5° Coloquio de proyectos
de Becarios en Seguridad Informática

Herramienta para monitoreo de bitácoras relacionadas con servicios web

José Juan Armenta Segura
Diego Alfonso Serrano Guillén

UNAM CERT

DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Objetivo

Contar con una herramienta que permita reportar eventos de seguridad relacionados con:

- Servidor web
- Servidor de base de datos

Objetivo

Los eventos que se reportarán son:

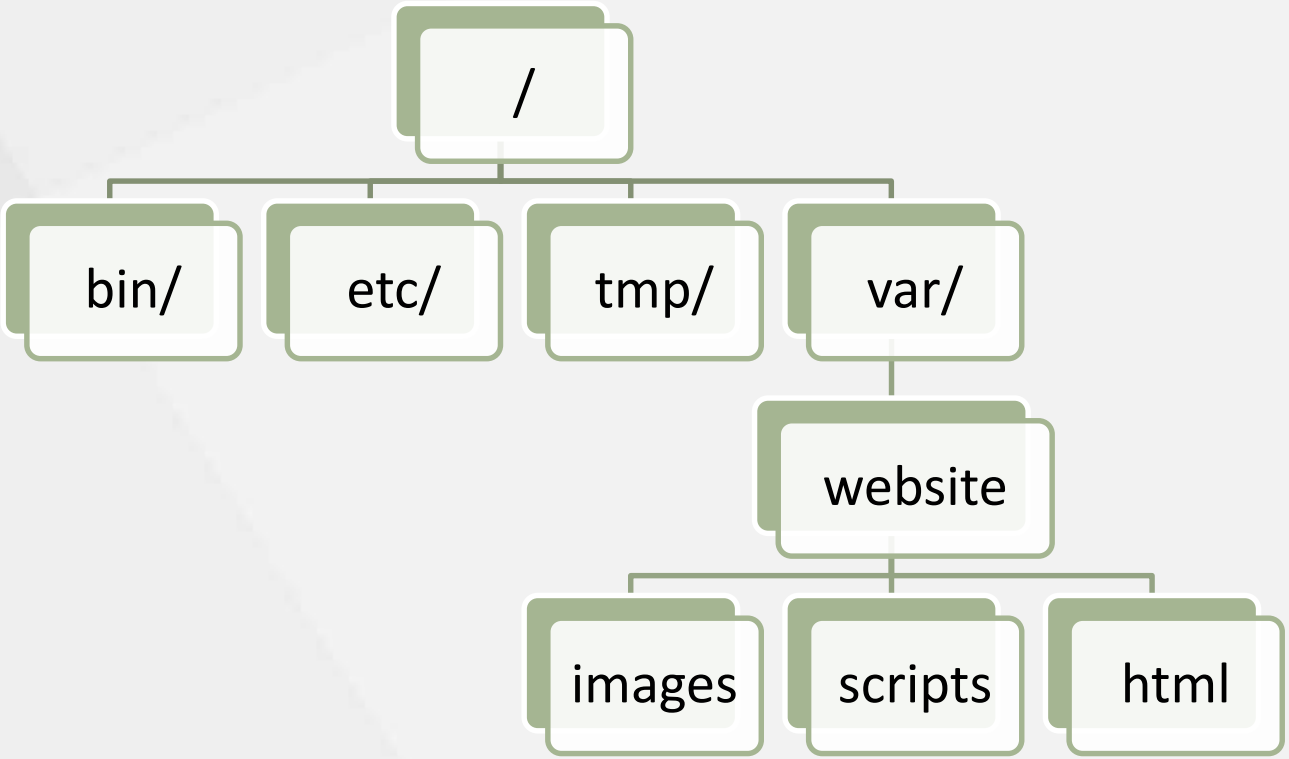
- Cross-site scripting (XSS)
- SQL injection (SQLi)
- Web crawler
- Defacement
- Path traversal

XSS (Cross-site scripting)

- Inyección de código malicioso del lado del cliente
- Robo de credenciales
- Modificar el contenido de un sitio web

