ISO 27001 REPORTE DE VULNERABILIDAD DE INYECCIÓN SQL

INTRODUCCIÓN: Es un reporte detallado de identificación de explotación y vulnerabilidad de inyección sql.

DESCRIPCIÓN DEL INCIDENTE:

Durante la evaluación de seguridad de DVWA, se descubrió una vulnerabilidad de inyección SQL

Método de inyección SQL utilizado:

Para replicar y demostrar la vulnerabilidad, se utilizó la siguiente carga útil SQL en el campo "ID de usuario":
sql
' UNION SELECT username, password FROM users WHERE id = 1 #

Impacto del incidente:

La explotación de esta vulnerabilidad podría permitir a un atacante:

● Acceder y extraer información confidencial de la base de datos, incluidas las credenciales de usuario.
● Modificar, eliminar o comprometer datos confidenciales almacenados en la aplicación.

Recomendaciones:

En base a los hallazgos de esta evaluación de seguridad, se recomiendan las siguientes medidas correctivas y preventivas:

1. Validación de entrada: Implementar validaciones de entrada estrictas para todos los datos suministrados por el usuario, utilizando

parámetros seguros en las consultas SQL para evitar la inyección SQL.
2. Pruebas de penetración: Realizar auditorías de seguridad periódicas, incluidas pruebas de penetración, para identificar
y mitigar las vulnerabilidades de seguridad antes de que sean explotadas por los atacantes.
3. Educación y concientización: Capacitar al personal técnico y no técnico en prácticas de desarrollo de aplicaciones seguras y generar conciencia sobre los riesgos asociados con las vulnerabilidades de seguridad.

Conclusiones

La identificación y explotación exitosa de la vulnerabilidad de inyección SQL en DVWA subraya
la importancia de la seguridad proactiva en el desarrollo y mantenimiento de aplicaciones web.
Implementar controles de seguridad sólidos y seguir las mejores prácticas de ciberseguridad son esenciales para proteger los activos críticos y garantizar la continuidad del negocio.