

¿Qué es OWASP?

OWASP significa Open Web Application Security Project. Es una organización sin ánimo de lucro, a nivel mundial, dedicada a mejorar la seguridad del software. Su objetivo es proporcionar recursos gratuitos y abiertos (documentación, guías, herramientas, metodologías, laboratorios, etc.) que ayuden a desarrolladores, empresas y universidades a construir aplicaciones más seguras.

En otras palabras, OWASP es como una comunidad global que comparte buenas prácticas, estándares y proyectos de seguridad para que el software que construimos sea menos vulnerable a ataques.

Control de acceso roto

Los sistemas de control de acceso están destinados a garantizar que solo los usuarios legítimos tengan acceso a los datos o a la funcionalidad. La vulnerabilidad en la categoría de control de acceso roto incluye cualquier problema que permita a un atacante eludir los controles de acceso o que no implemente el principio de privilegio mínimo. Por ejemplo, una aplicación web podría permitir a un usuario acceder a la cuenta de otro usuario modificando la URL proporcionada.

Fallas criptográficas

Los algoritmos criptográficos son invaluable para proteger la privacidad y la seguridad de los datos; sin embargo, estos algoritmos pueden ser muy sensibles a errores de implementación o configuración. Las fallas criptográficas incluyen la imposibilidad de utilizar el cifrado, configuraciones incorrectas de los algoritmos criptográficos y una gestión de claves insegura. Por ejemplo, una organización podría usar un algoritmo hash inseguro para el almacenamiento de contraseñas, no usar las contraseñas o usar la misma sal para todas las contraseñas de usuario almacenadas.

Uso de bcryptjs

bcryptjs es una librería de JavaScript puro que implementa el algoritmo de hashing bcrypt, el cual se usa para proteger contraseñas antes de almacenarlas en una base de datos.