Gestión de Incidentes conforme a ISO 27001

Informe – Vulnerabilidad de Inyección SQL

Estado: Cerrado con acciones correctivas definidas

1. Resumen ejecutivo

Durante el período auditado se confirmó un incidente de seguridad de la información que afectó a un sistema productivo expuesto a Internet. El incidente consistió en una inyección SQL que permitió el acceso no autorizado a credenciales almacenadas en la base de datos de la aplicación.

El ataque fue posible debido a deficiencias en el diseño seguro de la aplicación, ausencia de validación de entradas y falta de controles de detección temprana. El incidente fue detectado mediante monitoreo de seguridad y análisis de logs, tras observar comportamientos anómalos en el proceso de autenticación.

2. Descripción detallada del incidente

El día 09/01/2026, un actor no autenticado interactuó con el campo “User ID” de la aplicación web corporativa. Mediante la manipulación del campo de entrada el atacante logró alterar la lógica de la consulta SQL ejecutada por el backend.

Se utilizó la siguiente carga útil SQL en el campo “User ID”:

1' AND '1'='2

Como resultado, el sistema retornó información correspondiente a múltiples registros de usuarios, permitiendo el acceso a credenciales almacenadas en la base de datos.

El incidente afectó directamente el principio de confidencialidad, al exponer información sensible a un sujeto no autorizado.

3. Alcance y activos afectados

Activo principal: Aplicación web de autenticación

Activo secundario: Base de datos de usuarios

Tipo de información comprometida: Credenciales

Usuarios potencialmente afectados: Usuarios registrados en la plataforma

Entorno: Producción

4. Detección del incidente

La detección del incidente no fue inmediata y se produjo a través de una combinación de controles técnicos y revisión humana, lo que evidencia debilidades en la capacidad de detección temprana.

4.1. Mecanismos de detección involucrados

- Análisis de logs de aplicación
    - Se identificaron múltiples intentos de autenticación exitosos desde una misma dirección IP sin correspondencia con credenciales válidas conocidas.
    - Se observaron patrones atípicos en los parámetros enviados al backend.

- Alertas del sistema de monitoreo
    - El SIEM generó una alerta de severidad media por accesos consecutivos a cuentas diferentes en un corto período de tiempo

- Revisión manual
    - El equipo de operaciones detectó inconsistencias entre los registros de autenticación y los accesos reales de usuarios legítimos.
    - Se inició una investigación al correlacionar eventos del servidor web y de la base de datos.

4.2 Tiempo de detección

Tiempo hasta detección: Aproximadamente 4 horas

Clasificación: Detección tardía

5. Análisis de causa raíz

La causa raíz del incidente no fue el ataque en sí, sino una cadena de fallos organizacionales, técnicos y de proceso.

5.1 Causas técnicas

- Uso de consultas SQL dinámicas construidas mediante concatenación directa de entradas del usuario.
- Ausencia de consultas parametrizadas.
- Falta de validación de entradas del lado del servidor.

- Almacenamiento de credenciales accesible por una cuenta de base de datos con permisos excesivos.

5.2 Causas de proceso

- Inexistencia de revisiones de seguridad en el ciclo de desarrollo (SSDLC).
- Falta de pruebas de seguridad (SAST / DAST) previas al despliegue.
- Ausencia de un checklist de controles mínimos antes de pasar a producción.

5.3 Causas organizacionales

- Falta de concientización en desarrollo seguro.
- Seguridad tratada como un requisito posterior y no como un componente del diseño.
- Roles y responsabilidades de seguridad no formalizados.

Conclusión de causa raíz:

El incidente fue consecuencia directa de una deficiente gobernanza de seguridad de aplicaciones, alineada de forma insuficiente con los controles exigidos por ISO/IEC 27001.

6. Impacto

6.1 Impacto en la seguridad de la información

- Confidencialidad: Comprometida
- Integridad: No evidenciada como afectada
- Disponibilidad: No afectada

6.2 Impacto organizacional

- Riesgo de acceso no autorizado a cuentas de usuario.
- Potencial incumplimiento de normativas de protección de datos.
- Daño reputacional en caso de divulgación.

7. Respuesta al incidente

Las acciones ejecutadas fueron:

1. Aislamiento temporal del sistema afectado.
2. Revocación de credenciales comprometidas.
3. Análisis forense de logs de aplicación y base de datos.
4. Corrección inmediata del código vulnerable.
5. Notificación interna al responsable de seguridad de la información.

8. Acciones correctivas

- Implementación obligatoria de consultas parametrizadas.
- Aplicación del principio de mínimos privilegios en base de datos.
- Integración de controles de seguridad en el ciclo de desarrollo.
- Activación de reglas específicas en WAF para detección de inyección.
- Mejora del monitoreo y correlación de eventos en el SIEM.
- Capacitación técnica al equipo de desarrollo.

9. Conclusión del auditor

El incidente demuestra una madurez insuficiente en la gestión de la seguridad de aplicaciones, incompatible con los requisitos esperados de un sistema en producción bajo ISO/IEC 27001.

Si bien la respuesta permitió contener el incidente, la detección tardía y la causa raíz evidencian la necesidad de mejoras estructurales y no solo técnicas.