Trabajo Biblioteca

Presentado por:

Yordy Erik Nuñez Pineda.

Presentado a:

Carlos Julio Cadena.

Centro de la Industria, la Empresa y los Servicios.

Ficha: 2694667 – Fecha: 30/06/2024

Neiva – Huila

¿Qué es injection HTML?

La inyección de HTML es una vulnerabilidad de seguridad que ocurre cuando una aplicación web permite que se inserte código HTML malicioso en su contenido. Esto puede ocurrir, por ejemplo, cuando un usuario puede introducir datos que se muestran en la página sin ser correctamente sanitizados. La inyección de HTML puede llevar a varios problemas de seguridad, como el Cross-Site Scripting (XSS), que permite a los atacantes ejecutar scripts maliciosos en el navegador de otros usuarios.

¿Qué es injection SQL?

La inyección de SQL (SQL Injection) es una técnica de ataque que explota vulnerabilidades en una aplicación para ejecutar comandos SQL no autorizados a través de una entrada de usuario maliciosamente modificada. Esta vulnerabilidad ocurre cuando la aplicación no valida o sanitiza adecuadamente la entrada del usuario, lo que permite al atacante alterar la consulta SQL ejecutada en la base de datos.