Path traversal

- Acceso a directorios o archivos fuera de la raíz del directorio del sitio



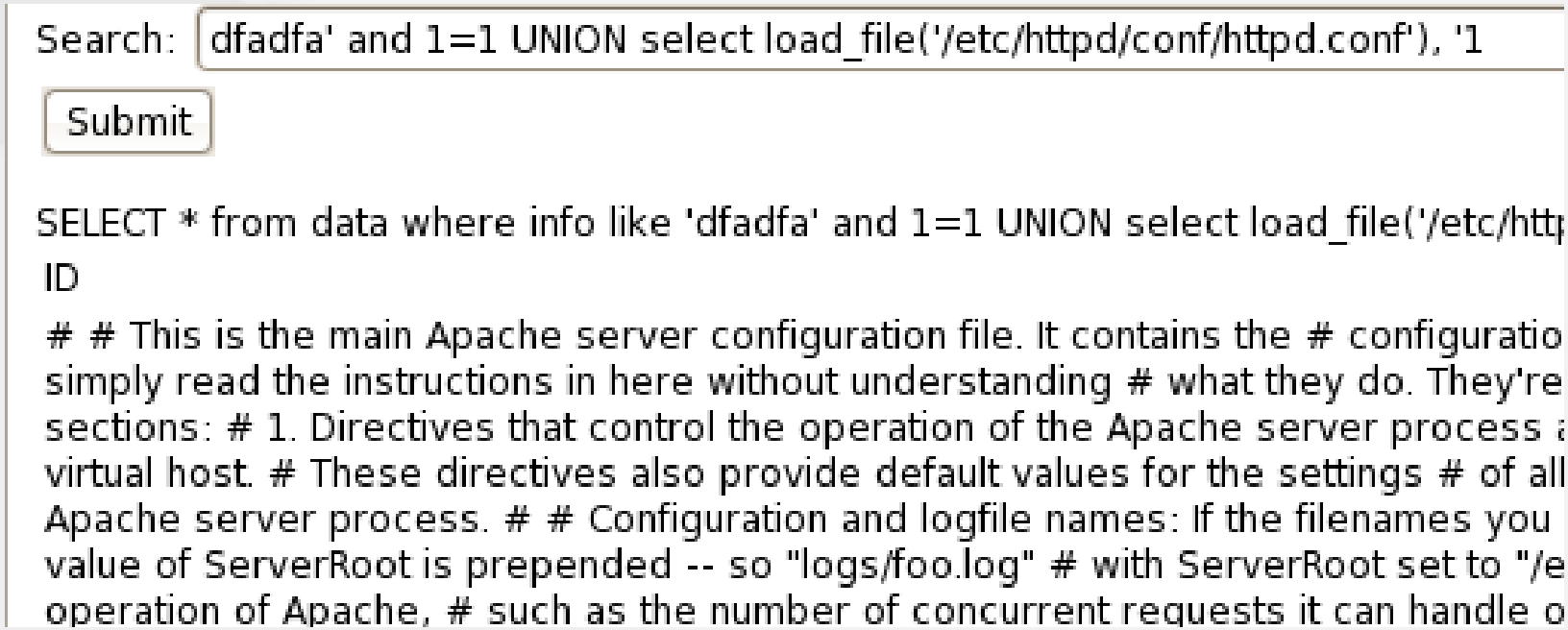
Path traversal

Web crawler

- Herramienta para explorar sitios web automáticamente
- Usado por buscadores y atacantes
- Realiza muchas peticiones

SQLi

- Inserción de sentencias SQL
- Manipular una base de datos



Defacement


Hy Admin,
Just want to tell you this site is not secure
Please Fix it As Soon As Possible (ASAP)
I have to go now
Just Remember We Will Come Again
Bye ..
Peace Contect fb Me:
PLEASE UPGRADE YOUR SECURITY

