

Alcapdemy:

Curso de Cross-Site Scripting (XSS)

1. Cross-Site Scripting (XSS)

XSS es una vulnerabilidad web que permite a un atacante inyectar scripts maliciosos en una página web. Estos scripts pueden robar datos (como cookies) o realizar acciones.

2. Tipos de XSS

-Reflected XSS:

El script malicioso se envía en una solicitud y se refleja en la respuesta.

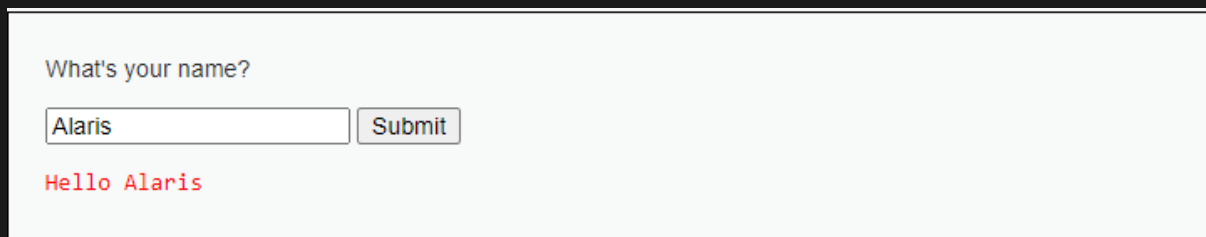
-Stored XSS:

El script malicioso se almacena en el servidor (como en un comentario) y se muestra a otros usuarios.

3. Detectar un XSS

-Reflected XSS:

1. Busca una entrada de texto en la web, prueba a introducir cualquier cosa

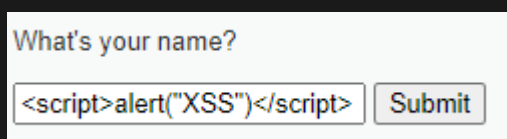


What's your name?

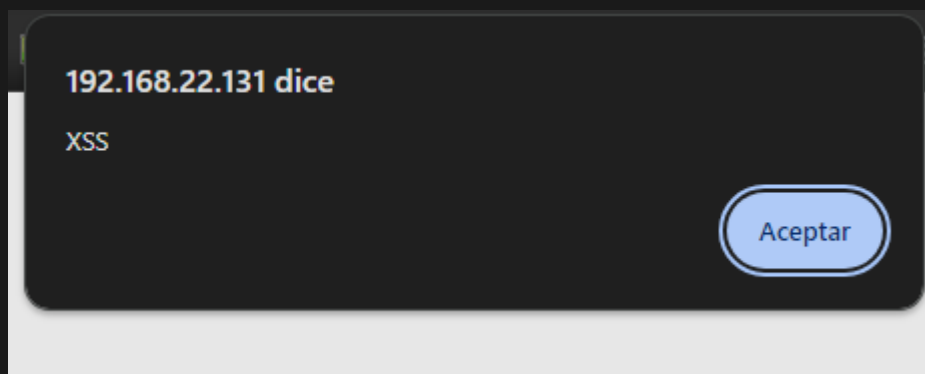
Hello Alaris

En este caso nos está reflejando lo que hemos puesto en la entrada de texto

2. Prueba a poner un script que nos de una alerta para ver si es vulnerable a XSS



What's your name?



El navegador nos muestra la alerta con el mensaje que hemos puesto, lo que significa que es vulnerable a XSS (reflected)

-Stored XSS:

1. Busca una entrada de texto en la web, prueba a introducir cualquier cosa

A form for a guestbook. It has two input fields: 'Name *' and 'Message *'. Below the 'Message *' field is a 'Sign Guestbook' button. Below the form is a preview area showing 'Name: test' and 'Message: This is a test comment.'

En este caso es un blog en el que pones tu nombre y un mensaje

2. Probamos a modificar el html con una etiqueta html

A form for a guestbook, similar to the one above. The 'Name *' field contains 'Alaris'. The 'Message *' field contains '<h1>XSS</h1>'. Below the form is a preview area showing 'Name: Alaris' and 'Message: XSS' in a large, bold font.

Es vulnerable a XSS debido a que el tamaño del mensaje se ha puesto en el tamaño de la etiqueta h1. Este XSS es de tipo stored debido a que se almacena en el servidor y también se está mostrando a otros usuarios

4.Explotar XSS

Hay múltiples formas de explotar un XSS, tantas que no puedo enumerarlas todas aquí. Lo importante que debes saber es que puedes ejecutar scripts maliciosos en el navegador de las víctimas. Estos scripts maliciosos pueden ser creados por ti si sabes programación, o puedes encontrarlos en internet.