

hACKING éTICO

Unidad 2. Actividad 27



7 de FEBRERO de 2024

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

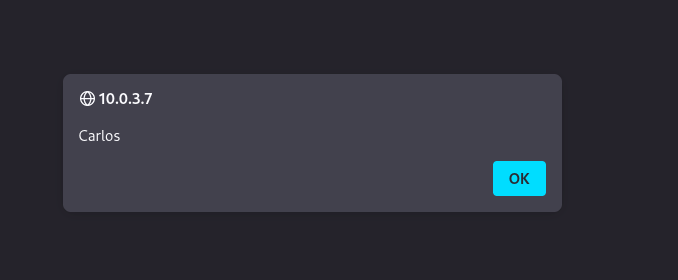
Índice

[XSS – Cross Site Scripting 2](#_Toc158221704)

# XSS – Cross Site Scripting

**Ejercicio 1: XSS Reflejado básico**

Primero la imagen del alert creada:

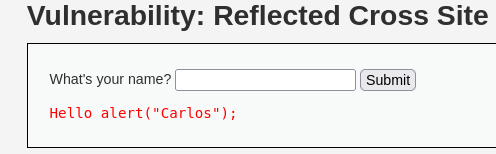


Después código usado:



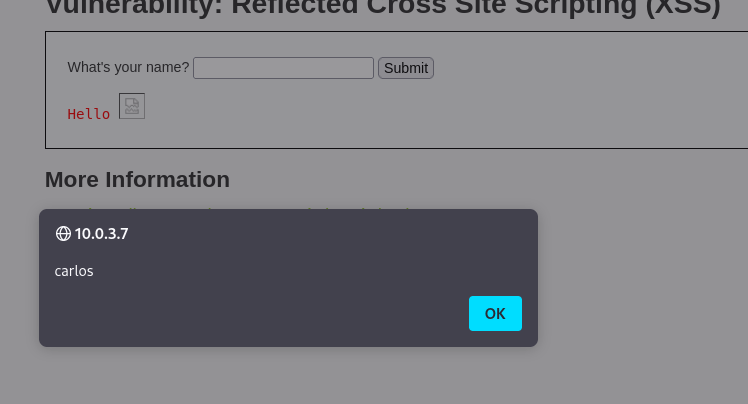
**Ejercicio 2: XSS Reflejado nivel medio**

Probamos de la primera forma:

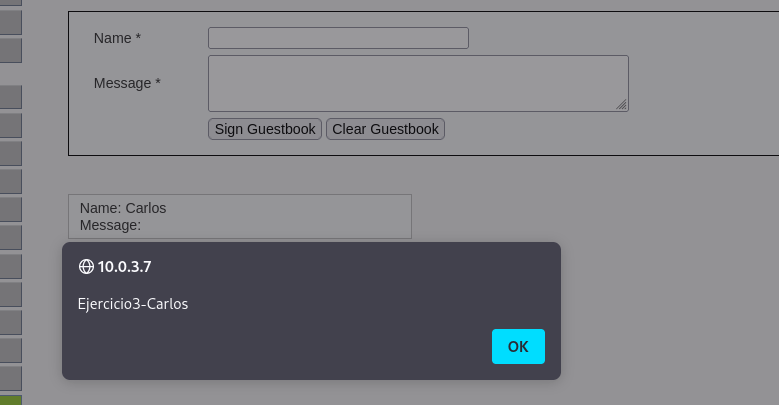




Probamos usando una imagen con evento:



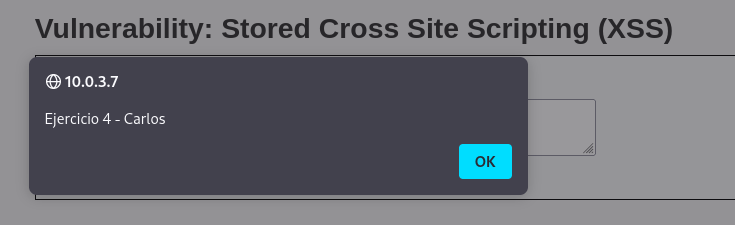
**Ejercicio 3: XSS Almacenado nivel bajo**En nombre he puesto mi nombre y en mensaje he puesto <IMG SRC="#" onerror="alert('Carlos')">





