

Centro de Operaciones de Ciberseguridad

#SiempreAlerta



REVISANDO TÉCNICAMENTE CADA UNO DE LOS RIESGOS PRESENTES EN LAS APLICACIONES WEB

A3 CROSS-SITE SCRIPTING - XSS

Autor: Christian Mendoza Bonzo.

Objetivo: Describirles a los desarrolladores y gerentes de proyectos en desarrollo en qué consisten las vulnerabilidades de CROSS-SITE SCRIPTING,

alternativas para detectarlas y los mecanismos de protección.

Fecha: Septiembre 26, 2016.



Continuando con la descripción de los riesgos en aplicaciones, ahora desarrollaremos la descripción de cada uno de los riesgos, cómo identificarlos y qué acciones podemos tomar.

Adicionalmente hemos optado por no traducir el nombre de esta vulnerabilidad del inglés al español, dado que la traducción en sí no refleja su equivalente.

A2- Cross-site scripting.-

Este tipo de fallas ocurren cuando datos no confiables son enviados al navegador sin una validación y codificación apropiada, lo que puede permitir a un atacante ejecutar una secuencia de comandos en el navegador de la víctima con lo cual éste podría secuestrar las sesiones de los usuarios, destruir sitios web o dirigirlos a sitios maliciosos.

Revisemos paso a paso cómo se puede manejar este tipo de am<mark>enazas</mark> antes que se transformen en un riesgo.

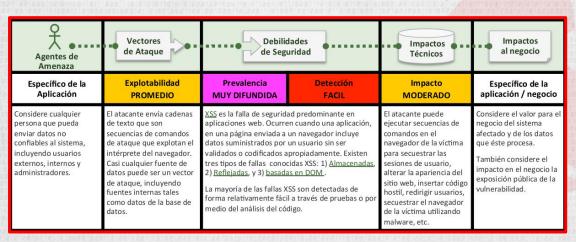


Fig 1. Cross-site Scripting. Copyright por: Owasp. Re-impreso con Permiso

¿Cómo conocer si soy vulnerable?

Existen varias formas de conocer si se es o no vulnerable, presentamos algunas opciones que le permitirán conocerlo:

- √ Se es vulnerable si no se asegura que todas las entradas de datos ingresadas por los usuarios estén codificadas adecuadamente.
- √ Si no se verifica en el momento de ingreso que los datos proporcionados sean seguros antes de ser incluidos en la página de salida.
- √ Si hay falta de manejo de controles o validaciones en los ingresos de datos.
- √ Por la utilización de un API insegura.

√ Si no hay una correcta configuración de los permisos de cada objeto en la aplicación web como: frames, imágenes, entre otros.

¿Cómo prevenirlo?

Para evitar pérdida de autenticación y gestión de sesiones se recomienda los siguientes ítems:

- La opción preferida es codificar los datos no confiables basados en el contexto HTML (cuerpo, atributo, javascript, css o url) donde serán ubicados.
- 2. Se recomienda la validación de entradas positivas o de listas blancas, aunque se debe de considerar que esto no es una defensa completa.
- 3. Tener un módulo exclusivo para validaciones, el mismo que debe de incluir al menos longitud del campo, tipo de caracteres, formatos y reglas del negocio que debe cumplir el dato antes de ser aceptado como entrada.
- 4. Efectuar revisiones de código programadas o cuando surga <mark>un cam</mark>bio.
- 5. Considere utilizar políticas de seguridad de contenido.
- Contar con mecanismos de protección como: IPS, controles de acceso (firewalls), multiples factores de autenticación y dispositivos especializados como WAF (Web Application Firewall).
- 7. Ejecutar pruebas estáticas y dinámicas sobre el software desarrollado.

Si desea conocer cómo podemos ayudarlo a proteger su información confidencial contáctenos a:

Email: info@secuinfor.com PBX: +593-4-3726620

Website: http://www.secuinfor.com