Buenas prácticas de seguridad en desarrollo

La guía que necesitas para crear software seguro

PABLO DEL ÁLAMO

Introducción

¡En un mundo donde las amenazas cibernéticas son inevitables, asegurarnos de que nuestras aplicaciones estén blindadas es esencial para proteger tanto nuestros sistemas como a nuestros usuarios.

La meta de este carrusel es guiarte a través de las mejores prácticas de seguridad en el desarrollo.

Descubrirás técnicas efectivas para crear software que no solo funcione bien, sino que sea seguro.

PABLO DEL ÁLAMO

La importancia de la seguridad

La seguridad no es un lujo, es una necesidad.

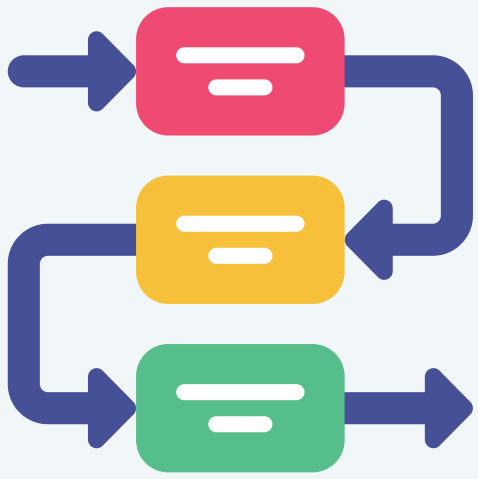
> Con cada línea de código que escribimos, debemos pensar en los posibles riesgos de seguridad. ¡Es como ponerle cinturones de seguridad a tu aplicación!

PABLO DEL ÁLAMO

Mantén tus dependencias al día

Actualiza las librerías y frameworks que utilizas.

Las vulnerabilidades conocidas suelen ser corregidas en versiones más recientes. 🔄



PABLO DEL ÁLAMO

Validación de entradas

Nunca confíes en el input del usuario.

Utiliza siempre validaciones para comprobar que los datos son lo que esperas.

Esto evita inyecciones de código y otros ataques.

PABLO DEL ÁLAMO

Autenticación robusta

Implementa sistemas de autenticación fuertes. Contraseñas robustas y, si es posible, autenticación de dos factores (2FA). 🔑🔒

PABLO DEL ÁLAMO

Gestión de sesiones

Asegúrate de que las sesiones de usuario caducan después de un período de inactividad.

No olvides invalidar las sesiones en el logout. ⏰

PABLO DEL ÁLAMO

Uso de HTTPS

Cualquier aplicación que maneje datos personales debe utilizar HTTPS.

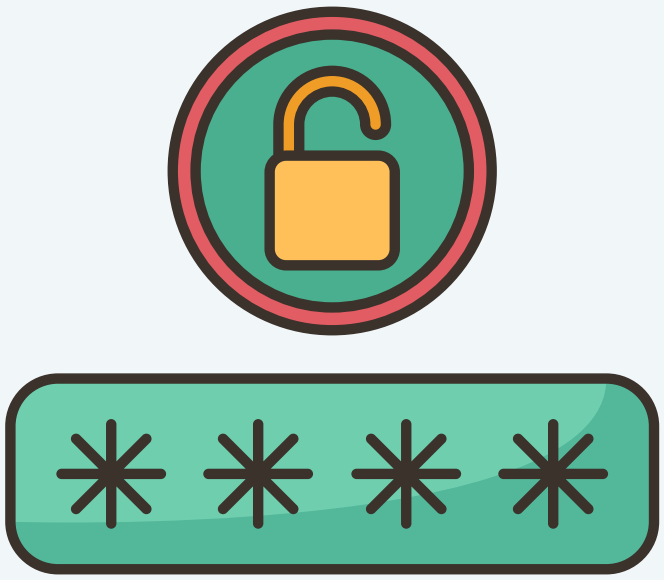
¡Cifra esos datos en tránsito! 🌐🔐

PABLO DEL ÁLAMO

Almacenamiento seguro de contraseñas

NUNCA almacenes contraseñas en texto plano.