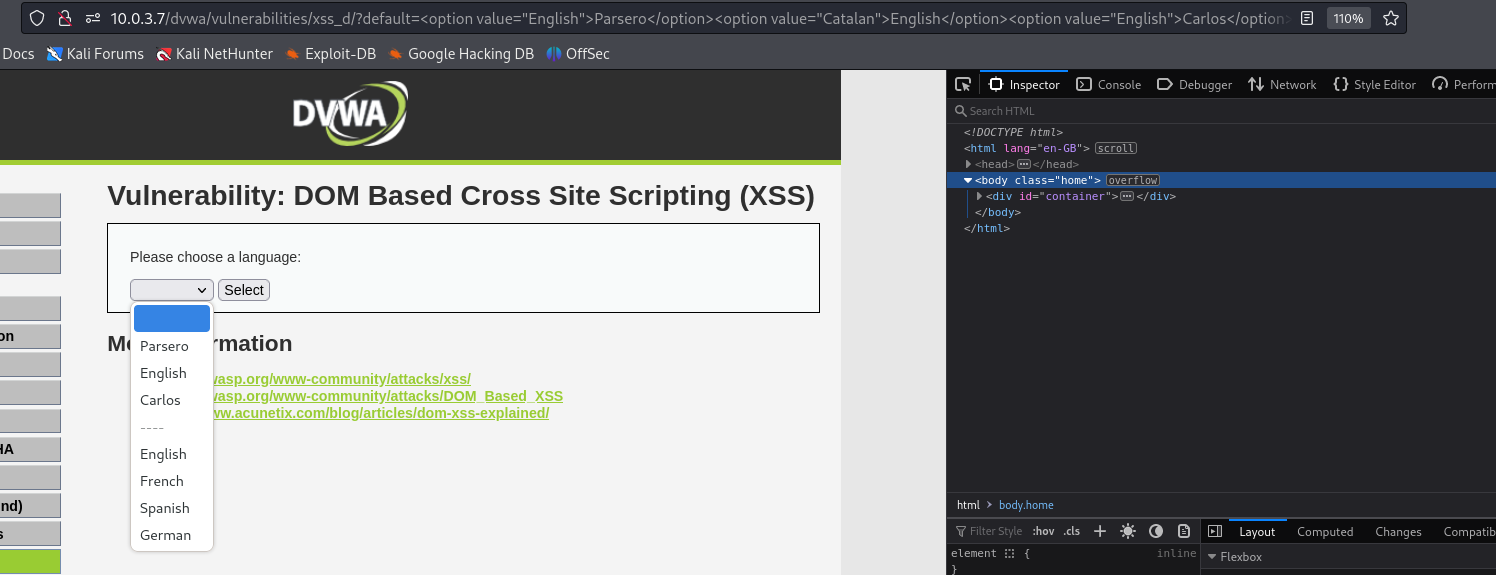
**Ejercicio 4: XSS Almacenado nivel medio**

He realizado lo mismo que antes solo que en vez de ponerlo en el mensaje lo he puesto en el nombre:



**Ejercicio 5: Dom XSS nivel bajo**

He copiado esto <option value="English">English</option> y he cambiado English por el nombre que quería y lo he puesto en la url 3 veces.



**Ejercicio 6: Imagen con trampa con Dom XSS**

En mi caso lo he hecho desde el apartado de DOM.

Primero he buscado un script que sirva para lo que nos pide el ejercicio:

<IMG SRC=# onmouseover="alert('Carlos')">

Ahora este vamos a editarlo, primero donde nos pone # vamos a poner la url de nuestra foto, donde pone Carlos vamos a continuar también poniendo document.cookie.

Ahora solo hay que buscar el lenguaje que queramos y simplemente cerramos el option y elselect y ya pegamos nuestro código:

