Ciberseguridad

¿Cuáles son los tipos de Cross-Site Scripting (XSS)?

Concientización

Ciberseguridad

XSS Reflejado

Ocurre cuando el script malicioso se envía como parte de una solicitud y es "reflejado" de inmediato en la respuesta de la aplicación web.

Ejemplo: El atacante puede enviar un enlace malicioso a la víctima y cuando haga clic en el enlace, el script incrustado en la URL se ejecuta en su navegador.

Concientización

Ciberseguridad

XSS Persistente

Ocurre cuando el código malicioso se almacena de forma permanente en el servidor web, como en una base de datos o en un archivo.

Ejemplo: Los atacantes suelen inyectar scripts en formularios de comentarios, post de foros o perfiles de usuarios, donde el script malicioso se guarda en el servidor.

Concientización

Ciberseguridad

XSS Basado en DOM

La vulnerabilidad no proviene de la respuesta del servidor, sino del código JavaScript en el lado del cliente. Aquí, el script malicioso se ejecuta manipulando el DOM (Document Object Model) de la página.

Ejemplo: El atacante manipula partes de la página web que interactúan con la URL o el contenido dinámico, haciendo que el navegador ejecute el script en la página sin necesidad de interacción con el servidor.

Concientización

Ciberseguridad

XSS A Ciegas

Es una variante donde el atacante no puede ver el resultado de su código inmediatamente, ya que el script malicioso se ejecuta en una interfaz de terceros (como un panel de administrador).

Ejemplo: El atacante puede inyectar un script en un campo de formulario. Cuando un administrador visualiza ese mensaje, el script se ejecuta en su navegador.

Concientización

Ciberseguridad

Seguinos y unite al discord para seguir aprendiendo

Guardar

Compartir

Seguir

Concientización