Puesta en producción segura

2 de Enero de 2024

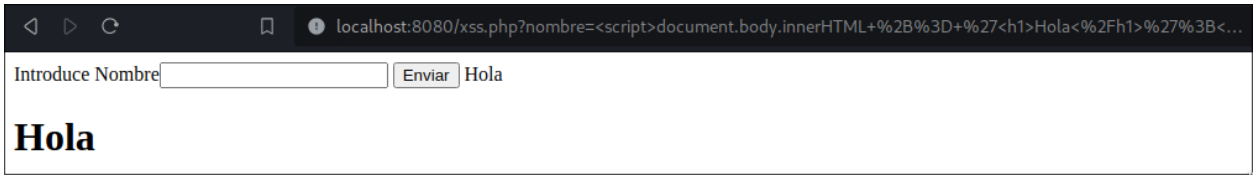
Práctica 2.5: XSS Reflejado

Jose Almirón López

Comenzamos con un código llamado 'xss.php', que presenta vulnerabilidades a ataques XSS. En este escenario, realizaremos pruebas para demostrar las amenazas potenciales asociadas y, posteriormente, procederemos a fortalecer y sanear el código para prevenir con eficacia este tipo de ataques.

1. Introduce el código Javascript necesario para mostrar el mensaje “Hola”.

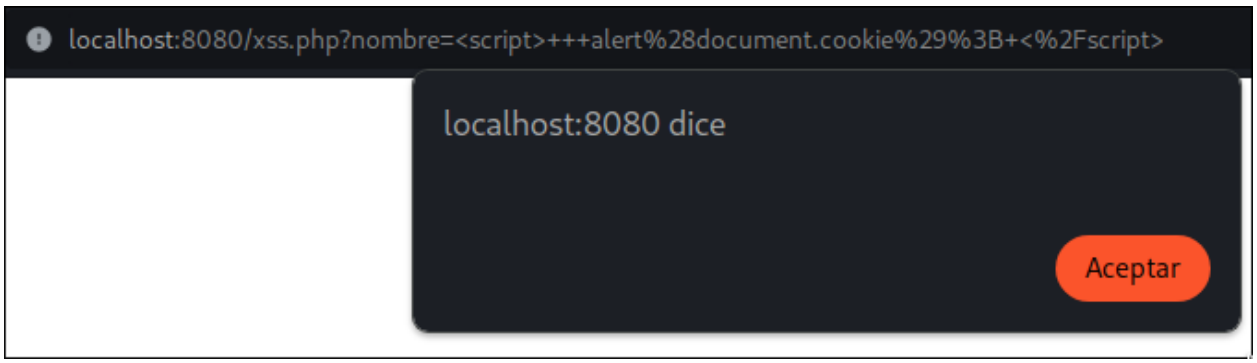
<script>document.body.innerHTML += '<h1>Hola</h1>';</script>



2. Introduce el código Javascript necesario para mostrar la cookie del usuario.

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

A pesar de lo evidenciado en la imagen, en este caso no se ha identificado ninguna cookie.



3. Introduce el código Javascript necesario para redirigir la página a Google.es usando la función “window.location” .

<script>window.location = 'https://www.google.es';</script>

4. Sanear los datos para evitar ataques XSS.

```php
<?php
if (isset($_GET["nombre"])) {
    $nombre = htmlspecialchars($_GET["nombre"], ENT_QUOTES, 'UTF-8');
    echo "Hola " . $nombre;
}
?>
```

- Se utiliza la función ***htmlspecialchars*** para escapar el contenido de ***$_GET["nombre"]***. Esto asegura que cualquier código HTML o script se convierta en texto plano y no se ejecute en el navegador.
- Se establece el tercer argumento de ***htmlspecialchars*** a '***UTF-8***' para especificar la codificación del conjunto de caracteres.