


# Hacking de Aplicaciones WEB

## SESION 3

 @WilliamMarchand

## Temario General

- ◆ 1. Introducción al Hacking Web
- ◆ 2. Protocolos y arquitectura web
- ◆ 3. Escaneo y enumeración de servicios Web
- ◆ 4. Inyección SQL (SQLi)
- ◆ 5. Cross Site Scripting (XSS)
- ◆ 6. Uso de herramientas (ZAP, BurpSuite)
- ◆ 7. File Upload
- ◆ 8. Explotación
- ◆ 9. Pruebas de autenticación.

# **CROSS SITE SCRIPTING (XSS)**

Top 03 OWASP

3

## **Conceptos Previos**

4

## ¿Qué es el XSS?

- ♦ Forma de ataque que aprovecha el mal filtrado de datos en una aplicación web. Es un ataque que se orienta al lado del cliente.
- ♦ Para cambiar el comportamiento de la aplicación se deberá **inyectar código** como por ejemplo **JavaScript** u otro tipo que se ejecute del lado del cliente (client-side).
- ♦ Lo que se realice con esta técnica no afecta directamente al servidor, sin embargo se pueden obtener cuentas de usuarios o redireccionar las visitas.
- ♦ Los tipos de XSS mas comunes son el **Reflejado** y el **Almacenado**.

5

## XSS Reflejado

- ♦ La inyección de código no permanece en la página que pueda afectar a todos los visitantes de la aplicaciones, por el contrario es dirigido a usuarios específicos.
- ♦ El código mas simple utilizado para verificar la vulnerabilidad XSS es el siguiente:

```
<script>alert("vulnerable a XSS")</script>
```

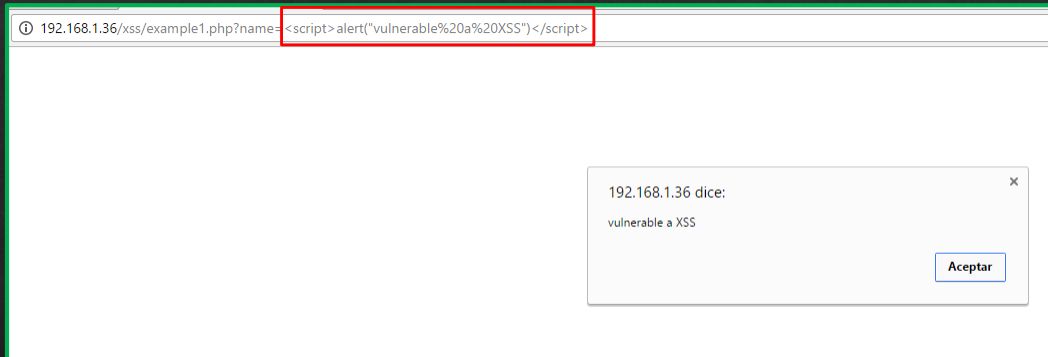
Opciones:

```
<script>alert(1)</script>
```

```
<script>alert("XSS")</script>
```

6

## XSS Reflejado



7

## XSS Reflejado

- Los desarrolladores pueden agregar ciertos filtros, como por ejemplo que no se permita las palabras `<script>` y `</script>`, pero cambiando a mayúsculas algunas letras se puede obtener el mismo resultado.

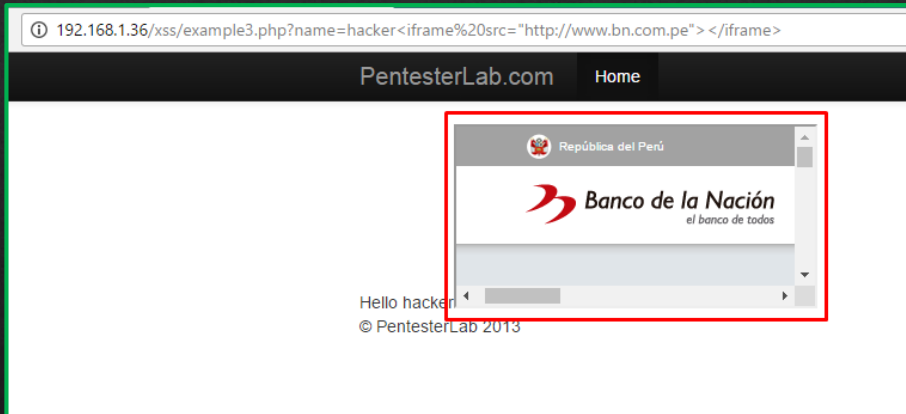


8

## XSS Reflejado

- ♦ Insertar paginas maliciosas dentro de la página real.

`<iframe src="http://www.bn.com.pe"></iframe>`



9

## XSS Reflejado

- ♦ Obtener cookies

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

- ♦ Se puede generar un ataque de obtener cookies con los inicios de sesión que el usuario haya realizado, por ejemplo, bancos, compras, servidores, etc.

10



## DESAFIO 5

- ◆ Realizar un ataque de DoS utilizando XSS en una web vulnerable.

**PUNTOS G: 3**

11

**UPLOAD FILE**

12

## DESAFIO 6

- ◈ Subir un archivo con código que ejecute comandos en un servidor web y obtener información de interés.
- ◈ Para escribir el script con código adecuado deberá identificar previamente el sistema operativo que tiene el servidor web.
- ◈ Mas datos en clases...

**PUNTOS G: 3**

13

## DESAFIO 7

- ◈ Hacer un DEFACE a una aplicación web.
- ◈ Subir un webshell
- ◈ La nueva página de inicio debe aparecer con el siguiente mensaje:

**“El grupo ..... Es responsable del DEFACE”**

**PUNTOS H: 8**

14