Protocolos de seguridad con pentesting y criptografía

Nombre: Angel Orlando Zambrano Uriña

Nao ID: 3117

Fecha: 30/08/2024

Nombre de la trayectoria: Consultor de Cyberseguridad

Título del reto: Protocolos de seguridad con pentesting y criptografía

Tablas de Registros

Lista de Requerimientos	
Historias de Usuarios	**Requerimientos**
Como desarrollador quiero que las pruebas de seguridad se integren en cada fase del desarrollo (Shift Left Security) para que las vulnerabilidades se detecten y corrijan temprano.	Integrar pruebas de seguridad automatizadas en cada fase del desarrollo.
Como administrador de sistema quiero tener la capacidad de gestionar los permisos de acceso de los usuarios para que solo personal autorizado pueda acceder a datos sensibles.	Proporcionar funcionalidad para gestionar permisos de acceso.
Como administrador de plataforma quiero un monitoreo continuo de los eventos de seguridad para que se puedan detectar y responder a incidentes en tiempo real.	Implementar monitoreo continuo de eventos de seguridad.
Como auditor de seguridad quiero poder acceder a informes detallados de vulnerabilidades y pruebas de seguridad para que pueda evaluar el cumplimiento de las políticas de seguridad.	Generar informes detallados de vulnerabilidades y pruebas de seguridad.
Como inversor potencial quiero asegurarme de que la plataforma cumpla con los estándares y regulaciones de seguridad para que pueda confiar en la seguridad de mi inversión.	Asegurar el cumplimiento de estándares y regulaciones de seguridad.
Como usuario final quiero que mi información personal y de pago esté cifrada para que esté protegida contra accesos no autorizados.	Implementar cifrado para información personal y de pago en tránsito y en reposo.

Lista priorizada			
Requerimientos	**Etapas**	**Estimación de Tiempo**	**Entregables**
Integrar pruebas de seguridad automatizadas en cada fase del desarrollo.	Sprint 1 (Fase de pruebas)	1 semana	Pipeline de CI/CD con pruebas de seguridad e informes de pruebas de seguridad.
Proporcionar funcionalidad para gestionar permisos de acceso.	Sprint 1 (Fase de implementación)	1 semana	Sistema de gestión de accesos y documentación de permisos.
Implementar monitoreo continuo de eventos de seguridad.	Sprint 1 (Fase de monitoreo)	1 semana	Sistema de monitoreo de seguridad, alertas configuradas, y panel de control de seguridad.
Generar informes detallados de vulnerabilidades y pruebas de seguridad.	Sprint 1 (Fase de informes detallados)	1 semana	Informes de vulnerabilidades e informes de cumplimiento de seguridad.
Asegurar el cumplimiento de estándares y regulaciones de seguridad.	Sprint 1 (Fase de cumplimiento y regulaciones)	1 semana	Documentación de cumplimiento y certificación de seguridad.
Implementar cifrado para información personal y de pago en tránsito y en reposo.	Sprint 1 (Fase de implementación)	1 semana	Sistema de cifrado implementado e informe de validación de cifrado.