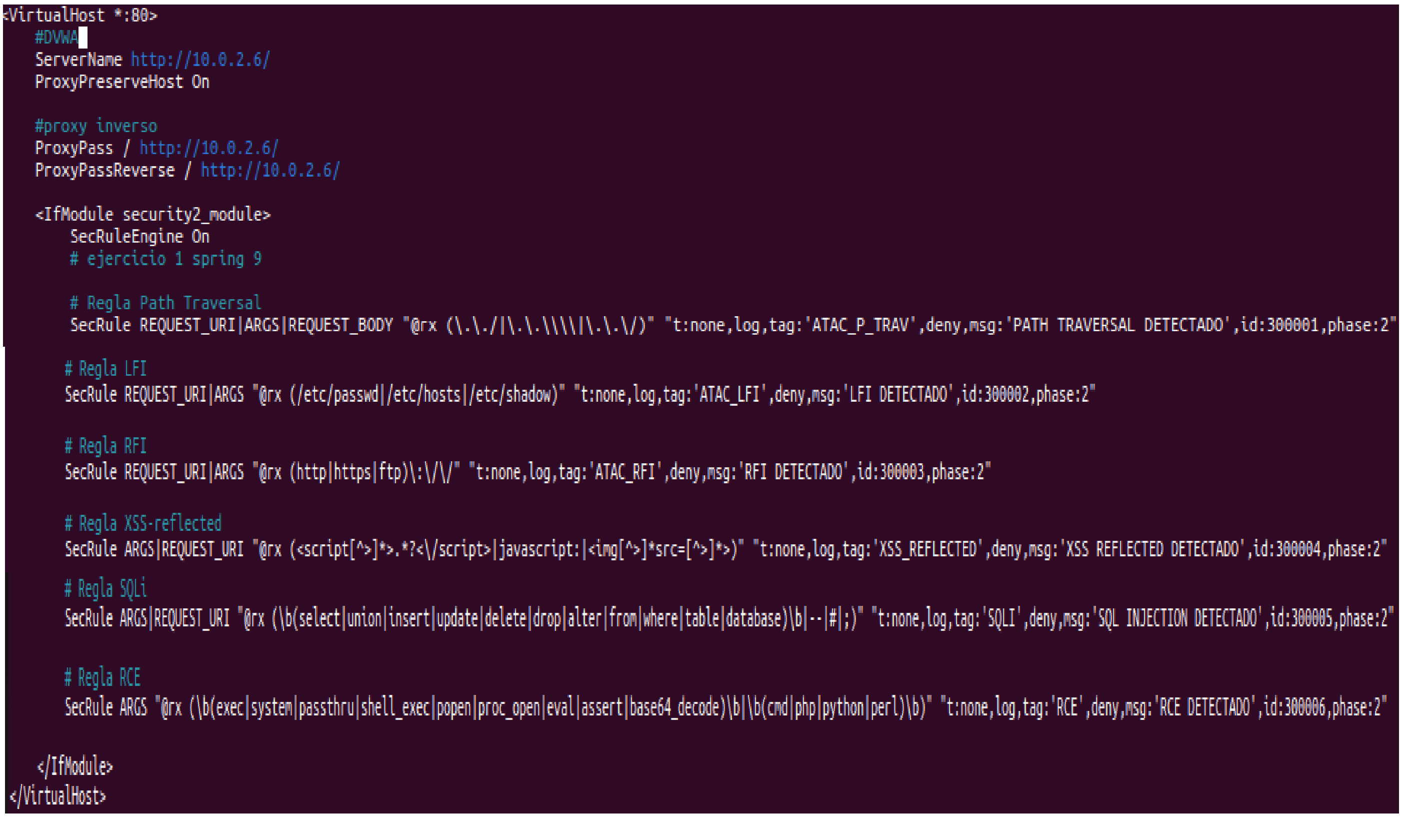
EJERCICIO 1 DEL SPRING 9

REGLAS WAF

1.- REGLAS PARA LA REALIZACION DEL EJERCICIO

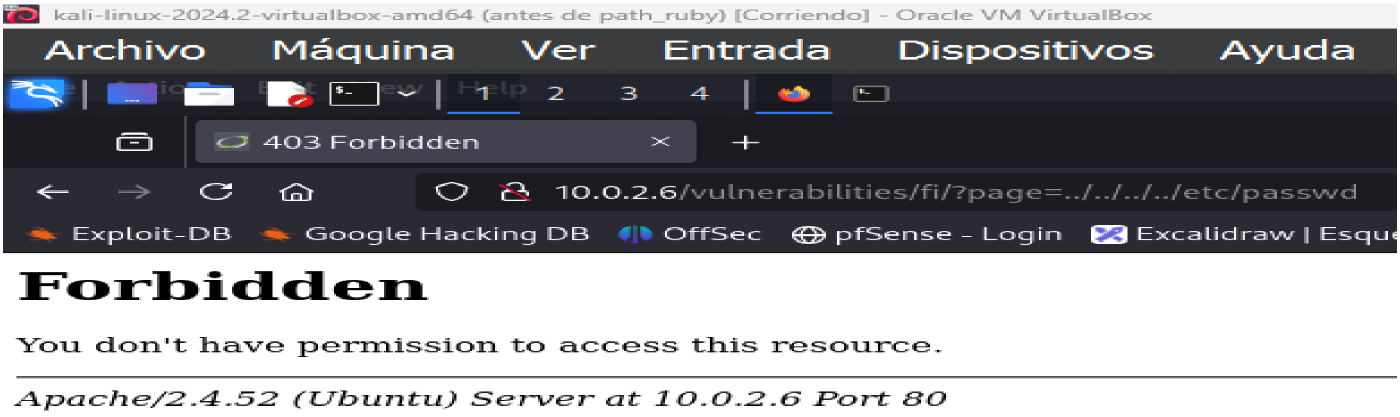


```
<VirtualHost *:80>
    #DWWA
    ServerName http://10.0.2.6/
    ProxyPreserveHost On

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

    <IfModule security2_module>
        SecRuleEngine On
        # ejercicio 1 spring 9

        # Regla Path Traversal
        SecRule REQUEST_URI|ARGS|REQUEST_BODY "@rx (\.\./|\.\.\\\\|\.\.\/)" "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)" "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 (\b(select|union|insert|update|delete|drop|alter|from|where|table|database)\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|base64_decode)\b|\b(cmd|php|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 EN KALI

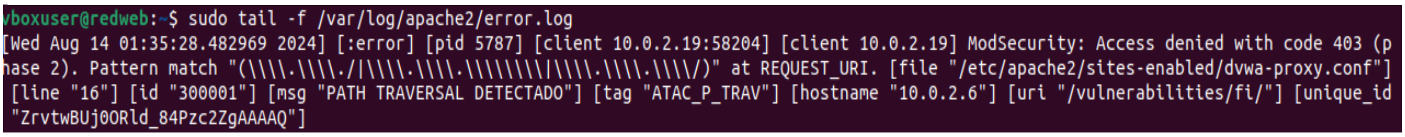
