

# ATAQUES XSS





**XSS es un ataque dirigido a páginas web y consistente en poder inyectar código HTML y Javascript sin que sea validado para conseguir algún provecho**

# 1.

## INTRODUCCIÓN

# INTRODUCCIÓN

XSS es un vector de ataque usado para robar:

- Información sensible
- Secuestrar sesiones de usuario
- Subyugar en la integridad del sistema
- ...

Tipos de XSS:

- Directa
- Reflejada

# 2.

## TIPOS DE XSS

# XSS DIRECTA

- También conocida como **persistente**
- Difícil de encontrar
- Suele encontrarse en formularios
- Con este método, **siempre que alguien entre en la ruta donde se ha inyectado el código se ejecutará en su navegador**
- Defacement `<div>`

# XSS INDIRECTA

- También conocida como **reflejada**
- Más fácil de encontrar
- Código inyectado a través de formularios, URL, programas en Flash o incluso vídeos
- Complicado tener éxito **ya que hay que conseguir que alguien entre en el enlace malicioso.**
- ¿Ingeniería social?

# 3.

## EJEMPLOS DE XSS

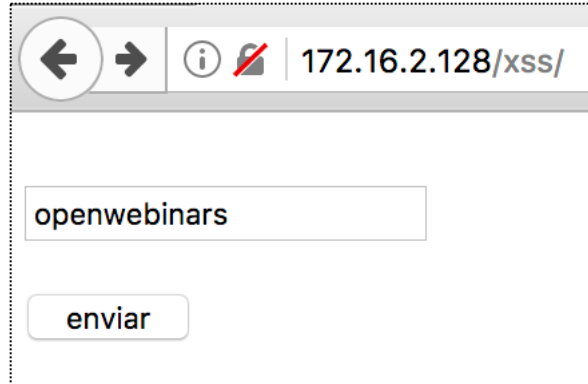


# 1º EJEMPLO (FORMULARIO)

```
<HTML>
  <HEAD><TITLE>XSS EJEMP1</TITLE></HEAD>
  <BODY>
    <FORM METHOD="get" ACTION="xss.php">
      <INPUT TYPE="text" NAME="vuln">
      <INPUT TYPE="submit" VALUE="enviar">
    </FORM>
  </BODY>
</HTML>
```

```
<?php
  $var = $_GET["vuln"];
  echo "Has escrito: ".$var;
?>
```

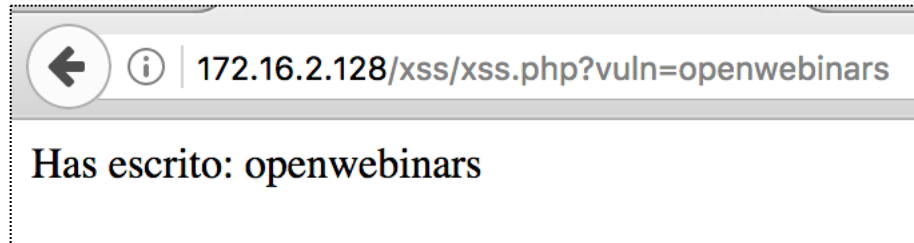
# 1º EJEMPLO (FORMULARIO)



172.16.2.128/xss/

openwebinars

enviar



172.16.2.128/xss/xss.php?vuln=openwebinars

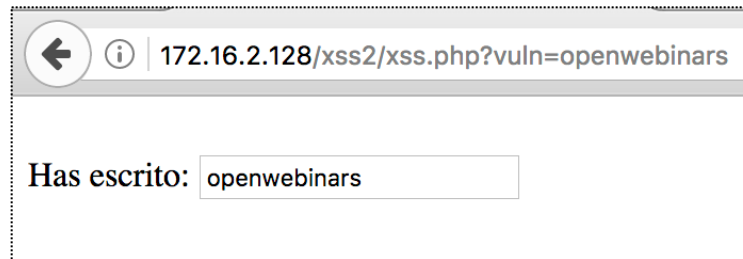
Has escrito: openwebinars

## 2º EJEMPLO (INSERTADO EN CAJA)

```
<?php
$var = $_GET["vuln"];
?>
<FORM>
  Has escrito: <INPUT TYPE="text" VALUE="<?php echo $var; ?>">
</FORM>
```



