

UNIVERSIDAD AUTÓNOMA DE CHIAPAS



FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
CAMPUS 1

ING. EN DESARROLLO Y TECNOLOGÍAS DE SOFTWARE

7 "M"

OPT.2 - ANÁLISIS DE VULNERABILIDADES

SUB2 - HUELLAS DIGITALES Y RECONOCIMIENTO

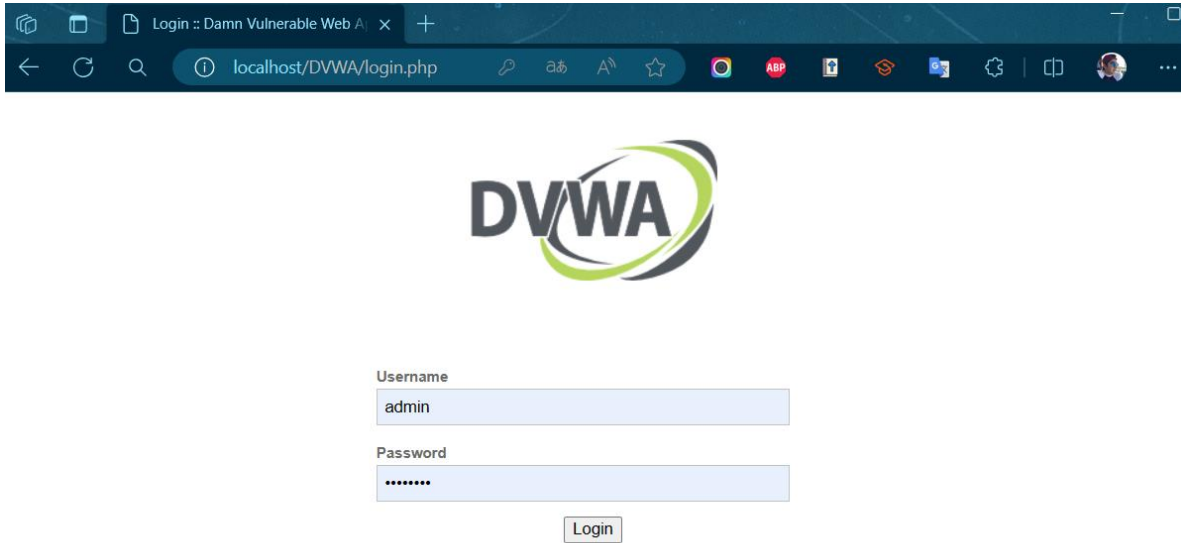
ACT. 2.5 REALIZAR LA INSTALACIÓN DE LA APLICACIÓN WEB
DVWA LOS SIGUIENTES ATAQUES AL DVWA

ALUMNO: MARCO ANTONIO ZÚÑIGA MORALES – A211121

DOCENTE: DR. LUIS GUTIÉRREZ ALFARO

TUXTLA GUTIÉRREZ, CHIAPAS
SÁBADO, 23 DE MARZO DE 2024

DVWA instalado



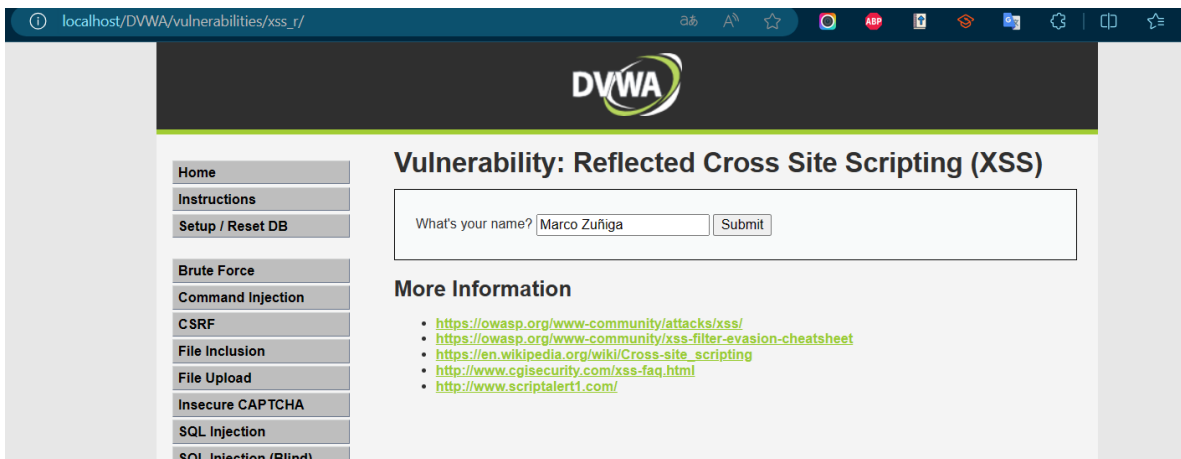
A screenshot of a web browser showing the DVWA login page. The address bar indicates the URL is localhost/DVWA/login.php. The page features the DVWA logo at the top. Below the logo, there are two input fields: 'Username' with the text 'admin' and 'Password' with masked characters. A 'Login' button is positioned below the password field.

