Informe ISO 27001: vulnerabilidad de inyección SQL

Weiyu

July 2025

1. Introduction

Este informe detalla la identificación y explotación de una vulnerabilidad de inyección SQL en la aplicación web Damn Vulnerable (DVWA). La prueba se realizó en un entorno controlado (máquina virtual) para demostrar una vulnerabilidad común y su posible impacto en la seguridad de la aplicación.

2. Descripción del incidente

Durante la evaluación de seguridad de DVWA, se descubrió una vulnerabilidad de inyección SQL en el módulo Ïnyección SQL". Esta vulnerabilidad permite a un atacante inyectar consultas SQL maliciosas a través de los campos de entrada de la aplicación web, comprometiendo así confidencialidad y integridad de los datos almacenados en la base de datos.

3. Proceso de reproducción

La consulta realizada tras introducir 1' OR '1'='1:

SELECT * FROM usuarios WHERE id = '1' OR '1'='1'

Esta consulta siempre es verdadera ya que '1' es igual a '1', entonces se obtiene las credenciales de todos los usuarios tras realizar esta consulta.

4. Impacto del incidente

Esto hace que todos los credenciales de los usuarios guardados en la DB sean expuestos, comprometiendo la confidencialidad y la integridad de los datos ya que a posterior sería posible modificar datos en esta DB.

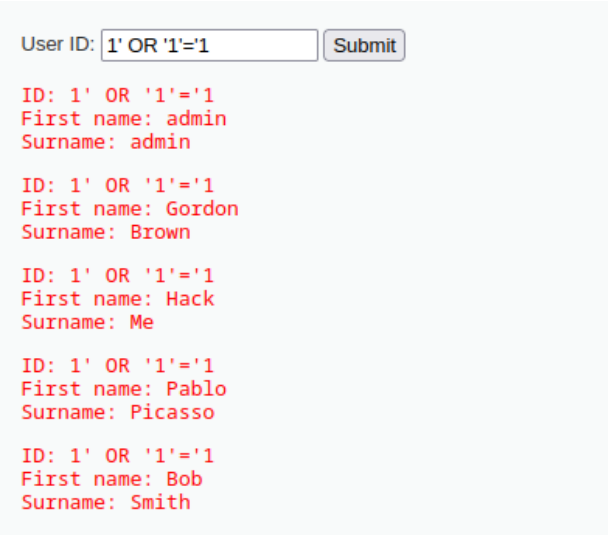

Figura 1: Resultado de la Inyección SQL

5. Recomendaciones

Lo que se debería realizar:

1. Validando los inputs del DB, no permitiendoles realizar este tipo de consultas.
2. Realizar un estudio para ver si hay datos filtrados.
3. Realizar pruebas de penetración, para ver si hay más baches.
4. Planificar auditorías externas para que un tercero realice pruebas con el fin de que sea más fiable.
5. Concienciar a los programadores y arquitectos sobre este tipo de problemas, ya que desde la planificación de la creación del DB tiene que tener en cuenta este tipo de problemas.

6. Conclusión

Este tipo de incidentes enseña la importancia de realizar pruebas en las consultas SQL y pensar en la seguridad desde el inicio de la creación del DB. Ya que desde la base de la aplicación es necesario tener en cuenta la seguridad.