- ✓ PATH TRAVERSAL:


kali-linux-2024.2-virtualbox-amd64 (antes de path_ruby) [Corriendo] - Oracle VM VirtualBox
Archivo
Máquina
Ver
Entrada
Dispositivos
Ayuda
1
2
3
4
403 Forbidden
10.0.2.6/vulnerabilities/fi/?page=../../../../etc/passwd
Exploit-DB
Google Hacking DB
OffSec
pfSense - Login
Excalidraw | Esque

Forbidden

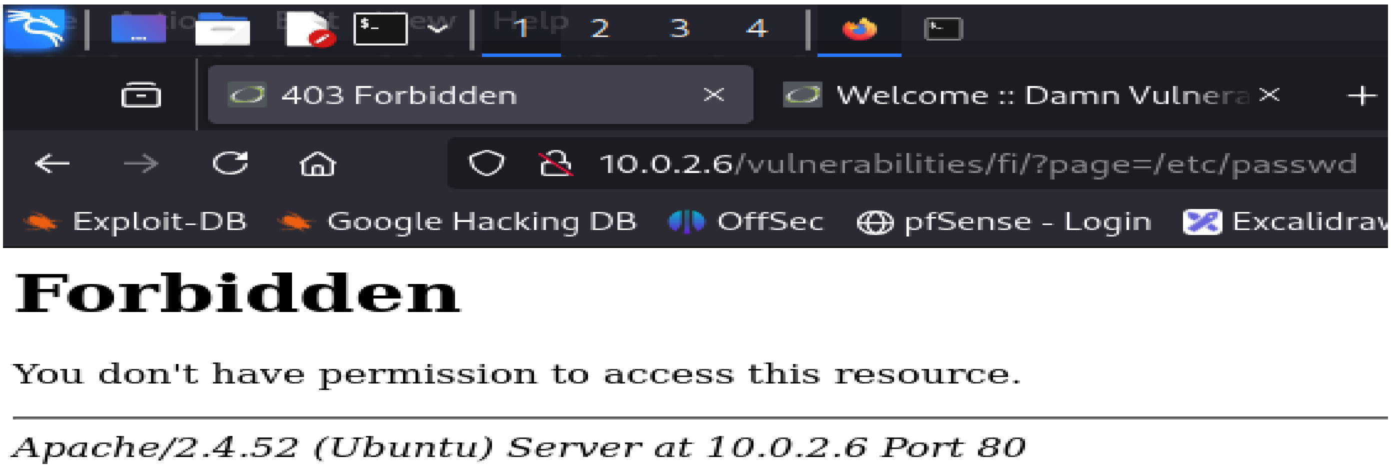
You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at 10.0.2.6 Port 80



```
vboxuser@redweb:~$ sudo tail -f /var/log/apache2/error.log
[Wed Aug 14 01:35:28.482969 2024] [:error] [pid 5787] [client 10.0.2.19:58204] [client 10.0.2.19] ModSecurity: Access denied with code 403 (p
hase 2). Pattern match "(\\\\.\\\\./|\\\\.\\\\.\\\\\\\\|\\\\.\\\\.\\\\/)" at REQUEST_URI. [file "/etc/apache2/sites-enabled/dvwa-proxy.conf"]
 [line "16"] [id "300001"] [msg "PATH TRAVERSAL DETECTADO"] [tag "ATAC_P_TRAV"] [hostname "10.0.2.6"] [uri "/vulnerabilities/fi/"] [unique_id
