ISO 27001 Vulnerabilidad SQL injection

Introducción:

En este reporte se realizó una exploración de vulnerabilidad de SQL injection en DWVA, se realiza bajo un ambiente controlado para poder estudiar los impactos de seguridad.

Descripción del incidente:

Se descubrió durante el escaneo en SQL injection una vulnerabilidad el cual mostraba datos personales de los usuarios guardados en la base de datos, comprometiendo la confidencialidad y la integridad de los usuarios.

Método utilizado en SQL injection:

Para replicar y demostrar la vulnerabilidad se utilizó el siguiente comando en el módulo SQL injection.

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

Impacto del incidente:

Esta vulnerabilidad lo que permite es que ciberatacantes puedan acceder a información confidencial de los usuarios almacenada en la base de datos.
Adjudicarse información delicada, para que los ciberatacantes puedan acceder a credenciales sin autorización de los usuarios.

Recomendaciones:

Realizar escaneos de forma periódica para detectar vulnerabilidades a futuro.
Usar un WAF para la protección de la página web realizando un monitoreo, filtración y bloqueo del tráfico HTTP(s) que sea malicioso.
Capacitar al personal TI sobre los ataques de SQL injection para que conozcan sus riesgos y las buenas prácticas.
La base de datos tenga la regla de “los principios de privilegios mínimos” es decir, que solo el personal asignado tenga acceso a la intervención de la base de datos, y el resto sólo para lectura.

Conclusión:

Se concluye que 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 robustos y seguir las mejores prácticas de ciberseguridad es esencial para proteger los activos críticos y garantizar la continuidad del negocio.