Herramientas utilizadas

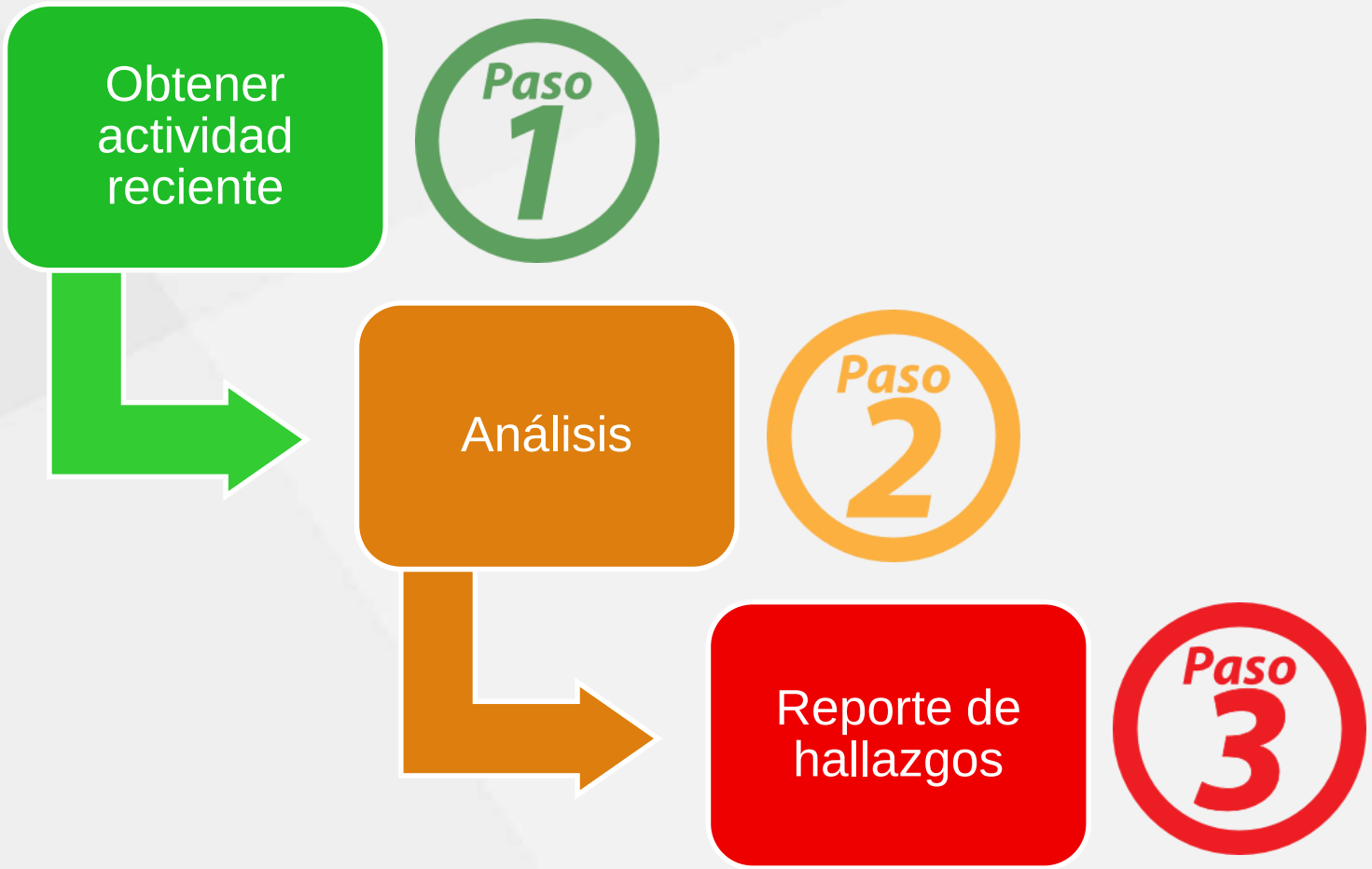
- Para el entorno de pruebas

Herramientas utilizadas

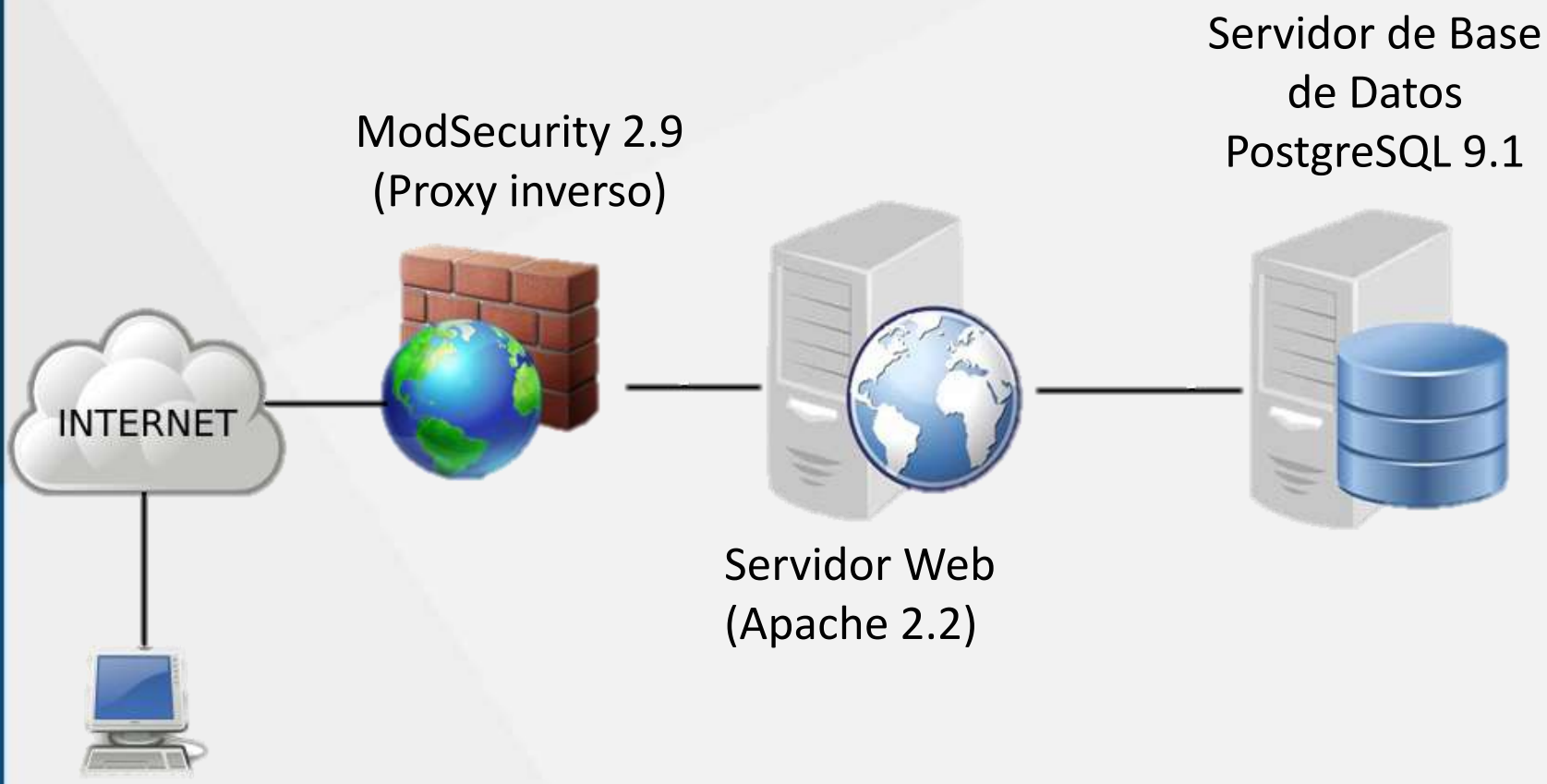
- Para generar datos en las bitácoras

