

# GUÍA 3: CÓMO REALIZAR CROSS SITE SCRIPTING



**CRISTHIAN EDUARDO CASTILLO MENESES**  
**CHRISTIAN CAMILO URCUQUI LÓPEZ**

19 DE FEBRERO DE 2018

## Contenido

INTRODUCCIÓN .....	3
¿Qué es Cross-Site Scripting? .....	3
Material Necesario .....	4
CROSS-SITE SCRIPTING .....	5

## INTRODUCCIÓN

### ¿Qué es Cross-Site Scripting?

Es un ataque de inyección de código malicioso, en su mayoría JavaScript, para su posterior ejecución, se puede hacer a sitios web, aplicaciones locales y al navegador. Puede ser usado para robar sesiones de usuarios, infectar a los visitantes de la web, entre otros.

Esta situación es causada por la incorrecta validación de datos de entrada que son usadas en ciertas aplicaciones, o no sanear la salida adecuada para su presentación como página web.

### **Cross-Site Scripting persistente o directo:**

Consiste en inyectar código en un sitio web, el cual pasa a formar parte del propio código del sitio web. Afecta a todos los usuarios que ingresan al sitio web después.

### **Cross-Site Scripting reflejado o indirecto:**

Consiste en modificar valores que la aplicación usa para pasar variables entre dos páginas, sin usar sesiones, es muy común cuando se envía la información por medio de la url.

## Material Necesario

- **Metasploitable**

# Cross-Site Scripting (XSS)

1. Abrimos metasploitable y usamos el comando para ver la dirección IP del servidor.

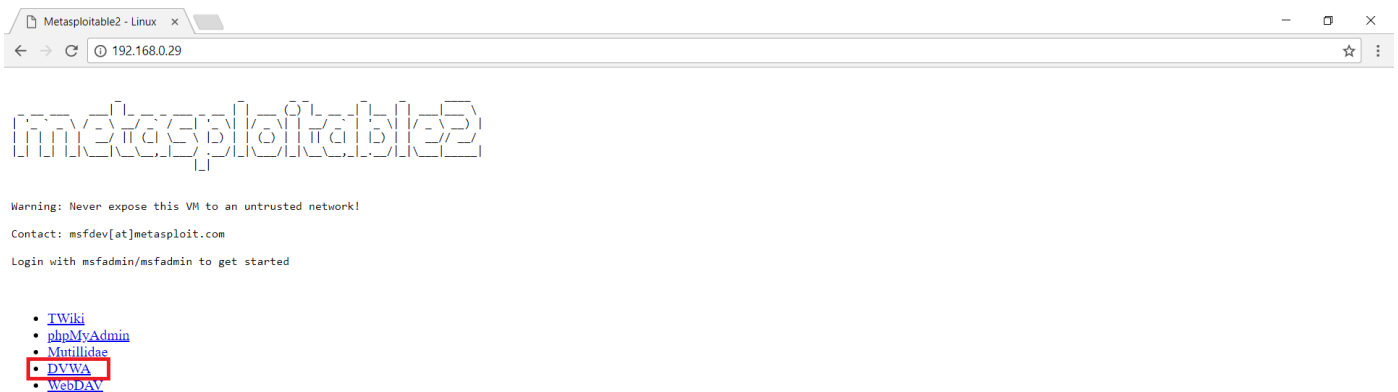
```
# ifconfig
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5e:e5:b4
          inet addr:192.168.0.29  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5e:e5b4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2556 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1465 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:279407 (272.8 KB)  TX bytes:1614776 (1.5 MB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:550 errors:0 dropped:0 overruns:0 frame:0
          TX packets:550 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:244213 (238.4 KB)  TX bytes:244213 (238.4 KB)

msfadmin@metasploitable:~$ _
```

2. Introducimos la dirección IP en algún navegador web e ingresamos en Damn Vulnerable Web App (DVWA).



# GUÍA 3: CÓMO REALIZAR CROSS SITE SCRIPTING

CRISTHIAN EDUARDO CASTILLO MENESES – CHRISTIAN CAMILO URCUQUI LÓPEZ

## 3. Logueamos dentro de DVWA

**Usuario:** admin

**Contraseña:** password



Username

Password

Login

You have logged out

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

### WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing **XAMPP** onto a local machine inside your LAN which is used solely for testing.

### Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

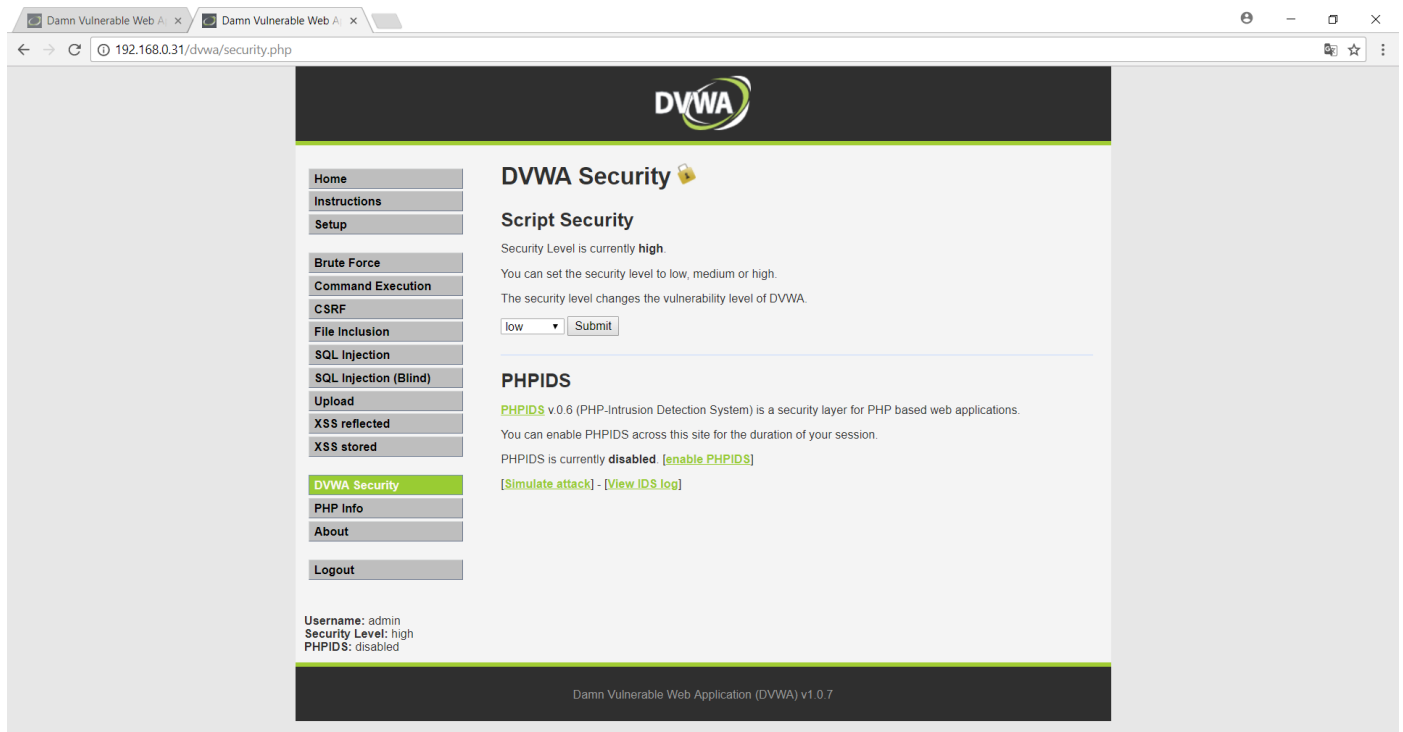
### General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Username: admin  
Security Level: high  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

4. Con el fin de mostrar el ataque cambiaremos la seguridad del sitio a low.



## 5. Nos dirigimos a XSS stored.

Al enviar un mensaje nos damos cuenta de que el mensaje enviado se muestra en pantalla y si recargamos la página se mantendrá ahí, algo similar a lo que pasa cuando comentamos en alguna red social.

**DVWA**

**Vulnerability: Stored Cross Site Scripting (XSS)**

Name \*

Message \*

Name: test  
Message: This is a test comment.

