

Mod Security. Desactivación global de reglas por path

Introducción

Una vez más, con el tema de Mod Security, compruebo que el 99% de los administradores de sistemas, sigue la misma pauta de siempre, la salida hacia adelante más fácil, deshabilitando todo.

Soy cabezón, y no he basado mi seguridad en mis máquinas, en abrir la puerta menoscabando la seguridad perimetral.

Tengo cliente a los que llevo sus servicios, que son incapaces de aguantar en firme, con las normas y reglas de seguridad que trato de imponerles, pese a que eso suponga un aumento de costes en horas para limpiar problemas derivados de los **mini hackeaos**

Escenario

En el caso que me llevó a este tema, estaba implicado [DirectAdmin](#) y el webmail [RoundCube](#) en una situación algo especial.

Con las cuentas de sistema `usuario` usadas como cuenta de correo, RoundCube recibía una serie de errores al lanzarse prohibiciones vía Mod Security.

“ Connection Error (Failed to reach the server)! !Error de conexión fallo al intentar alcanzar el servidor)!

“ Cuando teneos problemas con RoundCube como con muchas aplicaciones web, insisto a mis clientes que observen las webmaster tools del navegador y/o al menos las cabeceras de respuesta (406) más allá de los mensajes tipo **Alert** de las aplicaciones.

Al final, localizando las reglas afectadas por RoundCube a nivel hostname, salieron a la palestra las siguiente reglas afectadas:

- 911100
- 932260
- 920340
- 932235
- 941100
- 941130
- 941160
- 941170
- 949110
- 980130

Todas ellas, con Paranoia Level 1, [ModSecurity :: Concepto Paranoia Level](#)

Uy... que cosas. EL **PR 1** es básicamente el nivel con menor número de falsos positivos, y muchas de estas rules, ofrecen una protección extraordinaria a muchos de los errores más comunes de los "programadores" de javascript.

Así que las soluciones que se presentan en, StackOverFlow, el foro de DirectAdmin, y otras muchas, no me convencían, porque se trata de atajos (workaround) que llevan a la desactivación de la regla de forma global, o en su defecto, no cumplen con la documentación de Mod Security o de DirectAdmin.

Solución (Actualizado 8/01/2025)

Al final vi el método antiguo (me llama mas la atención que el nuevo) ofrecido por Directadmin y que usamos en [Como bloquear los Bad bots \(Bot basura\) usando ModeSecurity en Directadmin nueva](#) que es mas manejable y programable.

/usr/local/directadmin/custombuild/custom/modsecurity/conf/

Hay que crear este path como repositorio de los ficheros especificos que creemos para el manejo de ModSecuirty sin miedo a que se eliminen.

```
mkdir -p /usr/local/directadmin/custombuild/custom/modsecurity/conf/
```

Fichero de exclusiones

En mi caso uso `/usr/local/directadmin/custombuild/custom/modsecurity/conf/01_REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf`, pero como es una precarga, le asigno numeros bajos como 00, 01, 02 con el fin de que sean los primeros en cargar.

Tenemos un ejemplo de como tratar el tema en el fichero `/etc/modsecurity.d/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example`

Una vez creado, o modificado, **SIEMPRE** debemos verificar primero (si usamos nginx o apache+nginx) que no hay ningun problema, con:

```
nginx -t
```

Una vez verificado, procedemos a reconstruir los ficheros de configuracion con:

```
> da build modsecurity_rules
Installing OWASP Core Rule Set for ModSecurity...
download_cached: using cached '/usr/local/directadmin/custombuild/cache/owasp-modsecurity-crs-4.9.0.tar.gz'
file
Copying custom ModSecurity rules to /etc/modsecurity.d/...
Installation of ModSecurity Rule Set has been finished.
```

Después reconstruimos la configuración.

```
> da build rewrite_confs
cp: cannot remove '/etc/httpd/conf/extra/httpd-directoryindex.conf': Operation not permitted
2025/01/08 17:15:27 info executing task      task=action=rewrite&value=ips
2025/01/08 17:15:27 info finished task      duration=10.262712ms task=action=rewrite&value=ips
Using 5.135.93.75 for your server IP
Copying custom ModSecurity rules to /etc/modsecurity.d/...
Restarting apache.
Installing OWASP Core Rule Set for ModSecurity...
download_cached: using cached '/usr/local/directadmin/custombuild/cache/owasp-modsecurity-crs-4.9.0.tar.gz'
file
Copying custom ModSecurity rules to /etc/modsecurity.d/...
Installation of ModSecurity Rule Set has been finished.
2025/01/08 17:15:31 info executing task      task=action=rewrite&value=ips
2025/01/08 17:15:31 info finished task      duration=7.557145ms task=action=rewrite&value=ips
Using 5.135.93.75 for your server IP
Using 5.135.93.75 for your server IP
```

Copying custom ModSecurity rules to /etc/modsecurity.d/...

2025/01/08 17:15:34 info executing task task=action=rewrite&value=nginx

2025/01/08 17:15:40 info finished task duration=6.360399294s task=action=rewrite&value=nginx

Restarting nginx.

Ya podríamos hacer pruebas.

Ejemplos

```
SecRule REQUEST_FILENAME "@beginsWith /roundcube" \  
    "id:1001,\ \  
    phase:2,\ \  
    pass,\ \  
    nolog,\ \  
    ctl:ruleRemoveById=911100,\ \  
    ctl:ruleRemoveById=932260,\ \  
    ctl:ruleRemoveById=920340,\ \  
    ctl:ruleRemoveById=932235,\ \  
    ctl:ruleRemoveById=941100,\ \  
    ctl:ruleRemoveById=941130,\ \  
    ctl:ruleRemoveById=941160,\ \  
    ctl:ruleRemoveById=941170,\ \  
    ctl:ruleRemoveById=949110,\ \  
    ctl:ruleRemoveById=980130"
```

Idea y apuntes

- [ModSecurity Rules: Global or for Hostname?](#)
- [How do I skip certain rules for parameter in a path in ModSecurity?](#)

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Revision #4

Created 1 September 2024 17:09:35 by Abkrim

Updated 8 January 2025 17:16:55 by Abkrim