Nikto

Funcionamiento

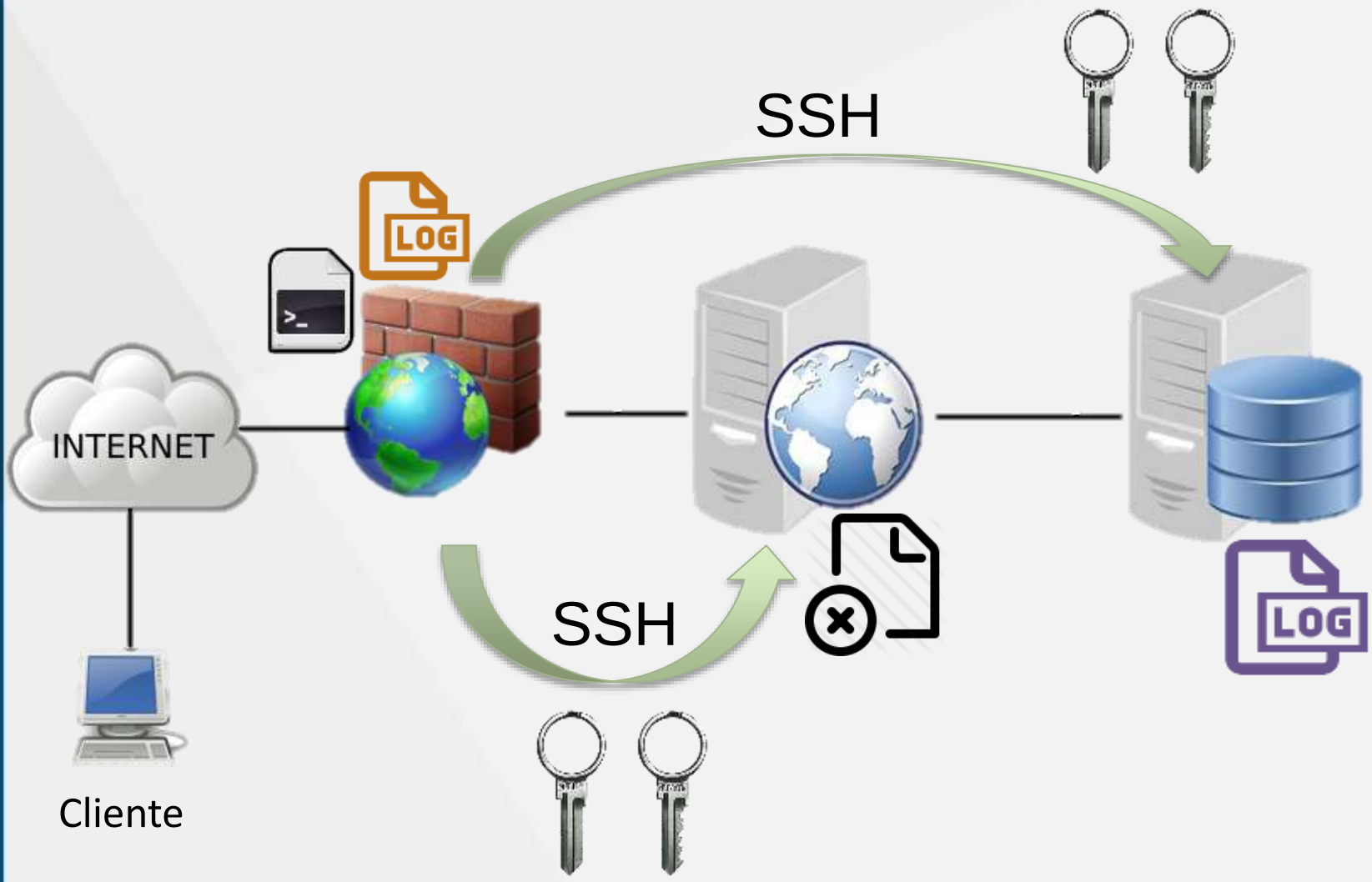


Paso 1 Obtener actividad reciente

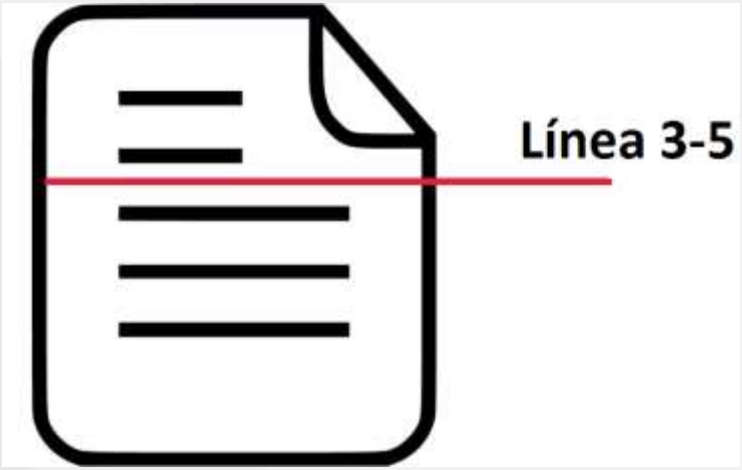


Paso 1

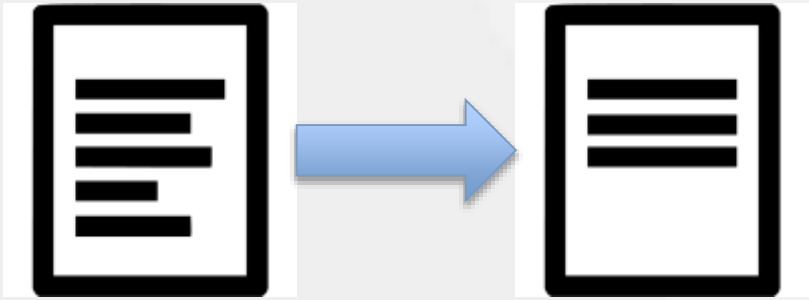
Obtener actividad reciente



Paso 1 Obtener actividad reciente



Se obtienen las líneas de la actividad reciente.



Se cambio el formato de las bitácoras de Apache.

