Reporte de Incidente ISO 27001 – Vulnerabilidad SQL Injection

Introducción

Este informe detalla la identificación y explotación de una vulnerabilidad de SQL Injection en la aplicación web Dawn Vulnerable Web Application (DVWA). La prueba ha sido realizada en un entorno controlado para demostrar una vulnerabilidad común y su posible impacto en la seguridad de las aplicaciones.

Descripción del Incidente

Durante la evaluación de seguridad de DVWA se ha encontrado una vulnerabilidad de SQL Injection en el módulo “SQL Injection”. La vulnerabilidad permite a un atacante inyectar consultas SQL maliciosas a través de los campos de entrada de la aplicación web, de esta manera se compromete la integridad y confidencialidad de los datos guardados en la base de datos.

Proceso de reproducción

Método de SQL Injection utilizado

Para demostrar la vulnerabilidad se ha utilizado el payload de SQL en el campo “User ID”, el payload es:

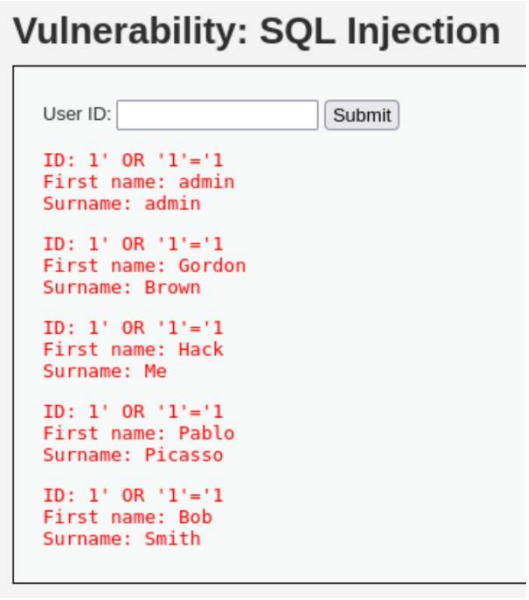
```
UNION SELECT username, password FROM users WHERE id = 1' OR '1'='1
```

Este payload explota la vulnerabilidad al modificar la consulta SWL original de manera que devuelve los nombres y apellidos de los usuarios almacenados en la tabla de usuarios. Al ejecutar con éxito este SQL Injection se obtienen las credenciales de los usuarios sin autorización.

Impacto del incidente

Explotar esta vulnerabilidad podría permitir a un atacante:

- Acceder y extraer información confidencial de la base de datos incluyendo las credenciales de usuario.



Esta vulnerabilidad representa un riesgo muy importante en la confidencialidad de la información.

Recomendaciones

En base al descubrimiento de la vulnerabilidad se recomiendan las siguientes medidas correctivas y preventivas:

1. Implementar controles de acceso para no permitir que todo el mundo pueda acceder a la base de datos o a otra información confidencial.
2. Realizar auditorías de seguridad periódicas, incluidas pruebas de penetración, para identificar y mitigar vulnerabilidades de seguridad antes de que sean explotadas por atacantes.

Conclusión

La identificación y explotación exitosa de la vulnerabilidad de SQL Injection en DVWA demuestra la importancia de la seguridad en el desarrollo y mantenimiento de aplicaciones web. Además, hay que destacar la implementación de controles de seguridad robustos para proteger información crítica y confidencial.