Informe de Gestión de Incidentes
Norma ISO 27001

1. Introducción

Este informe describe la identificación y explotación de una vulnerabilidad de inyección SQL en la aplicación **Damn Vulnerable Web Application (DVWA)**. La prueba se llevó a cabo en un entorno controlado con el propósito de detectar posibles fallos de seguridad y evaluar su impacto.

2. Descripción del Incidente

Durante el análisis de seguridad, se descubrió una vulnerabilidad de **inyección SQL** en la sección "SQL Injection" de DVWA. Esta falla permite a un atacante manipular consultas SQL enviadas a la base de datos a través de los campos de entrada de la aplicación web, lo que puede comprometer la información almacenada.

El problema se identificó al introducir datos maliciosos en el campo de búsqueda de usuarios, lo que reveló información confidencial de la base de datos sin necesidad de autenticación avanzada.

3. Proceso de Reproducción

Para demostrar esta vulnerabilidad, seguimos estos pasos:

1. Accedimos a la aplicación DVWA en el entorno de pruebas.

2. Iniciamos sesión con las credenciales (`admin` / `password`).

En la sección "SQL Injection", introdujimos el siguiente código en el campo "User ID":

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

3. Al enviar la solicitud, el sistema devolvió una lista completa de los usuarios almacenados en la base de datos, confirmando así la vulnerabilidad.

4. Impacto del Incidente

Si este fallo se explotara en un entorno real, las consecuencias podrían ser graves:

- **Exposición de datos sensibles**, como credenciales y datos personales de los usuarios.

- **Modificación o eliminación de información almacenada**, lo que afectaría la integridad de la base de datos.
- **Acceso no autorizado a funciones administrativas**, lo que pondría en riesgo el control total de la aplicación.

5. Medidas Correctivas y Preventivas

Para solucionar y prevenir este tipo de ataques, se recomienda:

- **Implementar consultas parametrizadas** para evitar que los datos introducidos por los usuarios alteren las consultas SQL.
- **Validar correctamente la entrada de datos**, asegurando que solo se aceptan valores esperados.
- **Aplicar el principio de privilegios mínimos**, limitando el acceso de los usuarios a la información estrictamente necesaria.
- **Realizar auditorías de seguridad periódicas**, detectando y corrigiendo vulnerabilidades antes de que sean explotadas.

6. Conclusión

Este caso resalta la importancia de aplicar **buenas prácticas de seguridad** en el desarrollo de aplicaciones web. Contar con medidas preventivas adecuadas y realizar pruebas de seguridad de manera continua es clave para proteger los datos y evitar ataques. Se recomienda seguir mejorando las estrategias de seguridad para reducir riesgos y fortalecer la protección de la información.