 "ZrvtwBUj0ORld_84Pzc2ZgAAAAQ"]
```

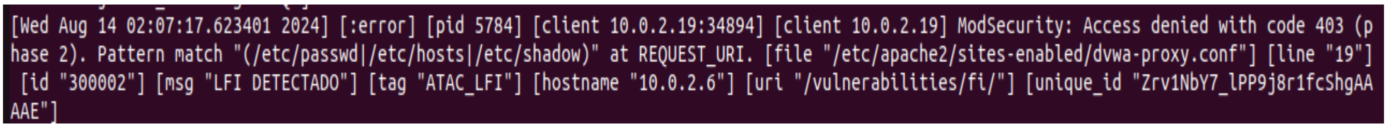
- ✓ LOCAL FILE INCLUSION (LFI)



Forbidden

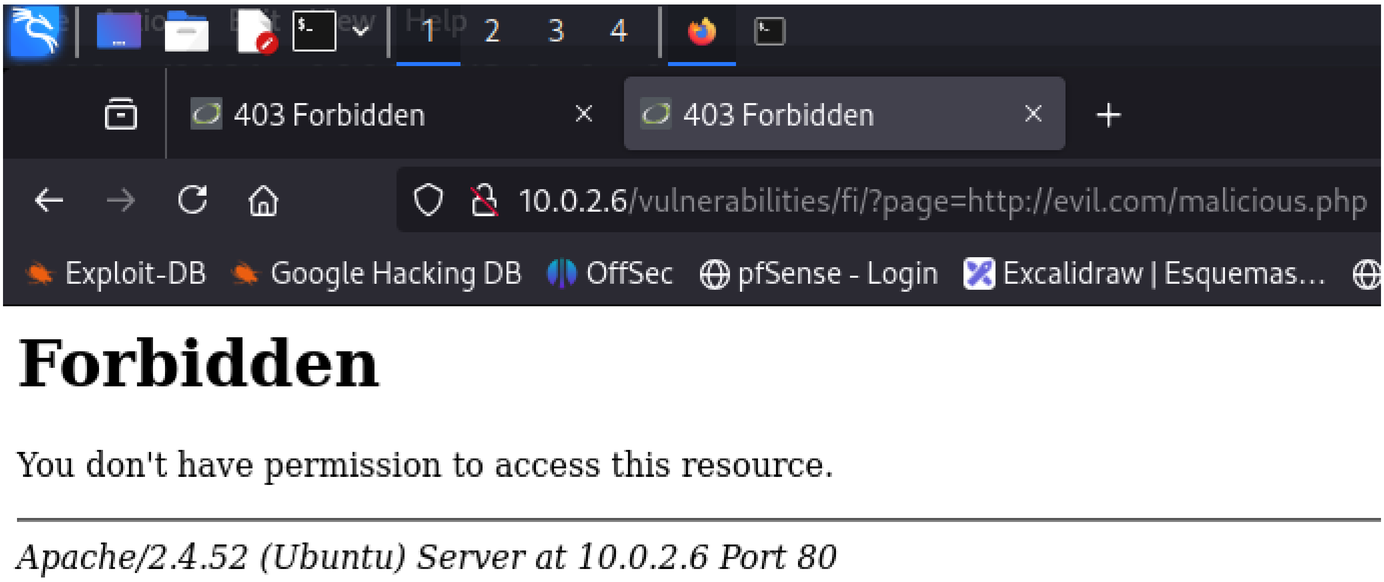
You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at 10.0.2.6 Port 80



```
[Wed Aug 14 02:07:17.623401 2024] [:error] [pid 5784] [client 10.0.2.19:34894] [client 10.0.2.19] ModSecurity: Access denied with code 403 (p
hase 2). Pattern match "(/etc/passwd|/etc/hosts|/etc/shadow)" at REQUEST_URI. [file "/etc/apache2/sites-enabled/dvwa-proxy.conf"] [line "19"]
 [id "300002"] [msg "LFI DETECTADO"] [tag "ATAC_LFI"] [hostname "10.0.2.6"] [uri "/vulnerabilities/fi/"] [unique_id "Zrv1NbY7_lPP9j8r1fcShgAA
AAE"]
```

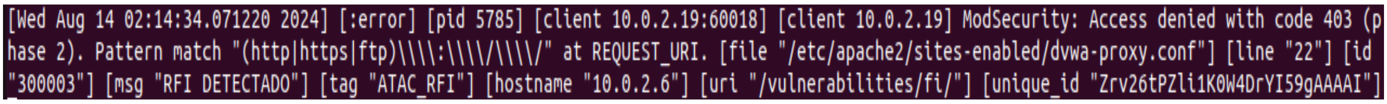
- ✓ REMOTE FILE INCLUSION(RFI)



Forbidden

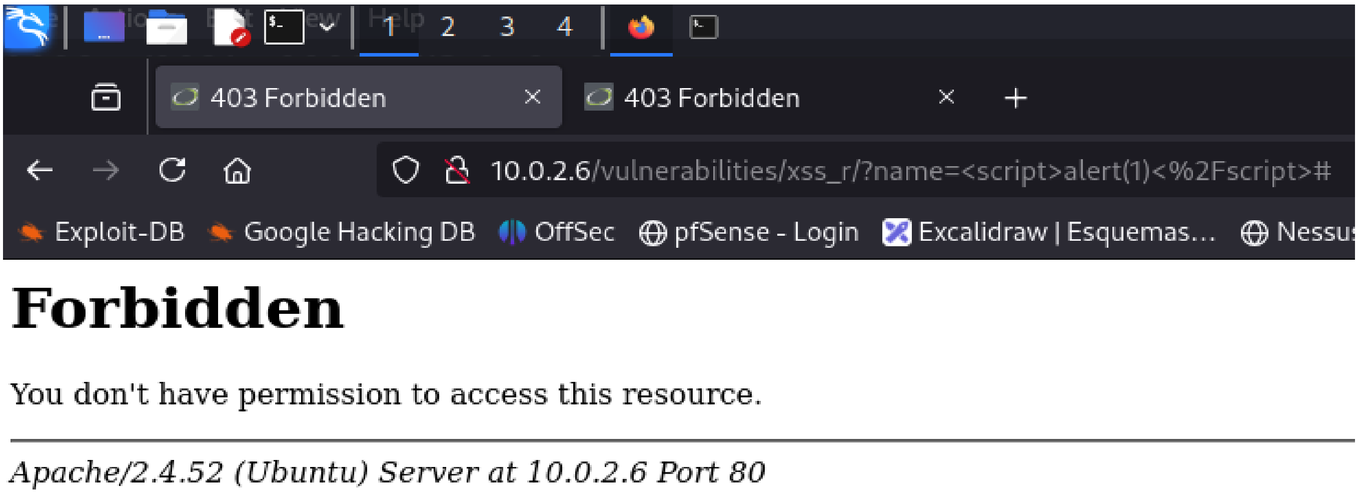