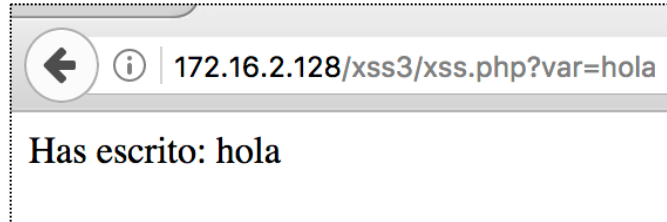
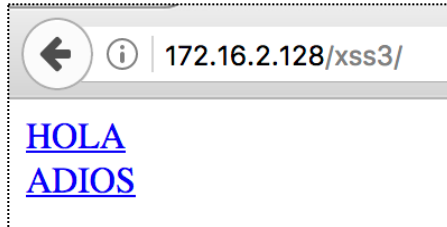
A screenshot of a web browser window. The address bar shows the URL '172.16.2.128/xss2/'. The page title is 'Ejercicio XSS caja de texto'. Below the title, there is a text input field containing the text 'openwebinars' and a button labeled 'enviar'.



A screenshot of a web browser window. The address bar shows the URL '172.16.2.128/xss2/xss.php?vuln=openwebinars'. The page content displays 'Has escrito:' followed by a text input field containing the text 'openwebinars'.

### 3º EJEMPLO (A TRAVÉS DE URL)

```
<BODY>  
  <A HREF="xss.php?vuln=hola">HOLA</A>  
  <A HREF="xss.php?vuln=adios">ADIOS</A>  
</BODY>
```



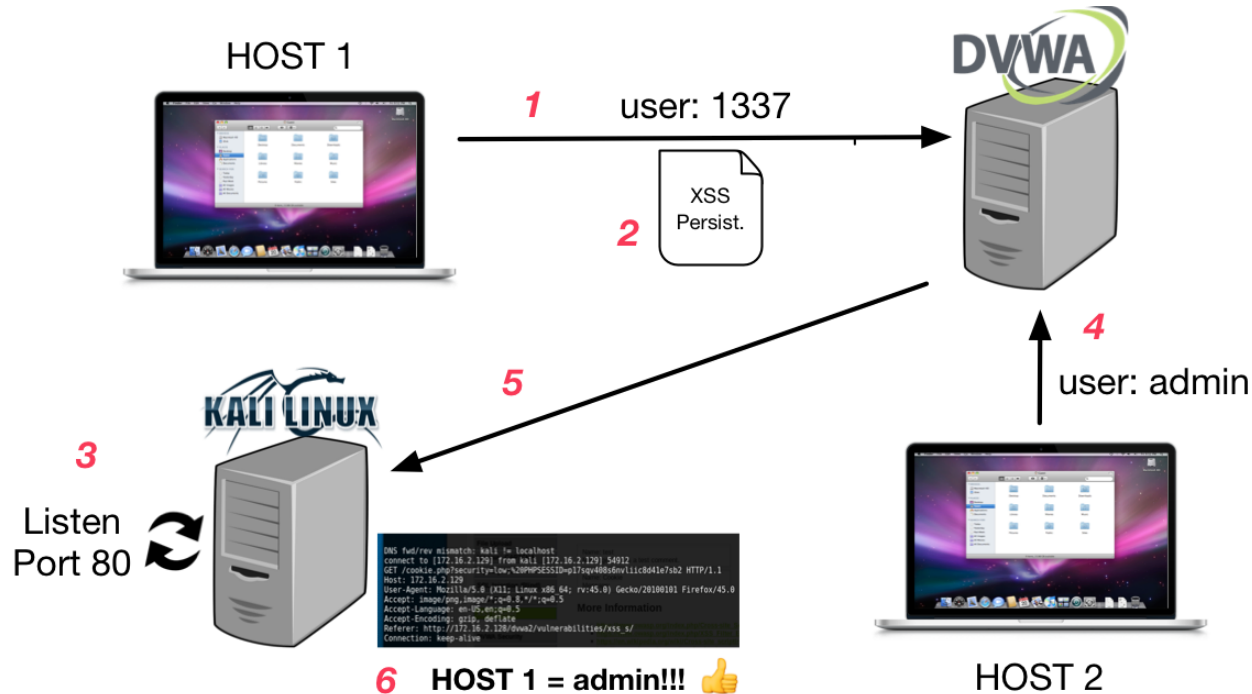
# 4.