Obtener actividad reciente

Antes:

192.168.35.129 - - [25/Oct/2016:03:54:11 -0500] "GET /ejemplo.php?name=diego%3Cscript%3Ealert(%22XSS%22)%3C/script%3E HTTP/1.1" 200 332 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0“

Después:

192.168.35.129<-->25/Oct/2016:03:54:11<-->GET<-->/ejemplo.php?name=diego%3Cscript%3Ealert(%22XSS%22)%3C/script%3E<-->HTTP/1.1<-->200<-->332<-->-<-->Mozilla/5.0 (Windows NT 6.3; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0

Paso 2

Análisis

- Codificación en hexadecimal
  y doble codificación

```
%3Cscript%253Ealert('XSS')%253C%252FsCrIpT%253E
<script>alert('XSS')</sCrIpT>
```

- Case insensitive
- No se analizan los datos enviados por POST
- Se puede indicar la omisión de algún ataque

Análisis: XSS reflejado

192.168.35.129<-->25/Oct/2016:03:54:11<-->GET<-->/ejemplo.php?name=diego%3Cscript%3Ealert(%22XSS%22)%3C/script%3E

- Existencia de variables en la URL
- ¿Existe una etiqueta HTML en alguna variable?
- Lista negra (script, src, entre otros)

Paso 2 Análisis: Path traversal

192.168.35.129<-->25/Oct/2016:03:54:11<-->GET<-->/ejemplo.php?name=../etc/passwd

- ¿El recurso solicitado tiene variables?
- Lista negra (../, etc/, tmp/, home/, etc/passwd)

Análisis: Crawler

- Múltiples peticiones del mismo cliente
- Promedio de peticiones por segundo (3 por segundo)
- User-Agent de buscadores
- Solicitud de recursos distintos

Análisis: Defacement

- Buscar los métodos PUT o DELETE en la petición
- Considerar si se tiene WebDAV instalado
- No hay más elementos para detectar este ataque

Análisis: SQLi

- Buscar sentencias SQL dentro de la petición
- No clasifica el tipo de ataque SQLi (Blind, DOM, entre otros)
- Relaciona la entrada de la bitácora del servidor web con la del servidor de base de datos

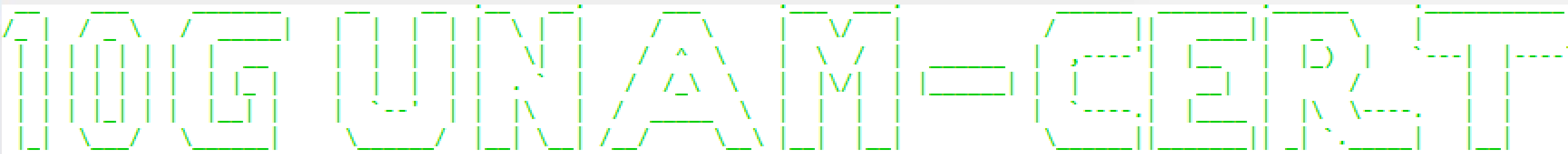
Herramienta

```
logs OK!
Conexion SSH al servidor: [192.168.36.130] WEB [Exitosa]
Conexion SSH al servidor: [192.168.36.128] WAF [Exitosa]
Conexion SSH al servidor: [192.168.36.128] MODsec [Exitosa]
Conexion SSH al servidor: [192.168.36.131] BD [Exitosa]
```

```
Thu Feb 16 00:32:14 CST 2017
```

Paso 3

Herramienta



```
Thu Feb 16 00:32:14 CST 2017


No log actual: 1
eMail enviados: 0


Análisis para el sitio: [www.drupal.proyecto.mx]

Mod Security mod: [On]
Error Script analizador.pl: None
Salida PATH: [0], XSS: [0], SQLi: [0], Defacement: [0], Crawler: [0]


Análisis para el sitio: [www.webdav.proyecto.mx]

Mod Security mod: [On]
Error Script analizador.pl: None
Salida PATH: [0], XSS: [0], SQLi: [0], Defacement: [0], Crawler: [0]


Análisis para el sitio: [www.drupal.vulne.proyecto.mx]

Mod Security mod: [On]
Error Script analizador.pl: None
Salida PATH: [0], XSS: [0], SQLi: [0], Defacement: [0], Crawler: [0]

No log actual: 2
eMail enviados: 0


Análisis para el sitio: [www.drupal.proyecto.mx]
```