You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at 10.0.2.6 Port 80



```
[Wed Aug 14 02:14:34.071220 2024] [:error] [pid 5785] [client 10.0.2.19:60018] [client 10.0.2.19] ModSecurity: Access denied with code 403 (p
hase 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 "10.0.2.6"] [uri "/vulnerabilities/fi/"] [unique_id "Zrv26tPZli1K0W4DrYI59gAAAAI"]
```

- ✓ CROSS SITE SCRIPTING REFLECTED (XSS REFLEJADO)

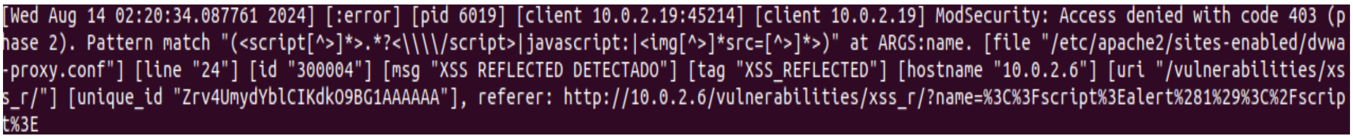


10.0.2.6/vulnerabilities/xss_r/?name=<script>alert(1)<%2Fscript>#

Forbidden

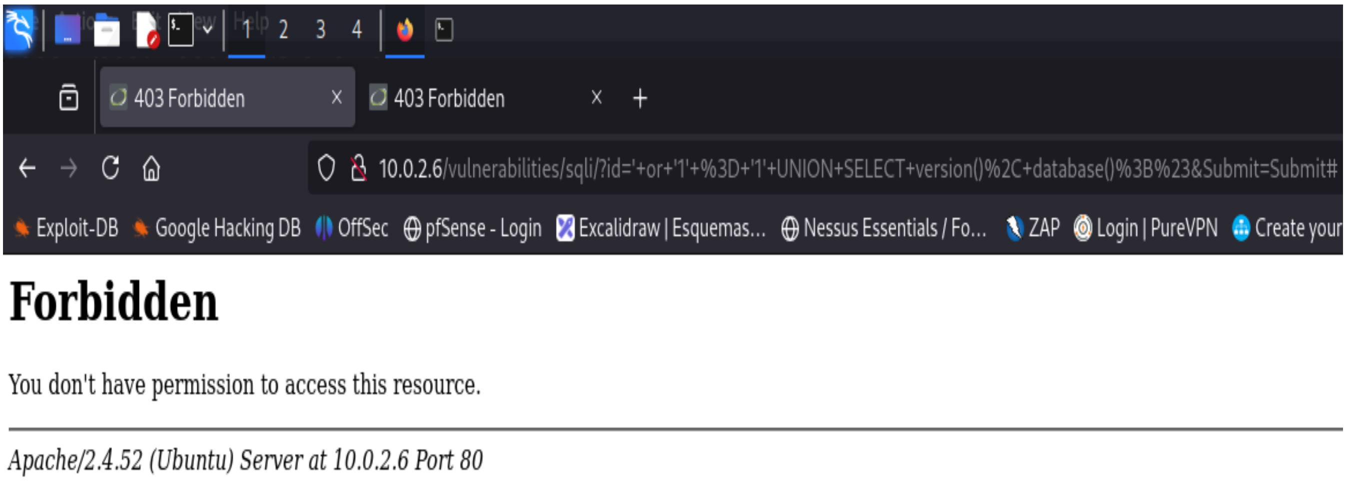
You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at 10.0.2.6 Port 80



```
[Wed Aug 14 02:20:34.087761 2024] [:error] [pid 6019] [client 10.0.2.19:45214] [client 10.0.2.19] ModSecurity: Access denied with code 403 (p
