Ataques XSS o cross-site scripting

Un ataque XSS (Cross-Site Scripting) es una vulnerabilidad de seguridad que ocurre cuando un atacante inyecta código malicioso, generalmente JavaScript, en páginas web vistas por otros usuarios. Este código se ejecuta en el navegador de la víctima, lo que permite al atacante robar información, tomar el control de la sesión del usuario, redirigir a otros sitios maliciosos o incluso modificar el contenido de la página web.

Existen varios tipos de ataques XSS, pero generalmente se dividen en tres categorías:

Reflejado (Reflected XSS): En este tipo de ataque, el código malicioso se inyecta a través de un enlace malicioso o un formulario en la página web. La entrada del usuario se refleja en la página web sin ser sanitizada adecuadamente, lo que permite que el código malicioso se ejecute en el navegador de la víctima cuando visita esa página específica.

En este caso, un atacante crea un enlace malicioso o un formulario que contiene código JavaScript malicioso.

Cuando un usuario hace clic en el enlace o envía el formulario, el código malicioso se envía al servidor web.

El servidor web devuelve la página al usuario, incluyendo el código malicioso en la respuesta.

El navegador del usuario ejecuta el código JavaScript, ya que lo considera parte de la página legítima.

Este tipo de ataque a menudo se utiliza en campañas de phishing, donde el atacante intenta engañar al usuario para que divulgue información confidencial.

Prevención: Los WAF permiten mitigar este riesgo mediante la sanitización y validación adecuada de todas las entradas del usuario antes de mostrarlas en la página. Esto implica codificar o escapar caracteres especiales para que el navegador los interprete como texto plano en lugar de código ejecutable.

Persistente (Stored XSS): En este caso, el código malicioso se almacena en la base de datos de la aplicación web, como en un comentario de un blog o un mensaje en un foro. Cuando otros usuarios acceden a la página que contiene el código malicioso, este se ejecuta en sus navegadores, lo que les expone al ataque.

En este caso, el código malicioso se almacena en la base de datos de la aplicación web, como en un comentario de un blog, un mensaje en un foro o un perfil de usuario.

Cuando otros usuarios acceden a la página que contiene el código malicioso, este se ejecuta en sus navegadores.

Este tipo de ataque puede ser especialmente peligroso porque puede afectar a múltiples usuarios y persistir en la página web durante períodos prolongados.

DOM-based XSS: Este tipo de ataque ocurre cuando la vulnerabilidad XSS reside en el lado del cliente en lugar del servidor. El código malicioso se ejecuta en el navegador del cliente manipulando el Document Object Model (DOM) de la página web.

En este tipo de ataque, el código malicioso se ejecuta en el navegador del cliente manipulando el DOM de la página web.

El atacante aprovecha las vulnerabilidades en el código JavaScript de la página web para ejecutar código malicioso.

Este tipo de XSS no involucra necesariamente comunicación con el servidor, lo que lo hace más difícil de detectar mediante técnicas tradicionales de seguridad del lado del servidor.

Revision #1
Created 4 February 2024 08:41:57 by etaboada
Updated 4 February 2024 08:49:34 by etaboada