Usa algoritmos de hashing como bcrypt para protegerlas adecuadamente. 🗃️🔒



PABLO DEL ÁLAMO

Control de acceso

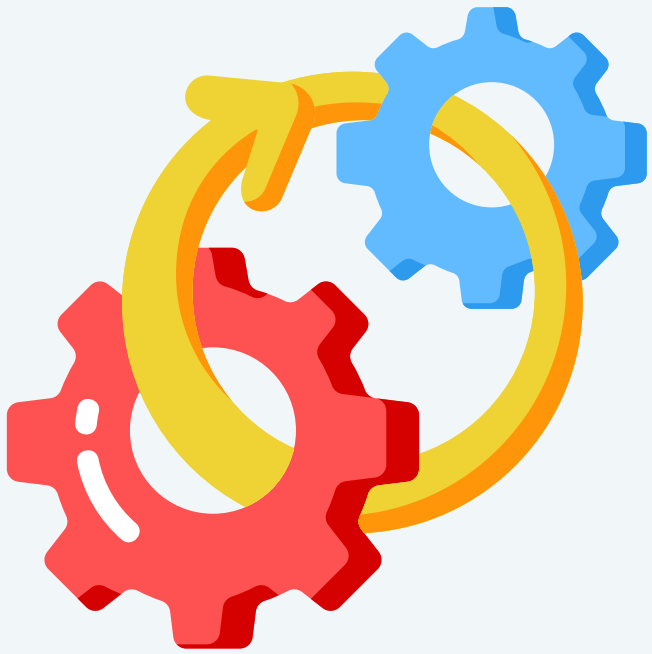
Implementa un modelo de control de acceso sólido.

Define roles y asigna permisos de forma adecuada para que solo los usuarios autorizados accedan a recursos sensibles. 🛡️

PABLO DEL ÁLAMO

Escaneo de seguridad automatizado

Integra herramientas de escaneo de seguridad en tu pipeline de CI/CD para detectar vulnerabilidades de forma automática. 🛠️

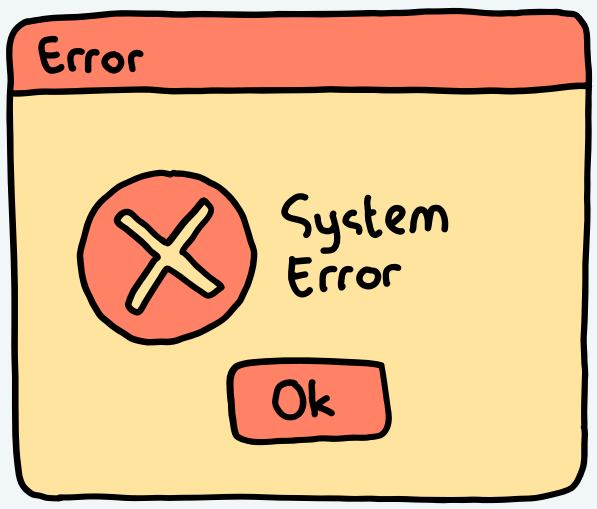


PABLO DEL ÁLAMO

Evita exposición de errores

No muestres mensajes de error detallados a los usuarios.

Podrían dar pistas a posibles atacantes sobre la estructura interna de tu sistema.

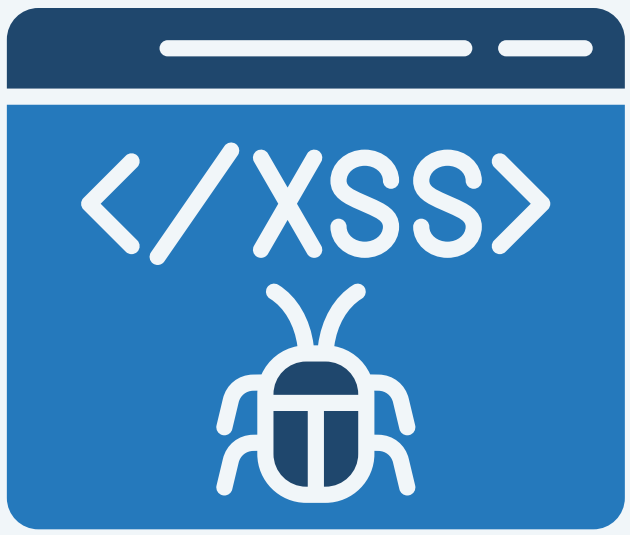


PABLO DEL ÁLAMO

Evita ataques XSS

Protege tu app de Cross Site Scripting (XSS).

