Cross-Site Request Forgery CSRF

La vulnerabilidad CSRF (Cross-Site Request Forgery) es un tipo de ataque que se produce cuando un usuario autenticado involuntariamente envía una solicitud malintencionada a un sitio web. Este ataque aprovecha la confianza del sitio web en la sesión activa del usuario para enviar una solicitud no autorizada, que puede provocar cambios no deseados en el estado de la cuenta del usuario, como transferencias de dinero, cambios de contraseña, eliminación de datos, entre otros.

Solución

Implementar tokens de seguridad CSRF en formularios HTML que se verifican en el servidor para garantizar que la solicitud sea legítima y no se haya falsificado.

Para conocer más a cerca de la vulnerabilidad y formas de mitigación consultar Cross-Site Request Forgery Prevention Cheat Sheet CSRF

Revision #2
Created 15 mayo 2023 12:16:21 by Vladimir Urquiola
Updated 24 mayo 2023 17:49:53 by Vladimir Urquiola