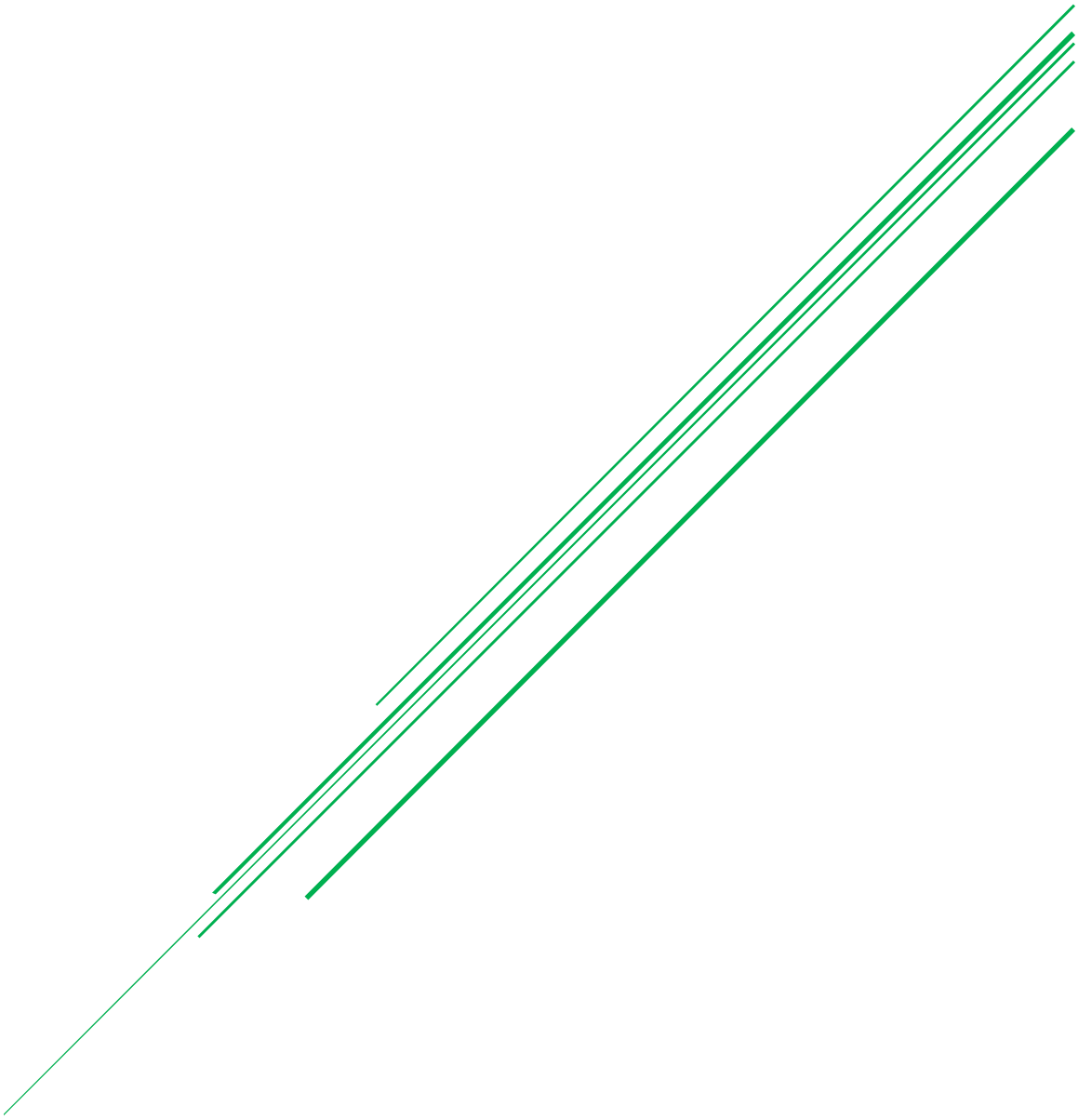
REPORTE- ATAQUES XSS VS CSRF

LUIS ALEJANDRO GÓMEZ SANTILLÁN - 190292



UTXJ

SEGURIDAD EN EL DESARROLLO DE APLICACIONES

1 Ataques CSRF

Un ataque CSRF es una técnica maliciosa que obliga al navegador web de una víctima, autenticada previamente en algún servicio como correo electrónico o banca online, a enviar una petición HTTP falsa a una aplicación web vulnerable.