Nunca confíes en el input y utiliza técnicas de sanitización y escape de caracteres. 🧼



PABLO DEL ÁLAMO

Inyección SQL y otras inyecciones

Usa consultas preparadas o stored procedures para prevenir ataques de inyección SQL.

No pongas los datos del usuario directamente en las consultas SQL.

PABLO DEL ÁLAMO

Logging y Monitorización

Implementa logging y monitorización para detectar actividades sospechosas y abordar incidentes de manera rápida. 📊🔍

PABLO DEL ÁLAMO

Mínimos privilegios

Sigue el principio del mínimo privilegio.

Da acceso sólo a los recursos y permisos que se necesitan. 🌿

PABLO DEL ÁLAMO

Educación continua

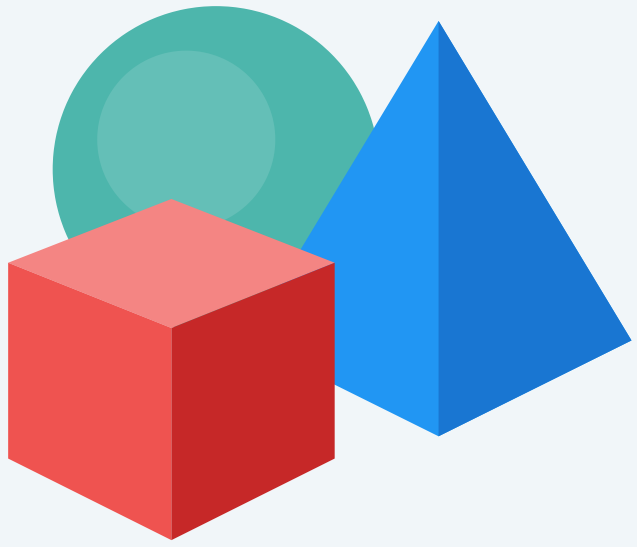
Mantente al día con las nuevas amenazas y técnicas de defensa.

Nunca dejes de aprender sobre ciberseguridad. 📚

PABLO DEL ÁLAMO

Cuidado con la serialización y deserialización

Controla qué objetos se serializan y deserializan para evitar ataques de deserialización maliciosa.



PABLO DEL ÁLAMO

Protección ante CSRF

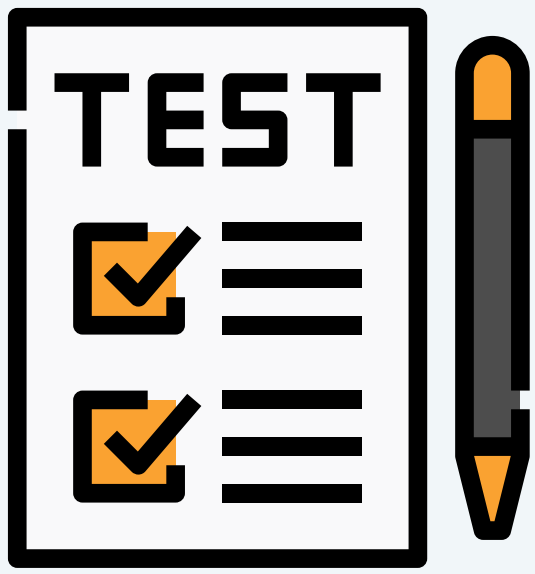
Usa tokens CSRF para proteger a tu app de ataques de Cross-Site Request Forgery.

PABLO DEL ÁLAMO

Testing de seguridad

Incorpora el testing de seguridad en tu ciclo de desarrollo.

¡Las pruebas penetración pueden descubrirte sorpresas! 🔍



PABLO DEL ÁLAMO

¿Te ha resultado útil?

- Comparte esta guía con tu equipo o amigos desarrolladores.
- Guárdala para tenerla siempre a mano.
- ¡Dale un like o comenta si tienes preguntas!

PABLO DEL ÁLAMO