Paso 3

Herramienta

```
Thu Feb 16 00:32:14 CST 2017


No log actual: 1
eMail enviados: 0


Análisis para el sitio: [www.drupal.proyecto.mx]

Mod Security mod: [On]
Error Script analizador.pl: None
Salida PATH: [0], XSS: [0], SQLi: [0], Defacement: [0], Crawler: [0]


Análisis para el sitio: [www.webdav.proyecto.mx]

Mod Security mod: [On]
Error Script analizador.pl: None
Salida PATH: [0], XSS: [0], SQLi: [0], Defacement: [0], Crawler: [0]


Análisis para el sitio: [www.drupal.vulne.proyecto.mx]

Mod Security mod: [On]
Error Script analizador.pl: None
Salida PATH: [0], XSS: [0], SQLi: [0], Defacement: [0], Crawler: [0]

No log actual: 2
eMail enviados: 0


Análisis para el sitio: [www.drupal.proyecto.mx]
```

Paso 3

Herramienta

```
Mod Security mod: [On]
Error Script analizador.pl: None
Salida PATH: [2], XSS: [0], SQLi: [0], Defacement: [0], Crawler: [1]

--------------------------->[ ¡¡¡¡¡Tal vez te esten atacando: ಠ_ಠ   !!!!!]<------------
¡¡¡¡¡Se envió correo electrónico!!!
No log actual: 11
eMail enviados: 2


Análisis para el sitio: [www.drupal.proyecto.mx]

Mod Security mod: [On]
Error Script analizador.pl: None
Salida PATH: [9], XSS: [2], SQLi: [0], Defacement: [0], Crawler: [0]

--------------------------->[ ¡¡¡¡¡Tal vez te esten atacando: ಠ_ಠ   !!!!!]<------------
¡¡¡¡¡Se envió correo electrónico!!!

Análisis para el sitio: [www.webdav.proyecto.mx]

Mod Security mod: [On]
Error Script analizador.pl: None
Salida PATH: [0], XSS: [0], SQLi: [0], Defacement: [0], Crawler: [0]


Análisis para el sitio: [www.drupal.vulne.proyecto.mx]

Mod Security mod: [On]
Error Script analizador.pl: None
Salida PATH: [53], XSS: [45], SQLi: [0], Defacement: [0], Crawler: [1]

--------------------------->[ ¡¡¡¡¡Tal vez te esten atacando: ಠ_ಠ   !!!!!]<------------
¡¡¡¡¡Se envió correo electrónico!!!
```

Paso 3

Reporte de hallazgos

unam.cert.log.send@gmail.com
Hoy, 12:39 a.m.
Usted

Se registró un aumento en la actividad maliciosa

Sitio: www.drupal.vulne.proyecto.mx

Seccion 1 : Resumen de los hallazgos

SQL injection:

Cross Site Scripting:

------> IP de origen: **192.168.36.1** Cantidad: **8**

Path Traversal:

------> IP de origen: **192.168.36.1** Cantidad: **13**

Crawler:

------> IP de origen: **192.168.36.1** Cantidad: **2**

Defacement:

------> IP de origen: **192.168.36.1** Cantidad: **1**

Paso 3 Reporte de hallazgos

Cross Site Scripting XSS								
IP	**Fecha**	**Metodo**	**Recurso**	**Referer**	**Codigo**	**Tamano en bytes**	**User-Agent**	**Herramienta detectada**
192.168.36.1	16/Feb/2017:00:39:18	GET	/altercast/AlterCast?op=%3cscript%3ealert(%22adobe_document_server_61.nasl%22)%3c%2fscript%3e	-	404	551	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-
192.168.36.1	16/Feb/2017:00:39:18	GET	/login?user=**%3Cscript%3EJavaScript:alert('cpanel_login_user_xss.nasl')%3B%3C%2Fscript%3E	-	404	537	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-
192.168.36.1	16/Feb/2017:00:39:18	GET	/item.fts?href=%22%3E%3Cscript%3Ealert(%22ftgate_44002.nasl%22)%3C%2Fscript%3E%3B	-	404	540	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-
192.168.36.1	16/Feb/2017:00:39:19	GET	/Websense/cgi-bin/WsCgiLogin.exe?Page=login&UserName=nessus%22%3e%3cscript%3ealert('websense_username_xss.nasl')%3c%2fscript%3e	-	404	563	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	Nessus
192.168.36.1	16/Feb/2017:00:39:19	GET	/console/faces/com_sun_web_ui/help/masthead.jsp?windowTitle=%3c/title%3e%3cscript%3ealert(%27sun_java_web_console_helpwindow_xss.nasl%27)%3c/script%3e	-	404	578	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-
192.168.36.1	16/Feb/2017:00:39:19	GET	/console/faces/com_sun_web_ui/help/helpwindow.jsp?windowTitle=%3c/title%3e%3cscript%3ealert(%27sun_java_web_console_helpwindow_xss.nasl%27)%3c/script%3e	-	404	580	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-