Username
admin

Password

Login

Ingresando al XXS (Reflected)



A screenshot of the DVWA 'Vulnerability: Reflected Cross Site Scripting (XSS)' page. The left sidebar contains a menu with options like Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, and SQL Injection (Blind). The main content area has the DVWA logo and the title 'Vulnerability: Reflected Cross Site Scripting (XSS)'. Below the title is a form with the text 'What's your name?' followed by an input field containing 'Marco Zuhiga' and a 'Submit' button. Underneath the form is a 'More Information' section with a list of links related to XSS attacks.

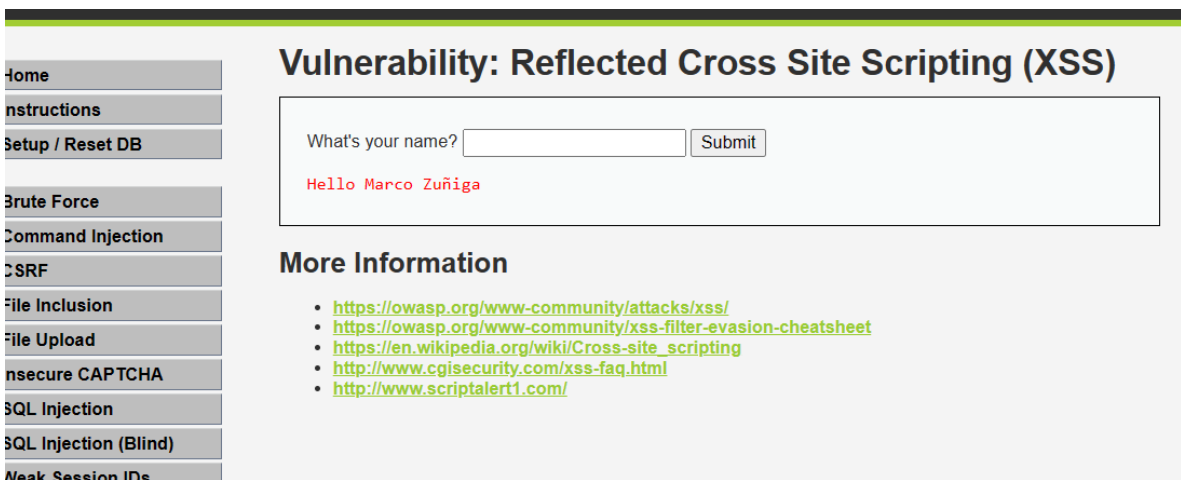
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Marco Zuhiga Submit

More Information

- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>



A screenshot of the DVWA 'Vulnerability: Reflected Cross Site Scripting (XSS)' page after a successful attack. The left sidebar is the same as in the previous screenshot. The main content area shows the DVWA logo and the title 'Vulnerability: Reflected Cross Site Scripting (XSS)'. Below the title is a form with the text 'What's your name?' followed by an empty input field and a 'Submit' button. Below the form, the text 'Hello Marco Zuhiga' is displayed in red, indicating the successful execution of the injected script. Underneath the form is a 'More Information' section with a list of links related to XSS attacks.

