Explotación de Vulnerabilidad de Inyección SQL en Aplicación Web DVWA

Introducción

El presente informe documenta la detección y explotación de una vulnerabilidad de tipo Inyección SQL en una aplicación web vulnerable denominada DVWA (Damn Vulnerable Web Application). El objetivo de esta práctica es comprender el funcionamiento de este tipo de vulnerabilidades en un entorno controlado y analizar su impacto, siguiendo un enfoque alineado con la norma ISO/IEC 27001.

Descripción del Incidente

Durante el análisis de seguridad de la aplicación DVWA, se identificó una vulnerabilidad de Inyección SQL en el módulo SQL Injection, la cual permite a un atacante manipular las consultas SQL ejecutadas por la aplicación. La vulnerabilidad se debe a la concatenación directa de entradas del usuario en las consultas SQL sin ningún tipo de validación ni uso de consultas preparadas.

Proceso de Reproducción

1. Se accedió a la aplicación DVWA desde el navegador web mediante la URL http://localhost/DVWA.
2. Se inició sesión utilizando las credenciales por defecto (admin / password).
3. Se configuró el nivel de seguridad de DVWA en Low desde el apartado DVWA Security.
4. Se accedió al módulo SQL Injection.
5. En el campo User ID se introdujo el payload: 1' OR '1'='1.
6. Al enviar la solicitud, la aplicación devolvió una lista completa de usuarios almacenados en la base de datos.

Impacto del Incidente

El impacto de esta vulnerabilidad es alto, ya que permite el acceso no autorizado a información sensible almacenada en la base de datos, la enumeración de usuarios sin autenticación válida y la posible escalada del ataque.

Recomendaciones

Se recomienda el uso de consultas preparadas, validación de entradas, principio de mínimos privilegios, uso de ORM y auditorías de seguridad periódicas.

Conclusión

La explotación realizada demuestra cómo una Inyección SQL puede comprometer gravemente la seguridad de una aplicación web cuando no se aplican buenas prácticas de desarrollo seguro.