REPORTE INCIDENTE VULNERACION SQL INJECTION

ISO 27001 - SQL Injection Vulnerability

Introducción

Descripción del incidente: 12/12/2024

El 12 de diciembre del presente año, se detecto un acceso no autorizado al servidor donde se almacenan archivos sensibles de la empresa. El incidente fue identificado a través de los registros del sistema de monitoreo de acceso, que indicaron que una cuenta de usuario, con privilegios de administrador, accedió a datos que no estaban dentro de su nivel de autorización.

Descripción del incidente

Durante la evaluación de seguridad de DVWA, se descubrió una vulnerabilidad de inyección SQL en el módulo "SQL Injection". Esta vulnerabilidad permite a un atacante inyectar consultas SQL maliciosas a través de los campos de entrada de la aplicación web, comprometiendo así la integridad y confidencialidad de los datos almacenados en la base de datos.SQL Injection

Para replicar y demostrar la vulnerabilidad, se utilizó la siguiente carga útil SQL en el campo "ID de usuario":

```
1' OR '1' = '1
```

Acción tomada

Desconexión inmediata de las estaciones de trabajo afectadas.

Análisis forense realizado en los sistemas afectados.

Limpieza y restauración de sistemas desde respaldos seguros.

Causa Raíz

Falta de actualizaciones de seguridad en las estaciones de trabajo.

Reglas de filtrado de tráfico de red insuficientes.

RECOMENDACIONES

Políticas de **seguridad en el correo electrónico** reforzadas con filtros anti-phishing.

Se planeó un curso de actualización en ciberseguridad para todos los empleados.

Estado del incidente: Cerrado. Medidas correctivas implementadas con éxito.

Conclusiones

La organización debe priorizar la adopción de **tecnologías de seguridad robustas** y **procedimientos de gestión de acceso** estrictos para garantizar la protección de la información confidencial y la continuidad operativa.