Así el ciberdelincuente es capaz de realizar una acción a través de su víctima, ya que la actividad maliciosa será procesada en nombre del usuario conectado, por lo que la aplicación pensará que se trata de una petición legítima.

1.1 Prevención

1.1.1 Validación por token secreto

El mecanismo más usado para prevenir vulnerabilidades de sitios cruzados es solicitar información adicional en cada petición HTTP para determinar si en realidad viene de una fuente confiable. Este proceso consiste en la inclusión de un token secreto o valor aleatorio; que se genera y se informa al navegador del usuario en el momento que inicie sesión.

Este código de validación debe ser difícil de adivinar y si una solicitud no incluye dicho código o este no coincide con el valor esperado, el servidor rechazará la petición.

1.1.2 Envío doble de cookies

Otra acción que puede ayudar a prevenir la falsificación de solicitudes en sitios cruzados es el envío doble de cookies. Se trata de una variante del mecanismo del token; ya que en este caso el código debe corresponderse con el identificador de sesión en la cookie.

El servidor debe comprobar que ambas sean iguales en cada solicitud. Pero como el sitio de donde proviene el ataque no es el mismo que el de la víctima; no se podrá realizar esta verificación y por ende, se rechazará la petición.

1.1.3 Comprobación de la cabecera HTTP Referer

También es posible prevenir vulnerabilidades de sitios cruzados comprobando la cabecera HTTP Referer. Cuando realizas una petición en una aplicación web el navegador emite una solicitud HTTP en la que se incluye una cabecera llamada ‘Referer’ que indica la URL que inició la petición.

Gracias a esta información, la cabecera puede saber si la segunda solicitud fue hecha desde el mismo sitio que la primera. Si el dominio no coincide entonces se evitará el ataque. Sin embargo, este mecanismo no suele usarse mucho; ya que la cabecera Referer muestra información sensible que afecta la privacidad de los usuarios como el contenido de la búsqueda hecha por el usuario.

2 Ataques XSS

El cross-site scripting (XSS) es un tipo de vulnerabilidad informática muy común en las aplicaciones web que permite a los atacantes colocar secuencias de comandos maliciosas en páginas web y, a su vez, instalan malware en los navegadores web de los usuarios.

Estos ataques no se limitan solamente a las páginas web disponibles en Internet, sino que también puede haber aplicaciones que tengas instaladas en tu ordenador que sean vulnerables a estos ataques de cross-site scripting (XSS).

2.1 Prevención

2.1.1 Por medio del cliente

Los navegadores trabajan proactivamente y liberan nuevas versiones frecuentemente para mantenerte a salvo. Por ejemplo:

- Google Chrome utiliza un filtro llamado XSSAuditor que analiza la solicitud HTTP y elimina funciones sospechosas de JavaScript.
- Mozilla Firefox utiliza un filtro XSS que modifica la carga útil mediante entidades HTML o codificaciones de URLs. Esto evita que se ejecute código malicioso en el navegador.
- Microsoft Internet Explorer utiliza un filtro que divide los datos enviados en dos categorías: confiables y no confiables con el objetivo de verificar la ejecución inmediata del código.

2.1.2 Utilizar frameworks seguros

Por diseño, automáticamente codifican el contenido para prevenir XSS, como en Ruby 3.0o React JS.

Codificar los datos de requerimientos HTTP

Los datos de requerimientos HTTP no confiables en los campos de salida HTML, deben ser codificados, (cuerpo, atributos, JavaScript, CSS, o URL) resuelve los XSS Reflejado y XSS Almacenado. La hoja de trucos OWASP para evitar XSS tiene detalles de las técnicas de codificación de datos requeridas.

2.2 Aplicar codificación sensitiva al contexto

Cuando se modifica el documento en el navegador del cliente, ayuda a prevenir XSS DOM. Cuando esta técnica no se puede aplicar, se pueden usar técnicas similares de codificación, como se explica en la hoja de trucos OWASP para evitar XSS DOM.

2.2.1 Habilitar una Política de Seguridad de Contenido (CSP)

Supone una defensa profunda para la mitigación de vulnerabilidades XSS, asumiendo que no hay otras vulnerabilidades que permitan colocar código malicioso vía inclusión de archivos locales, bibliotecas vulnerables en fuentes conocidas almacenadas en Redes de Distribución de Contenidos (CDN) o localmente.