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

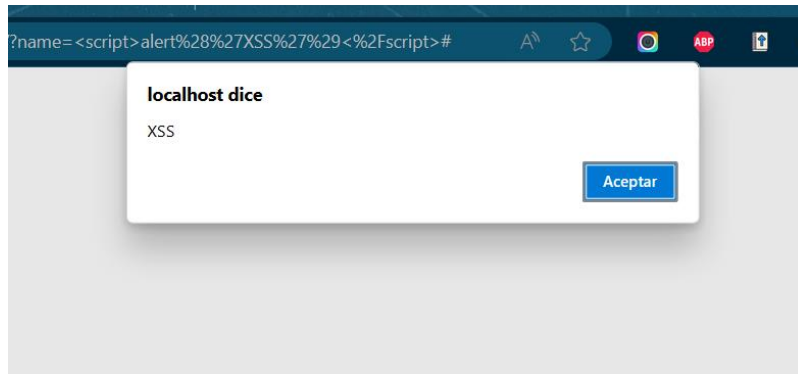
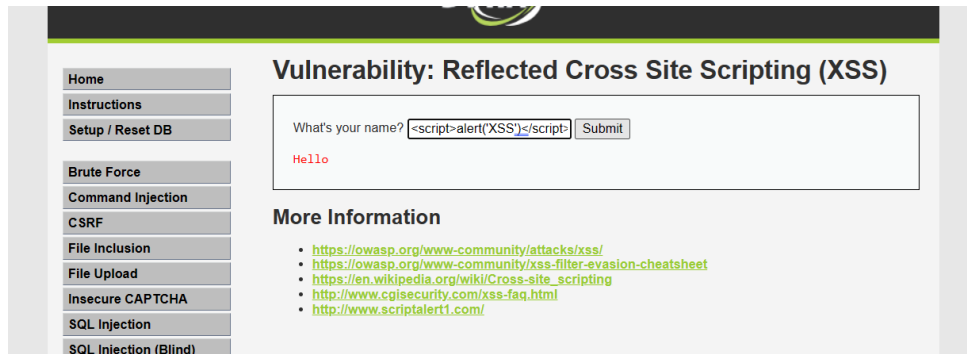
Hello Marco Zuhiga

More Information

- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- https://en.wikipedia.org/wiki/Cross-site_scripting
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

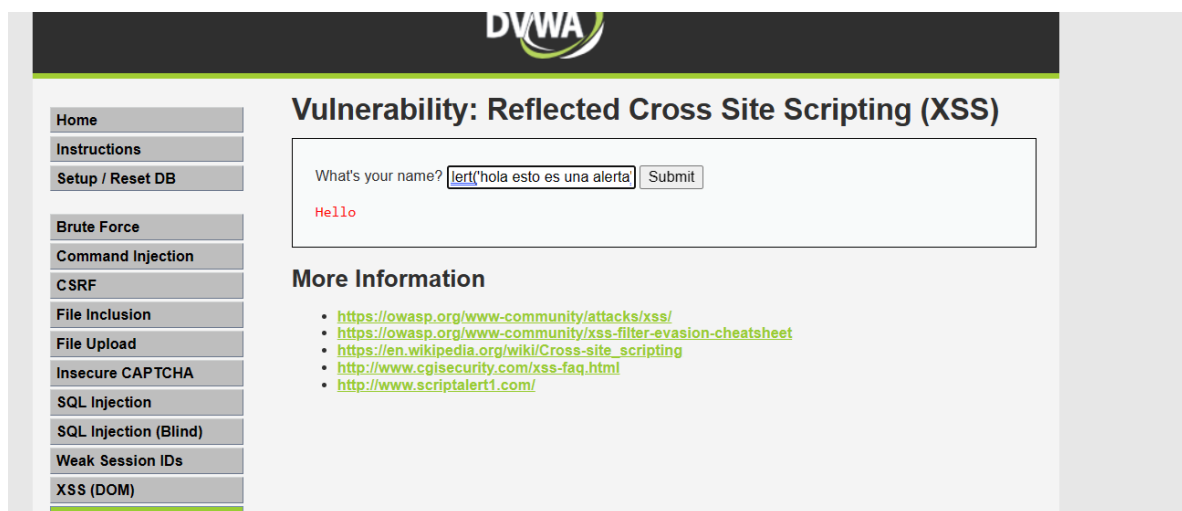
Ahora probaremos más scripts para ver la vulnerabilidad de DVWA

