Informe de Auditoría Ética – SecureBank S.A.

Fecha: 9 de junio de 2025
Equipo responsable: CyberGuard Consultores
Analista líder: Bastián Landskron
Versión: v1.0

---

1. Resumen Ejecutivo

Entre el 2 y el 6 de junio de 2025 se realizó una auditoría de hacking ético a la plataforma de banca en línea de SecureBank S.A. en su entorno de staging, con autorización formal del CTO. Se aplicó la guía OWASP Testing Guide y referencias de NIST SP 800-115, siguiendo fases de reconocimiento, análisis, explotación controlada y reporte. Se identificaron tres vulnerabilidades críticas (inyección SQL en el login, acceso abierto al panel administrativo y XSS persistente), por lo que se recomienda su mitigación inmediata y la adopción de un programa continuo de seguridad ofensiva-defensiva .

2. Alcance y Limitaciones

- **Alcance:**
    - **Aplicación web de banca en línea (entorno de staging).**
    - **Módulos auditados: formulario de autenticación, panel de administración, formulario de contacto.**
- **Limitaciones:**
    - **No se incluyeron pruebas de Denegación de Servicio (DoS).**
    - **No se accedió a datos reales de clientes ni a sistemas de producción.**
- **Autorización: Carta de aprobación firmada por el CTO de SecureBank S.A.**

3. Metodología

- **Fases aplicadas:**
    - **Reconocimiento: mapeo de rutas y tecnologías (Nmap, inspección manual).**
    - **Análisis de vulnerabilidades: escaneos con Burp Suite y OWASP ZAP.**
    - **Explotación controlada: uso de sqlmap y scripts personalizados para validar hallazgos.**
    - **Reporte: documentación técnica y recomendaciones.**
- **Estándares de referencia:**
    - **OWASP Testing Guide v5.1**
    - **NIST SP 800-115 Technical Guide to Information Security Testing and Assessment**

Blandskron

4. Hallazgos Técnicos

Vulnerabilidad	Descripción	Impacto	Riesgo	Evidencia	Recomendación
1. Inyección SQL en login	El parámetro `username` no filtra caracteres maliciosos, permitiendo consultas OR-based (`' OR '1'='1`) y bypass de autenticación.	Acceso no autorizado a cuentas	Alto	Captura Burp (“admin' OR '1'='1”)	Usar consultas preparadas (Prepared Statements) y validación de entrada en backend.
2. Panel de administración expuesto	La ruta `/admin` no exige autenticación en staging, otorgando control completo sobre la aplicación web.	Control total del sitio	Alto	Petición HTTP 200 en `/admin` sin token	Implementar middleware de autenticación y control de roles.
3. XSS persistente en formulario	El campo `nombre` del formulario de contacto almacena scripts (`<script>alert(1)</script>`) que luego se ejecutan en vista de administrador.	Robo de sesión, phishing interno	Medio	Pantalla con alerta JS tras guardar	Escapar y sanitizar todas las entradas antes de renderizar.

5. Recomendaciones Generales

- **Establecer un programa de gestión continua de parches, priorizando vulnerabilidades de alto impacto.**
- **Desplegar un WAF (Web Application Firewall) con reglas OWASP CRS para filtrar inyección y XSS.**
- **Forzar uso de HTTPS en todos los endpoints y deshabilitar HTTP.**
- **Revisar y reforzar políticas de contraseñas y mecanismos de bloqueo tras intentos fallidos.**
- **Implementar auditorías periódicas (mínimo trimestrales) y revisiones de código automatizadas en CI/CD.**

6. Consideraciones Éticas y Legales

- **Todas las pruebas se realizaron bajo autorización formal, en un entorno de staging, sin afectar datos reales ni servicios en producción.**
- **Se mantuvo confidencialidad de hallazgos y respetaron los códigos de ética de EC-Council y SANS.**
- **No se explotaron vulnerabilidades más allá de la verificación controlada; no se extrajeron datos sensibles.**

7. Conclusión

La plataforma de SecureBank S.A. presenta vulnerabilidades críticas que requieren atención inmediata. La inyección SQL y el acceso abierto al panel administrativo suponen un riesgo de compromiso total, mientras que el XSS persistente facilita ataques de phishing interno y robo de sesiones. Se recomienda abordar estos hallazgos en orden de prioridad (primero SQL y autenticación, luego XSS) e instaurar un ciclo de pruebas y mejoras continuas para robustecer la seguridad defensiva y ofensiva de la infraestructura.

8. Anexos

- **A. Capturas de pantalla (Burp Suite, consola de navegador).**
- **B. Trazas de Burp Suite (exportación XML).**
- **C. Scripts de prueba SQL y comandos de sqlmap.**
- **D. Lista de herramientas y versiones utilizadas.**