Matriz de Amenazas, Controles y Pruebas - API Notas Privadas Seguras

|  |  |  |
| --- | --- | --- |
| Amenaza | Control Implementado | Prueba de Validación |
| 1. Ataques de Fuerza Bruta | - Lockout después de 5 intentos fallidos por 15 minutos - Contraseñas con requisitos mínimos (10 chars, mayúsculas, minúsculas, números) | - Script de prueba con 6 intentos fallidos - Verificar bloqueo temporal - Intentar login después de 15 minutos |
| 2. Intercepción de Credenciales | - Contraseñas hasheadas con BCrypt (cost 12) - Cookies HttpOnly y SameSite - HTTPS obligatorio en producción | - Verificar hash en base de datos - Inspeccionar cookies en DevTools - Validar cabeceras HTTPS |
| 3. Cross-Site Scripting (XSS) | - Content Security Policy (CSP) - Validación de entrada con Jakarta Bean - Headers de seguridad (X-Content-Type-Options) | - Intentar inyectar scripts en notas - Verificar CSP en respuestas - Validar escape de caracteres |
| 4. CSRF | - Tokens CSRF - SameSite Cookies - Validación de origen | - Intentar requests sin token - Verificar cookie SameSite - Probar peticiones cross-origin |
| 5. Acceso No Autorizado | - JWT con tiempo corto de expiración - Validación de roles - Control de propiedad de recursos | - Intentar acceder sin token - Probar acceso a rutas admin - Intentar ver notas ajenas |
| 6. Session Hijacking | - Tokens JWT cortos - Sistema de refresh token - Revocación de tokens | - Verificar expiración de tokens - Probar refresh token - Validar revocación |
| 7. Inyección SQL | - JPA/Hibernate con consultas parametrizadas - Validación de entrada - Principio de menor privilegio | - Intentar inyección en búsquedas - Validar escape de caracteres - Verificar consultas preparadas |
| 8. Escalamiento de Privilegios | - Validación estricta de roles - Verificación de propiedad - Principio de menor privilegio | - Intentar modificar rol - Probar acceso admin como user - Verificar aislamiento de recursos |
| 9. Information Disclosure | - Headers de seguridad - HSTS - Manejo de errores controlado | - Verificar headers de respuesta - Probar HTTPS forzado - Validar mensajes de error |
| 10. DoS/DDoS | - Rate limiting - Timeouts configurados - Recursos máximos definidos | - Pruebas de carga - Verificar límites de rate - Validar timeouts |

Controles Transversales

1. Logging y Monitoreo

* Registro de intentos fallidos
* Auditoría de acciones críticas
* Alertas de seguridad

2. Gestión de Dependencias

* Actualizaciones regulares
* Escaneo de vulnerabilidades
* Versionado seguro

3. Configuración Segura

* Entornos separados
* Variables de entorno
* Hardening de servidor