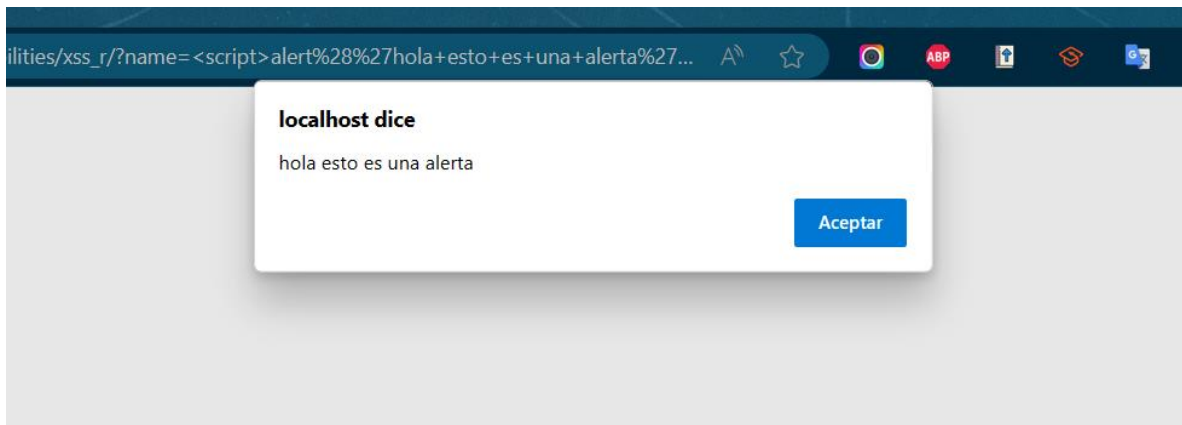
```
<script>alert('XSS')</script>
```



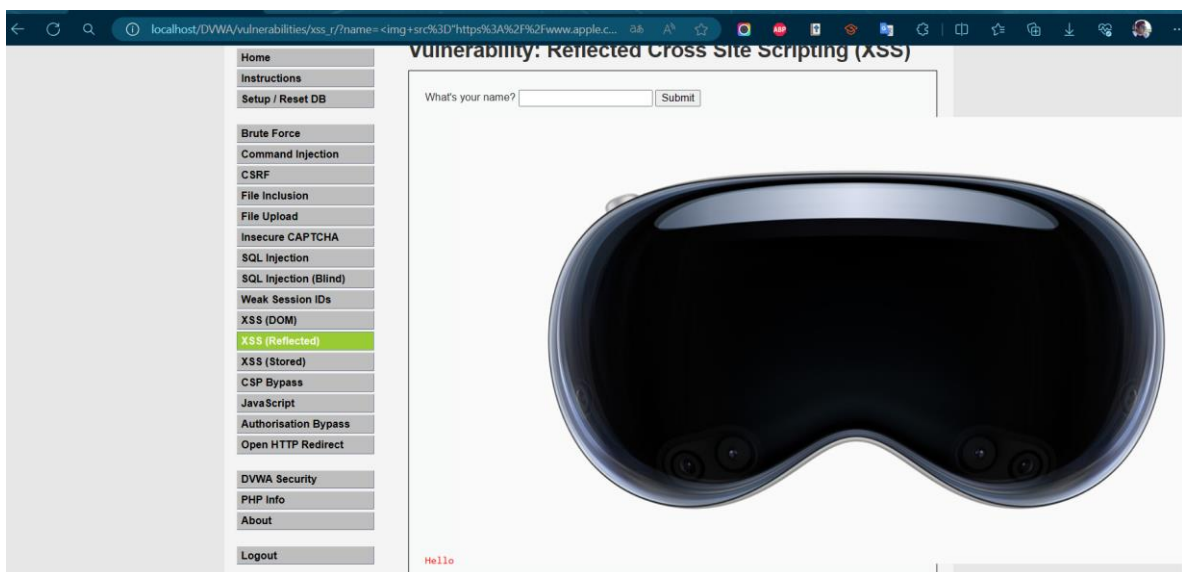
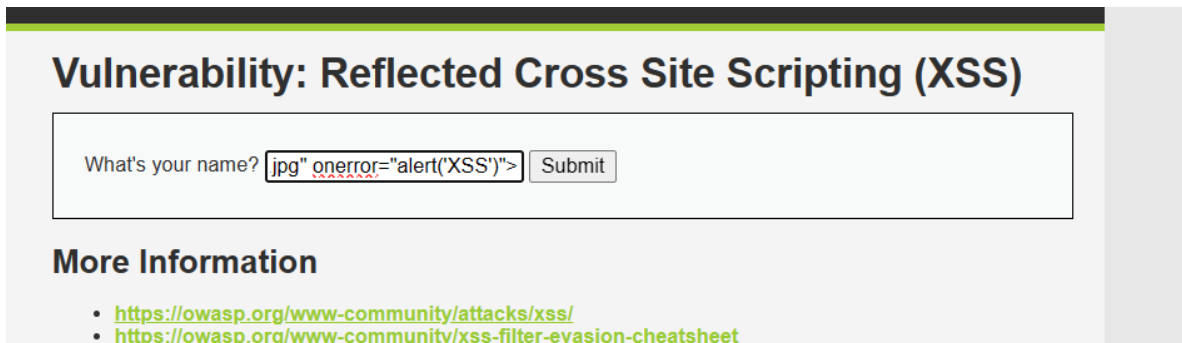
Modificaremos esta alerta para que salgan más cosas

```
<script>alert('hola esto es una alerta')</script>
```



