Desarrollo Seguro de API

Las API son un componente esencial de la arquitectura basada en microservicios y microservicios y una buena práctica permite una rápida evolución de las aplicaciones y simplifica su gestión. En esta presentación hablaremos de cómo cómo desarrollar API seguras para proteger los datos críticos de la empresa. empresa.

¿Qué es una API?

Tecnología

Interfaz que permite la comunicación entre diferentes diferentes componentes de de una aplicación.

Ventajas

Agilidad y flexibilidad en el desarrollo. Facilita la integración de herramientas de herramientas de terceros.

Importancia

Base tecnológica de servicios como PayPal, Uber, Amazon Web Services, entre otros.

¿Por qué desarrollar API seguras?

Integridad

Los datos no deben modificarse en tránsito sin consentimiento.

1

Confidencialidad

Los datos transmitidos deben ser conocidos solo por la parte a la que van destinados.

2

3

Disponibilidad

Las aplicaciones deben estar disponibles para los usuarios autorizados en todo momento.

Vulnerabilidades comunes en las API

Autorización Insegura

Autenticación inadecuada o falta de verificación de permisos pueden comprometer la seguridad de la API.

Injection Attacks

Atacantes pueden enviar comandos maliciosos a través de los parámetros de la API para ganar acceso no autorizado a la aplicación.

Bugs de seguridad

Los errores en el código pueden exponer a la aplicación a ataques fuera del plan.

Técnicas de defensa

Limitar accesos

Establecer controles de acceso y limitar las permisiones concedidas para limitar el daño en caso de ataque.

1

Autenticación y Autorización

Implementar métodos de autenticación y asegurarse que la autorización sea previa a la entrega de información.

2

3

Encriptación

Proteger lo datos en tránsito y en reposo y asegurarse que solo sean entregados al destinatario deseado.

Ejemplos de ataques a API

HTTP Parameter Pollution

Adulteración de parámetros para confundir y romper el programa.

Man in the Middle

Intercepta datos de la comunicación para su uso ilegal.

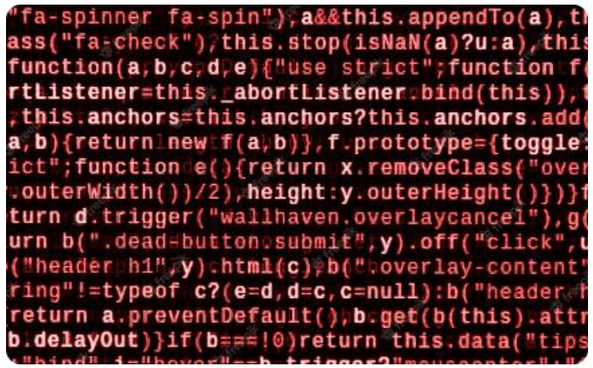
Cross-Site Scripting

Aprovechamiento de vulnerabilidades en la aplicación para ejecutar código.

Cómo realizar pruebas de seguridad en una API

Penetration Testing

Técnica de prueba de seguridad que busca explotar vulnerabilidades para evaluar la efectividad del sistema de seguridad.



Análisis Estático

Método que busca vulnerabilidades en el código fuente, antes de la etapa de testing.

Pruebas de la API

Pruebas realizadas específicamente a la interacción con la API.

Recomendaciones finales para el desarrollo seguro de API

1

Seguir Estándares

Seguir buenas practicas de seguridad como OAuth2 y OpenID Connect.

2

Actualizar el Software

Importante mantener el software actualizado para eliminar vulnerabilidades conocidas.

3

Trazar todo

Guardar registros de todas las interacciones en la aplicación para auditorías futuras.

Apoya tu proceso de remediaciones con:

ALINA

ALINA es un innovador chatbot impulsado por Inteligencia Artificial que te ayudará a resolver las remediaciones propuestas en este informe.

https://grupooruss.com/alina

¡Gracias!

www.grupooruss.com