



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
TERCERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL

Seminario web: Hardening de Apache

Ejercicios



TU AYUDA EN
CIBERSEGURIDAD



INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. Ejercicios prácticos	3
2. Solución del ejercicio:	5

ÍNDICE DE FIGURAS

Figura 1 - Líneas donde se aprecia la advertencia de ModSecurity.....	5
Figura 2 - Evidencias del ataque de inyección SQL (I).....	5
Figura 3 - Evidencias del ataque de inyección SQL (II).....	5
Figura 4 - Evidencias del ataque de inyección SQL (III).....	5

ÍNDICE DE CUADROS

Cuadro 1 - Fragmento fichero de log	3
Cuadro 2 - Fragmento fichero de log	3

1. EJERCICIOS PRÁCTICOS

Este ejercicio práctico consiste en identificar, a través del log proporcionado "modsec_audit.log", diferentes ataques realizados a nuestra aplicación "dummy" en el servidor web Apache. Las peticiones que se pueden apreciar son el resultado de tener activo "ModSecurity". Vamos a identificar los tipos de ataque y advertencias que nos podemos encontrar contestando a algunas preguntas.

Abriremos el fichero "log" con cualquier editor de texto.

- **Pregunta 1:** ¿Podrías indicar qué tipo de ataque es el que se realiza en este fragmento del fichero log?

```
--a19b5a47-B--  
GET /index.html?param?=../../../../../etc/passwd HTTP/1.1  
Host: 192.168.1.5:8888  
User-Agent: curl/7.65.1  
Accept: */*
```

Cuadro 1 - Fragmento fichero de log

Realizando una asociación con el tipo de regla que encaja a este tipo de ataque, ModSecurity genera en el log una serie de bloques informativos.

- **Pregunta 2:** ¿Podrías identificar las líneas donde aparezcan estos bloques?
- **Pregunta 3:** En este segundo caso, ¿podrías indicar qué tipo de ataque es el que se realiza en este fragmento del fichero log?

```
--97d8ad19-B--  
GET  
/index.html?param=&mfMo%3D6544%20AND%201%3D1%20UNION%20ALL%20SELECT%20  
1%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctab  
le_name%20FROM%20information_schema.tables%20WHERE%20%3E1--  
%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fp  
asswd%27%29%23 HTTP/1.1  
Accept-Encoding: gzip,deflate  
Host: 192.168.1.5:8888  
Accept: */*  
User-Agent: sqlmap/1.1.12#stable (http://sqlmap.org)  
Connection: close  
Cache-Control: no-cache
```

Cuadro 2 - Fragmento fichero de log

Realizando una asociación con el tipo de regla que encaja a este tipo de ataque, ModSecurity genera en el log una serie de bloques informativos.

- **Pregunta 4:** ¿Podrías identificar las líneas en el log donde aparezcan estos bloques?
- **Pregunta 5:** ¿Qué tipo de REQUEST-NUM-TIPO_DE_ATAQUE_***.conf es aplicado al detectar el ataque anterior?