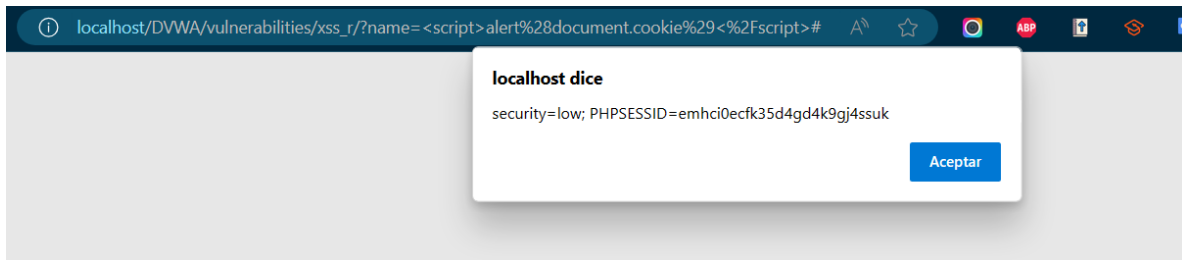


``



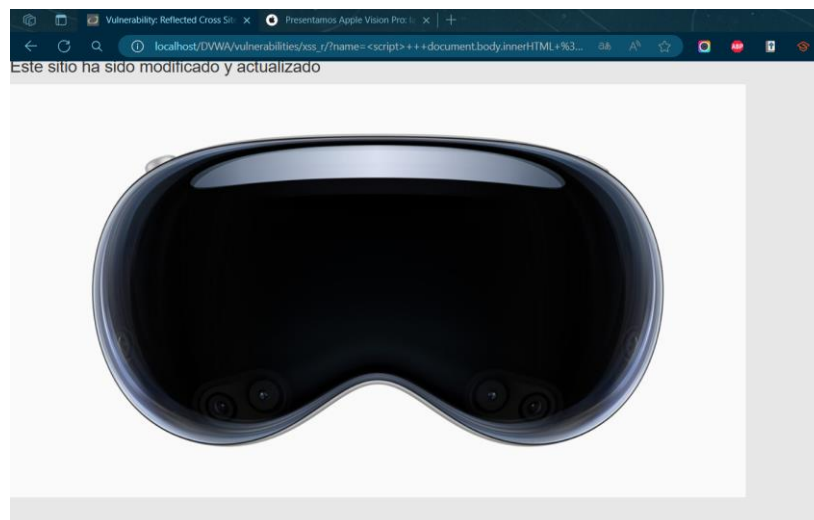
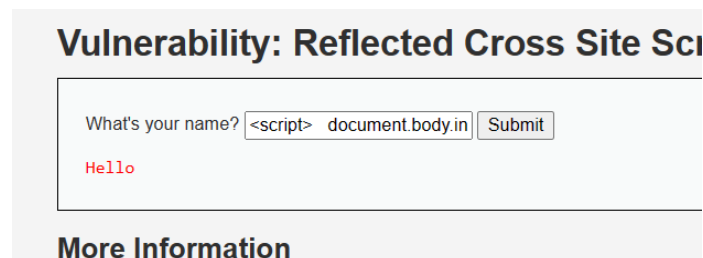
Script para obtener cookies:

