Evaluación Técnica Parte #1 - Consultor Senior de Seguridad de Aplicaciones

Consultor:

Erazo Mendoza Jeremy Sebastián

Offensive Security and Exploit Development Engineer

Quito, Junio del 2025

Contenido

Programa de capacitación para equipos de desarrollo.

Objetivo del Programa de Capacitación

Desarrollar competencias avanzadas en los equipos de desarrollo para que comprendan y apliquen principios de seguridad desde una perspectiva ofensiva y defensiva, especialmente enfocados en arquitecturas distribuidas como APIs REST y aplicaciones móviles, fortaleciendo su capacidad para diseñar y mantener sistemas con defensa en profundidad, gestión efectiva de riesgos y controles compensatorios, asegurando la resiliencia ante amenazas reales en el contexto fintech.

Plan Completo de Capacitación para Equipos de Desarrollo

Fase 1 – Diagnóstico y Fundamentos Técnicos (Semanas 1-3)

- Evaluación inicial del conocimiento de seguridad con pruebas técnicas y análisis de código.
- Formación en fundamentos avanzados de seguridad en aplicaciones: modelo de amenaza aplicado a fintech, autenticación y autorización robusta, criptografía aplicada (tokens, cifrado de datos en tránsito y reposo).
- Taller práctico: análisis y explotación de vulnerabilidades OWASP Top 10 contextualizadas a APIs y móviles, usando herramientas de pentesting básicas (Burp, Postman con tests de seguridad).
- Introducción al concepto de defensa en profundidad: múltiples capas y su importancia en la arquitectura.

Fase 2 – Arquitectura Segura y Controles Compensatorios (Semanas 4-6)

- Profundización en diseño seguro de arquitecturas distribuidas: segmentación de servicios, aislamiento de datos, controles de frontera y lógica.
- Definición y aplicación de controles compensatorios en el contexto fintech: rate limiting, validación estricta, control de sesión, logging seguro y análisis de anomalías.
- Taller de modelado de amenazas para casos específicos (autenticación, transferencia de fondos, manejo de errores).
- Introducción a la instrumentación y monitoreo de seguridad en APIs y apps (WAF, API Gateway, IDS/IPS).

Fase 3 – Integración DevSecOps y Automatización de Seguridad (Semanas 7-10)

- Capacitación avanzada en CI/CD seguro: integración y configuración avanzada de SAST, DAST, SCA y SBOM.
- Gestión avanzada de secretos y credenciales: uso de vaults, identidad basada en roles, rotación automática y auditoría.
- Taller: configuración y análisis de pipelines con énfasis en seguridad y reacción ante findings críticos.
- Simulación de incidentes de seguridad y respuesta inmediata: análisis y remediación rápida de findings.

Fase 4 – Cultura de Seguridad y Mentalidad Ofensiva (Semanas 11-12)

- Introducción a técnicas y tácticas ofensivas desde la perspectiva de Red Team (phishing, ingeniería social, explotación de APIs, ataques en móviles).
- Ejercicios prácticos tipo “capture the flag” (CTF) enfocados en vulnerabilidades reales de fintech.
- Taller de revisión crítica y aprendizaje sobre incidentes pasados de la organización y casos de estudio externos.
- Creación de un canal continuo de comunicación entre desarrollo y seguridad para compartir hallazgos y mejoras.

Explicación del Sentido y Valor de Cada Fase

- **Fase 1:** Se parte de un diagnóstico riguroso para identificar brechas reales en conocimiento y prácticas. El énfasis en fundamentos avanzados es clave para romper la falsa percepción de “seguridad superficial” y preparar al equipo para pensar como un atacante que aprovecha vulnerabilidades comunes en fintech.
- **Fase 2:** Aquí se traduce el conocimiento en diseño y aplicación práctica, enfatizando que la seguridad no es un único control, sino una combinación de barreras técnicas adaptadas a los riesgos del negocio. Los controles compensatorios se estudian para mitigar fallos inevitables o restricciones tecnológicas.
- **Fase 3:** Se fortalece la cultura DevSecOps con automatización real y análisis continuo, elevando el nivel de seguridad sin sacrificar agilidad. La integración con pipelines no es solo un requisito, es una práctica que reduce la ventana de exposición y mejora la trazabilidad de riesgos.
- **Fase 4:** La última fase busca generar empatía con la mentalidad atacante, mejorando la capacidad del equipo para anticipar, detectar y responder. Esto fortalece la cultura y motiva una colaboración real entre desarrollo y seguridad, fundamental para un modelo sostenible.