Paso 3

Reporte de hallazgos

Path Transversal

IP	Fecha	Metodo	Recurso	Referer	Codigo	Tamano en bytes	User-Agent	Herramienta detectada
192.168.36.1	16/Feb/2017:00:39:19	GET	/mxhelp/cgi-bin/namazucgi?lang=/../../../../../../../../../../../../boot.ini	-	404	556	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-
192.168.36.1	16/Feb/2017:00:39:21	GET	/error/%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cautoexec.bat	-	404	563	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-
192.168.36.1	16/Feb/2017:00:39:21	GET	/error/%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cwinnt%5cwin.ini	-	404	564	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-
192.168.36.1	16/Feb/2017:00:39:21	GET	/error/%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cboot.ini	-	404	559	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-
192.168.36.1	16/Feb/2017:00:39:22	GET	/login_up.php3?login_name=x&passwd=x&locale_id=../../../../../../../../../../../boot.ini%00.jpg	-	404	545	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-
192.168.36.1	16/Feb/2017:00:39:22	GET	/search?NS-query-pat=..\\..\\..\\..\\..\\..\\..\\..\\winnt\\win.ini	-	404	538	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-
192.168.36.1	16/Feb/2017:00:39:22	GET	/search?NS-query-pat=../../../../../../../../../etc/passwd	-	404	538	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-
192.168.36.1	16/Feb/2017:00:39:23	GET	/.%252e/.%252e/.%252e/.%252e/windows/win.ini	-	404	567	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	-
192.168.36.1	16/Feb/2017:00:39:2	GET	/.%252e/.%252e/.%252e/.%252	-	404	565	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT	-

Reporte de hallazgos

Web Crawler/Spider	
[Crawler] [192.168.36.1] [Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)] [16/Feb/2017:00:39:17 - 16/Feb/2017:00:39:26]	
Recurso	**Codigo**
/axis2/services/CUPMService/ping	404
/tsp//	404
/index.jsp	404
/ords/	404
/admin/LocalIndex.html	404
/iisadmpwd/aexp.htr	404
/snmx-cgi/fxm.exe	404
/axis/DirectDownload.jsp	404
/user_settings.cfg	404
/SE/EMC_SE.swf	404
/dev/	404
//	200
/status.xsl.	404
/lcds/messagebroker/http	404
/index.php/123	200

Paso 3

Reporte de hallazgos

Sección 2 : Resumen de los hallazgos ModSecurity

SQL injection:

------> IP de origen: **192.168.36.153** Cantidad: **17**

Cross Site Scripting:

Path Traversal:

Paso 3 Reporte de hallazgos

Sección 2 : Resumen de los hallazgos ModSecurity

SQL injection:

------> IP de origen: **192.168.36.153** Cantidad: **17**

Cross Site Scripting:

Path Traversal:

SQLi (ModSecurity)

IP	Fecha	Recurso	User-Agent
192.168.36.153	Fri Nov 11 03:30:29 2016	/sites/default/files/styles/large/public/field/image/flyer.jpg?itok=9IvaQ5ga"	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
192.168.36.153	Fri Nov 11 03:30:29 2016	/sites/default/files/styles/large/public/field/image/flyer.jpg?gt;&itok=9IvaQ5ga<img"	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0

Beneficios

- No requiere de gran cantidad de procesamiento
- Flexible a modificaciones
- No requiere configuraciones extra en las bitácoras
- Puede analizar bitácoras de distintas instancias

Oportunidades de mejora

- Tiempo de ejecución
- Detección de herramientas
- Clasificar los tipos de ataques
- Determinar si el intento exitoso o fallido

¡GRACIAS!

José Juan Armenta Segura
Departamento de Seguridad en Sistemas
UNAM-CERT
jose.armenta@cert.unam.mx

Diego Alfonso Serrano Guillén
UPIICSA (IPN)
diego.serrano@bec.seguridad.unam.mx