hase 2). Pattern match "(<script[^>]*>.*?<\\\\/script>|javascript:|<img[^>]*src=[^>]*>)" at ARGS:name. [file "/etc/apache2/sites-enabled/dvwa
-proxy.conf"] [line "24"] [id "300004"] [msg "XSS REFLECTED DETECTADO"] [tag "XSS_REFLECTED"] [hostname "10.0.2.6"] [uri "/vulnerabilities/xs
s_r/"] [unique_id "Zrv4UmydYblCIKdkO9BG1AAAAAA"], referer: http://10.0.2.6/vulnerabilities/xss_r/?name=%3C%3Fscript%3Ealert%281%29%3C%2Fscrip
t%3E
```

- ✓ SQL INJECTION (SQLi)

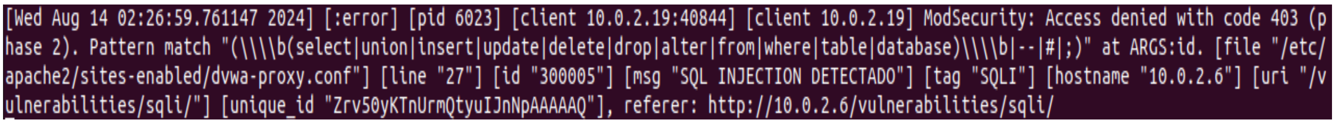


10.0.2.6/vulnerabilities/sqli/?id='+or+'1'+%3D+'1'+UNION+SELECT+version()%2C+database()%3B%23&Submit=Submit#

Forbidden

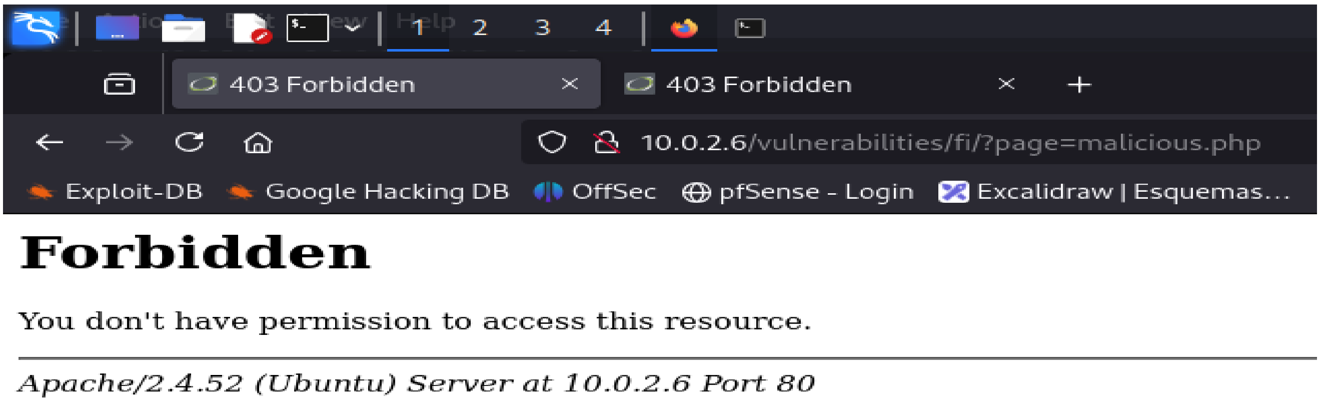
You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at 10.0.2.6 Port 80



```
[Wed Aug 14 02:26:59.761147 2024] [:error] [pid 6023] [client 10.0.2.19:40844] [client 10.0.2.19] ModSecurity: Access denied with code 403 (p