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



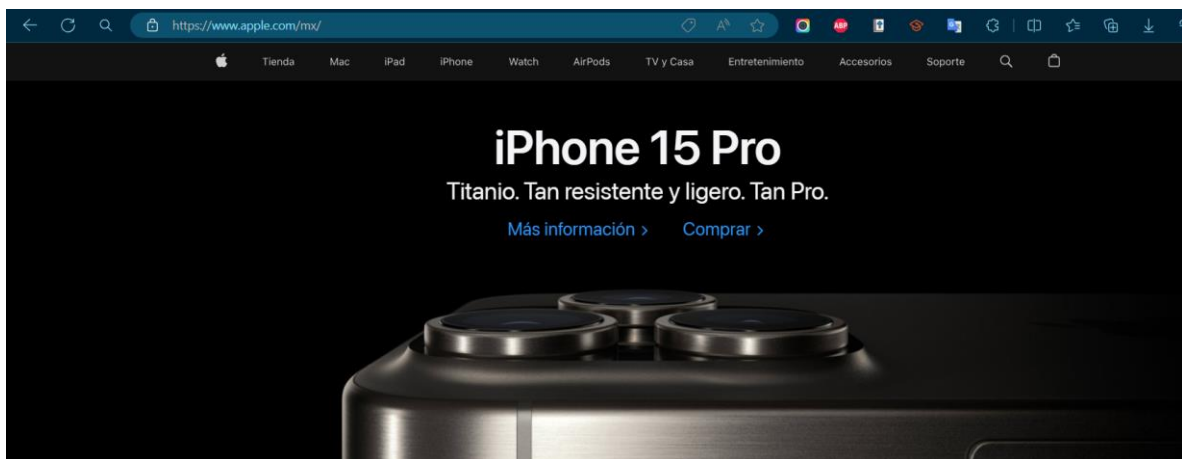
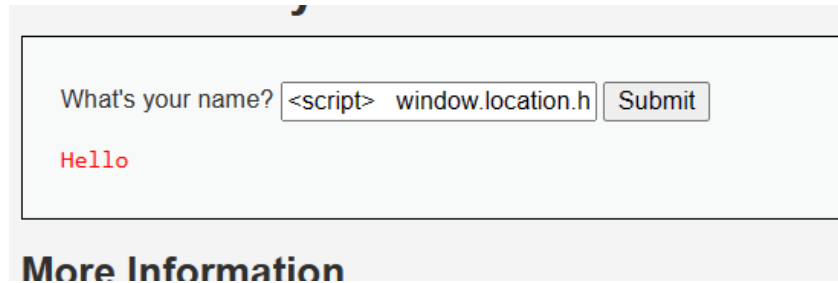
Script para modificar toda la página, en este caso le pondremos una imagen y un texto

```
<script>
  document.body.innerHTML = '<div style="font-family: Arial; font-size: 22px;">Este
  sitio ha sido modificado y actualizado</div><br>';
</script>
```



Script para redirigir a otro sitio cualquiera

```
<script>  
  window.location.href = 'https://www.apple.com/mx/';  
</script>
```



Conclusión

La explotación de vulnerabilidades XSS en aplicaciones web vulnerables, como se demuestra en los ejemplos anteriores, subraya la importancia crítica de implementar prácticas de desarrollo seguro. Esto incluye la validación y saneamiento riguroso de todas las entradas de usuario, la implementación de políticas de seguridad de contenido (CSP), y el uso de respuestas HTTP que restrinjan el acceso a las cookies a través de scripts.

Además, es fundamental educar a los desarrolladores sobre las mejores prácticas de seguridad y realizar auditorías de seguridad regulares en las aplicaciones web. Estas medidas son esenciales para proteger tanto a los usuarios como a las organizaciones de los impactos potencialmente devastadores de los ataques XSS y asegurar un entorno en línea más seguro y confiable.

Estos scripts sencillos que inserte dentro de DVWA nos da un claro ejemplo de cómo es que podemos hackear o modificar un sitio web que esta vulnerable, como en este caso DVWA tiene una configuración de seguridad vulnerable podemos ver podemos realizar estas consultas y que la página web sea modificada. Podemos realizar scripts mucho más elaborados para cambiar totalmente la página. Esto nos da una idea de lo importante que es tener y mantener un sitio seguro para que no nos pasen este tipo de cosas en el día a día. Podemos apreciar el objetivo de esta actividad insertando código en el apartado de XSS (Reflected) de DVWA.