## ROBO DE SESIONES (COOKIES)

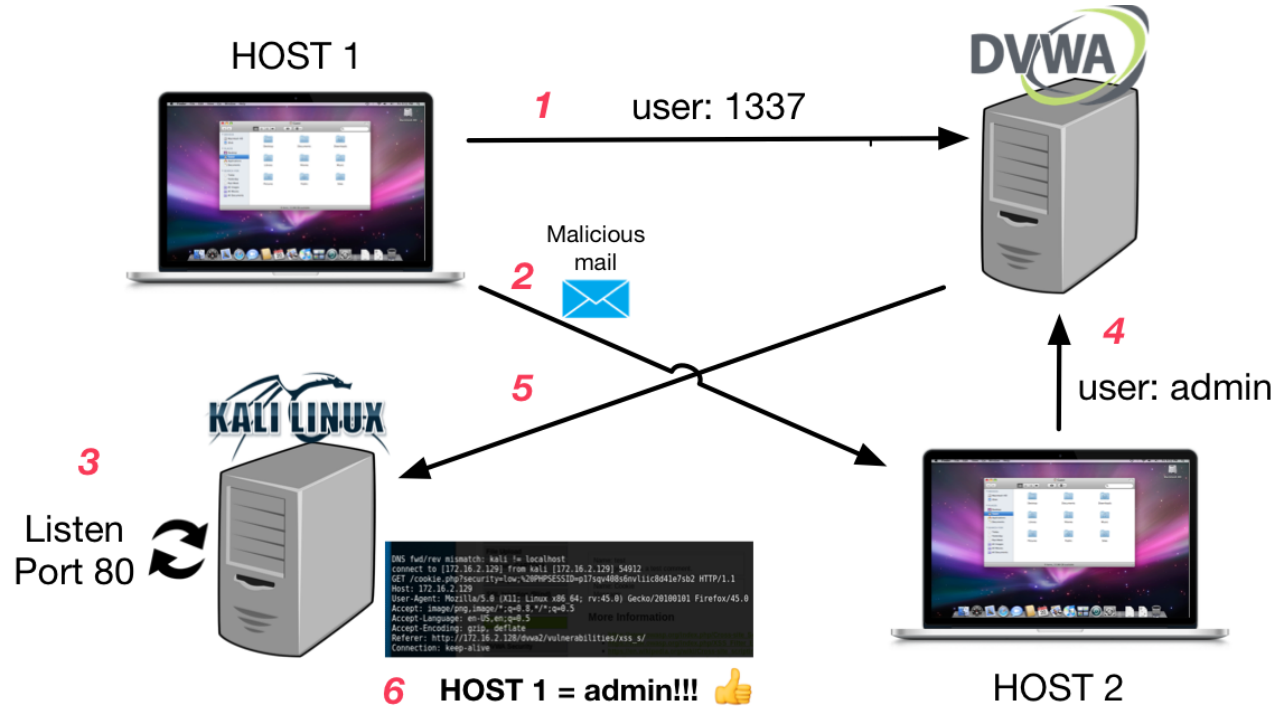
# COOKIES

- Almacenamiento temporal que usan páginas de internet
- Enviadas por la página web y almacenadas por los navegadores del cliente
- Actúan sobre los usuarios:
  - Los identifican y diferencian
  - Preferencias personales
  - Actividad realizada

# XSS PERSISTENTE



# XSS REFLEJADO





# 5.

## PREVENCIÓN

# PREVENCIÓN

Primera regla: ***No confiar nunca en datos obtenidos de usuarios o fuentes externas***

***Saneando datos:*** Manipular para quedarse con lo que interesa. Sanear el HTML: `script_tags()`;

***Escapando datos:*** Evita que el navegador lo ejecute y evalúe el código: `htmlspecialchars()`;