hase 2). Pattern match "(\\\\b(select|union|insert|update|delete|drop|alter|from|where|table|database)\\\\b|--|#|;)" at ARGS:id. [file "/etc/
apache2/sites-enabled/dvwa-proxy.conf"] [line "27"] [id "300005"] [msg "SQL INJECTION DETECTADO"] [tag "SQLI"] [hostname "10.0.2.6"] [uri "/v
ulnerabilities/sqli/"] [unique_id "Zrv50yKTnUrmQtyuIJnNpAAAAAQ"], referer: http://10.0.2.6/vulnerabilities/sqli/
```

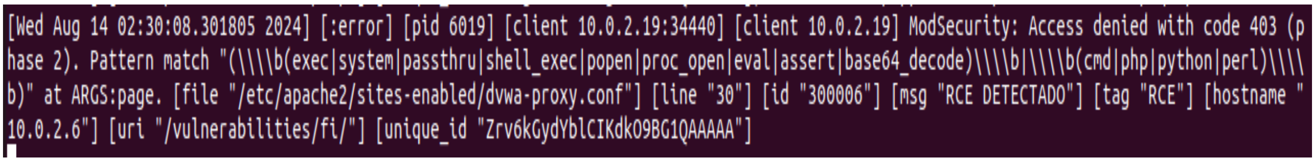
- ✓ REMOTE CODE EXECUTION (RCE)



Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at 10.0.2.6 Port 80



```
[Wed Aug 14 02:30:08.301805 2024] [:error] [pid 6019] [client 10.0.2.19:34440] [client 10.0.2.19] ModSecurity: Access denied with code 403 (p
hase 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 "30"] [id "300006"] [msg "RCE DETECTADO"] [tag "RCE"] [hostname "
10.0.2.6"] [uri "/vulnerabilities/fi/"] [unique_id "Zrv6kGydYblCIKdkO9BG1QAAAAA"]
```