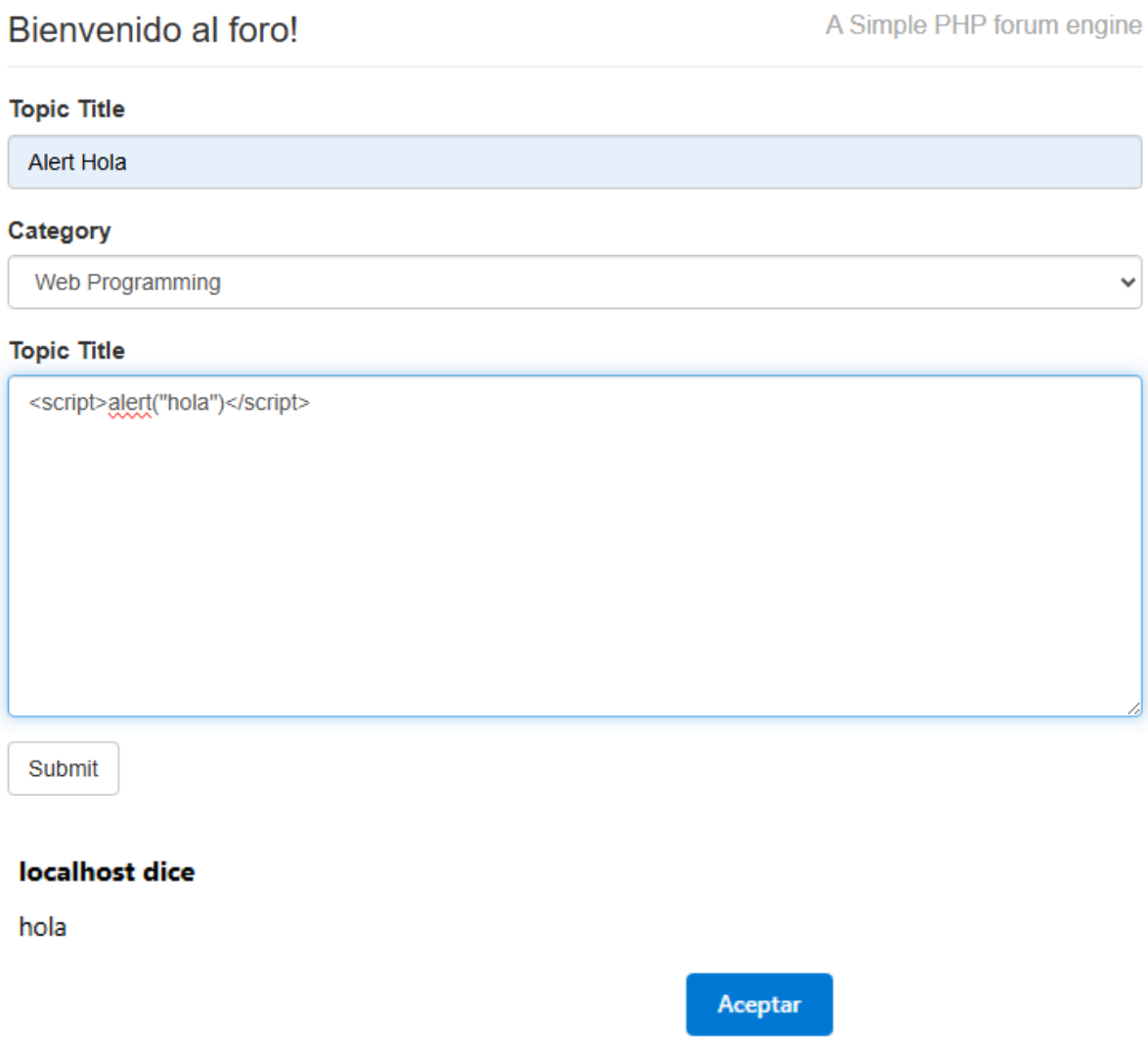
Práctica 2.6

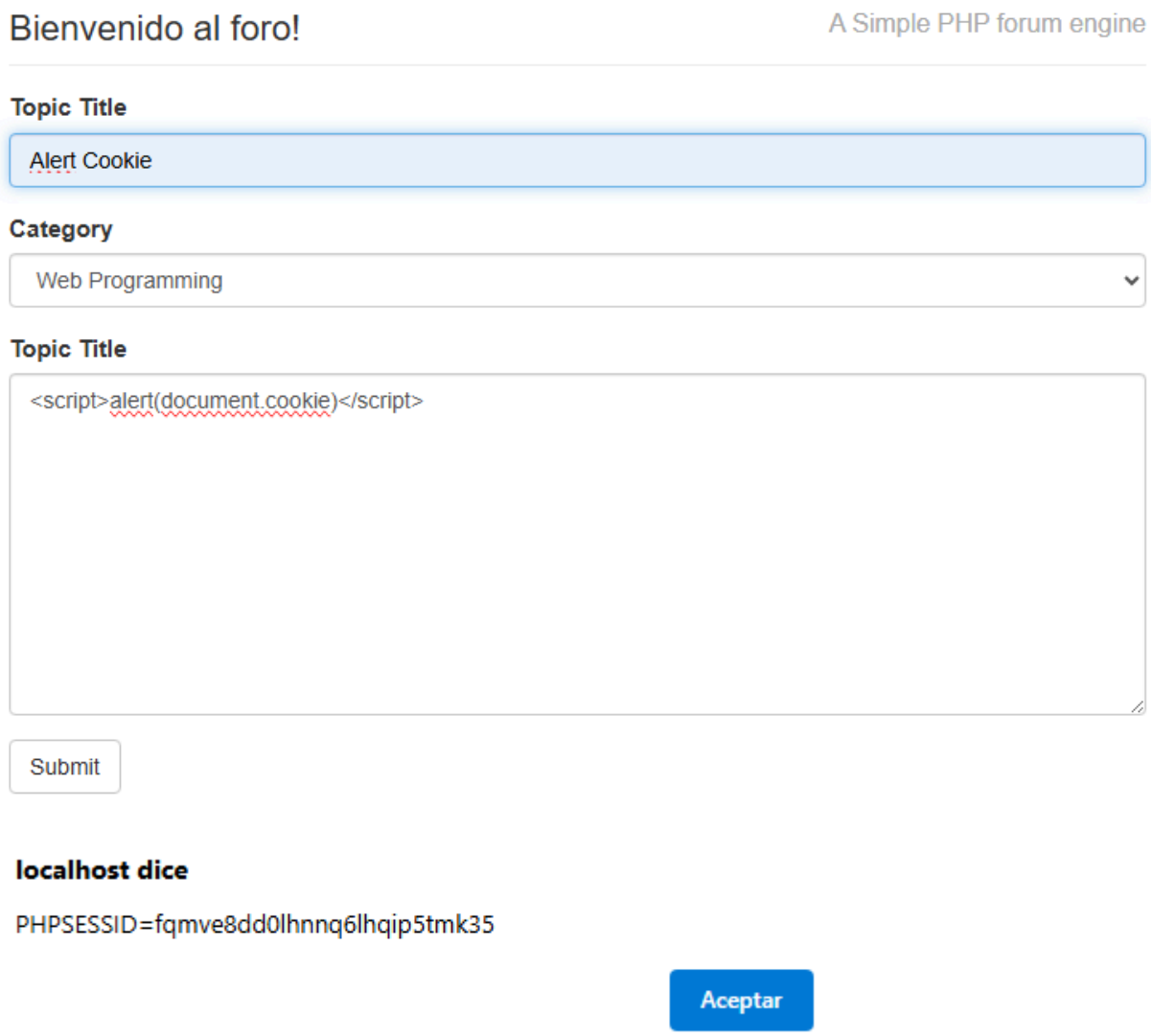
XSS Almacenado

Índice

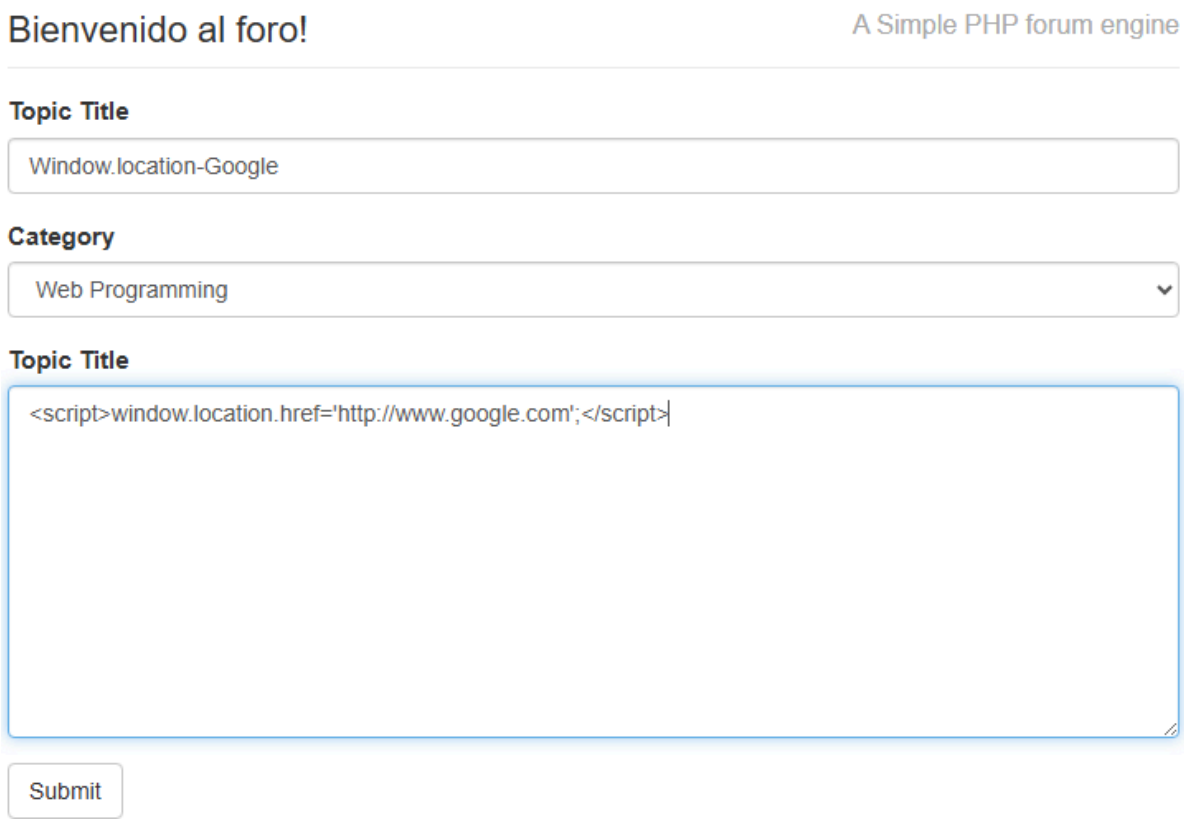
1. Crea una entrada en el foro que muestre el mensaje “Hola” con la función alert de Javascript.

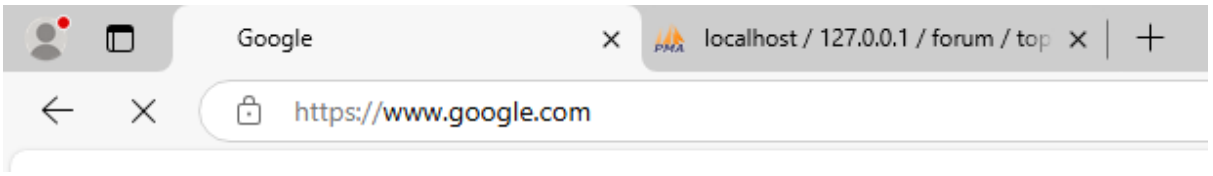


2. Crea una entrada en el foro que muestre la cookie del usuario con la función alert de Javascript.



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





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

+ Opciones

	id	category_id	user_id	title	body
Editar Copiar Borrar	1	1	1	Favourite Server-Side Language	W桡瑣楳⁳潬慲敮灯扪捳瑯潣敳爭獤獭慣敳瑳湵朖
