Universidad Autónoma de Chiapas
Facultad de contaduría y administración C-I

Carrera:
Lic. En ing en desarrollo y tecnologías de software.

Materia:
Análisis de vulnerabilidades.

Catedrático:
Mtro. Luis Gutiérrez Alfaro.

Nombre del alumno:
González Aguilar Eduardo - A211154

Semestre: 7. **Grupo:** M.

Nombre de la actividad:
Reporte de analisis.

Link de Github:
AguilarEduardo/AnalisisDeVulnerabilidades (github.com)

Fecha de entrega:
02/02/2024.

Conceptos básicos del XSS.

Introducción: El Cross-Site Scripting (XSS) es una vulnerabilidad de seguridad web que permite a los atacantes inyectar scripts maliciosos en páginas web visitadas por otros usuarios. Esta amenaza ha sido una preocupación constante en el panorama de seguridad cibernética, ya que puede dar lugar a robos de datos, ataques de phishing y comprometer la integridad de sitios web. En este informe, exploraremos los conceptos básicos del XSS.

Resumen: El cross-site scripting o XSS, también conocido como inyección de scripts entre sitios, es una vulnerabilidad de seguridad en aplicaciones web que permite a los atacantes ejecutar código malicioso en los navegadores de los usuarios aprovechando vulnerabilidades en las páginas web que estos visitan.Esta vulnerabilidad se aprovecha de la falta de validación y filtrado de datos de entrada por parte de las aplicaciones web, lo que permite que los atacantes inserten código JavaScript u otro código ejecutable en las webs visitadas por otros usuarios.El concepto detrás del XSS es que el atacante puede engañar a la aplicación web para que muestre contenido inseguro a los usuarios, haciéndoles creer que proviene de la página web legítima. Esto puede conducir a diversos tipos de ataques, como el robo de información confidencial, la suplantación de identidad o el secuestro de sesiones.

Resultados:

Tipos de XSS:

- **Almacenado:** Se inserta código malicioso en la base de datos y se presenta a los usuarios cuando solicitan la página.
- **Reflejado:** El código malicioso se inyecta en la URL y se refleja en la página web, afectando a los usuarios que acceden a esa URL.
- **Basado en DOM:** La manipulación del DOM permite la ejecución de scripts en el navegador del usuario.

Impacto del XSS:

- Robo de cookies y sesiones.
- Suplantación de identidad.
- Redirección a sitios maliciosos.
- Modificación de contenido web.

Prevención del XSS:

- Validación y escape de datos de entrada.
- Implementación de encabezados de seguridad HTTP, como Content Security Policy (CSP).
- Educación y concientización de los desarrolladores.

Bibliografia:

Maria Acibeiro, (31 de Junio del 2023), *"´¿Qué es el cross-site scripting (XSS) y como puedes puedes evitarlo?",* Go daddy. ¿Qué es el cross-site scripting (XSS) y cómo puedes evitarlo? - Blog (godaddy.com)

Esther Lugo Rojas, Cesar Alejandro Varela Cruz, (12 de diciembre del 2022), *"Cross-site scripting (XSS)",* Seguridad Unam. Cross-site scripting (XSS) | UNAM-CERT