Name: Prueba  
Message: Prueba

**More info**

<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>


Username: admin  
Security Level: low  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Si el desarrollador no valida que tipo de datos son enviados, se podrá hacer una inyección de código malicioso, en este caso mandaremos un *alert* por medio de java script.



6. Escribimos el código que vamos a inyectar en el campo del mensaje y lo enviamos.



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

**XSS stored**

DVWA Security

PHP Info

About

Logout

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

inyección

Message \*

<script>alert('Hacked')</script>

Sign Guestbook

Name: test

Message: This is a test comment.

Name: Prueba

Message: Prueba

### More info

<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

View Source

View Help

Username: admin

Security Level: low

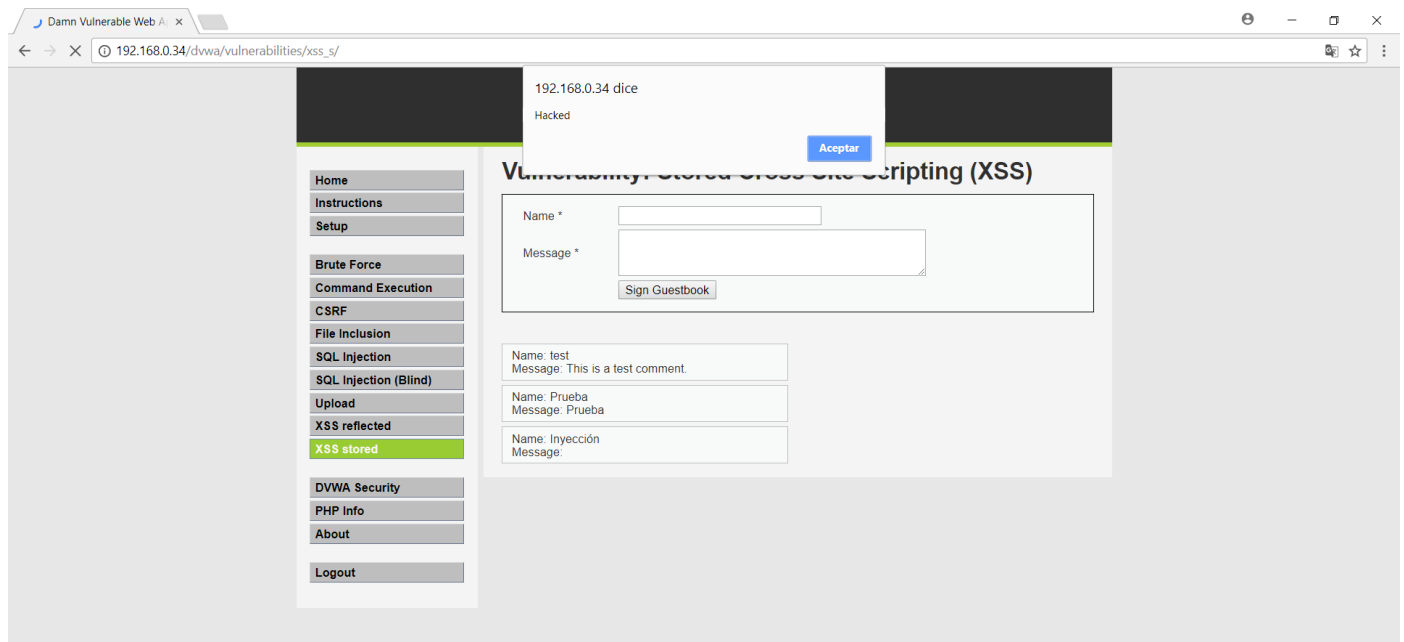
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

## GUÍA 3: CÓMO REALIZAR CROSS SITE SCRIPTING

CRISTHIAN EDUARDO CASTILLO MENESES – CHRISTIAN CAMILO URCUQUI LÓPEZ

Ahora el código JavaScript que hemos insertado pasará a formar parte del código de la página, por ende, todo el que visite este sitio web le saldrá dicho mensaje.



Si revisamos el código de la página nos daremos cuenta de que el código que hemos ingresado se encuentra en el código fuente como un script propio de la página