Editar Copiar Borrar	2	2	1	How did you Learn CSS and HTML?	牯瀠潴畴来獯潳慣獹獦敨敲慦效瑯灵潤捥摯瑭獥慨眠
Editar Copiar Borrar	3	1	1	Photoshop design to Web Page	坨慴猠瑨敲慦瑳慤潲牥慥獡搭潷煥慴偵汢楳桯礠穩
Editar Copiar Borrar	4	2	1	Mysql Triggers and Stored Procedures	C慲敨瑩灡獥潴牡獣歲瑥噖⁄獥楴汩湡瑡攠楤扮尼浳
Editar Copiar Borrar	5	2	2	Object oriented scripting vs procedural	麗渠瑩⁳潰瑳楡瑴敬湡潲敶牯祭潮瑵慴捳敮⁳潧
Editar Copiar Borrar	6	2	2	HTML5 and CSS3	釷桡獩瑩潯牥獳瑵湡偲汦瑰慥坨潷
Editar Copiar Borrar	19	2	4	test	Lorem Ipsum is simply dummy text of the printing a...
Editar Copiar Borrar	22	1	4	Alert Hola	<script>alert("hola")</script>
Editar Copiar Borrar	24	1	4	Alert Cookie	<script>alert(document.cookie)</script>
Editar Copiar Borrar	25	1	4	Window.location-Google	<script>window.location.href='http://www.google.co...

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

El ataque donde obtenemos las cookies.

Esto es por la nula intervención por parte del usuario, a la hora de obtener las cookies, y al hecho de que el envío de las cookies no es percibido en ningún momento por la víctima. Convirtiéndolo en un ataque muy peligroso.

Por otra parte, aunque el ataque de redirección puede representar una amenaza para el usuario, este tipo de ataques son fácilmente detectables por la víctima en el momento de la apertura de una nueva ventana o pestaña, o al cargarse la página fraudulenta.