VULNERABILIDAD DE INYECCIÓN SQL

Introducción

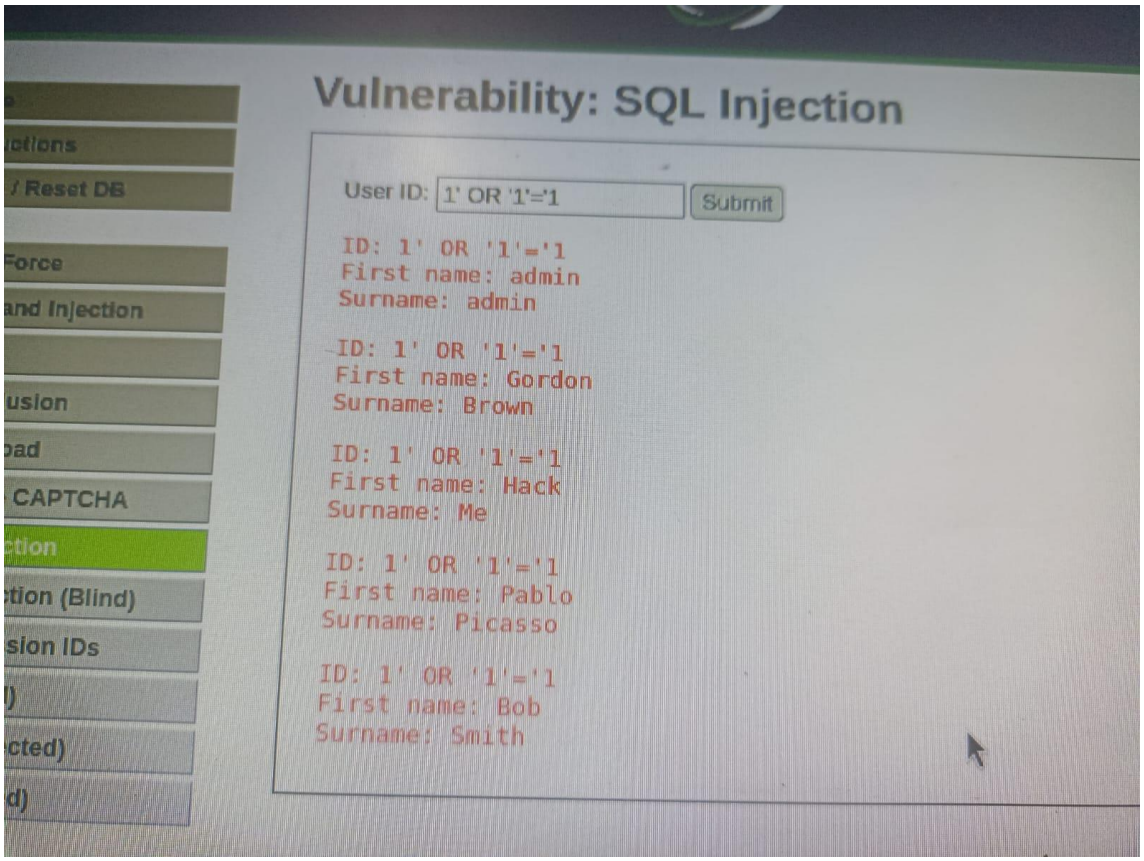
La inyección SQL es una vulnerabilidad que permite a un atacante manipular consultas a una base de datos insertando código malicioso en entradas de usuario, lo que puede resultar en el acceso no autorizado, modificación o eliminación de datos, e incluso el control total del sistema.

Descripción del incidente

En esta ocasión, usando DVWA (Damn Vulnerable Web Application) he “encontrado” y explotado una vulnerabilidad usando código malicioso.

Proceso de reproducción

Lo que hice fue colocar 1' OR '1'='1 en user ID y me muestra resultados de la base de datos que muestro a continuación.



Impacto del incidente

El impacto de una vulnerabilidad de inyección SQL puede ser grave, ya que permitiría al atacante acceder, modificar o eliminar datos sensibles en una base de datos, saltar mecanismos de autenticación y autorización, exfiltrar información personal o financiera, y en casos extremos, obtener control total sobre el servidor de la base de datos. Esto puede llevar a pérdida de datos, daño a la reputación de la empresa y pérdidas económicas significativas.

Recomendaciones

Para ayudar a mitigar este tipo de vulnerabilidad, en este caso se recomienda:

1. **Instalar un firewall de aplicaciones web (WAF)**: Ayuda a filtrar y bloquear ataques comunes, incluyendo intentos de inyección SQL.
2. **Mantén todo actualizado**: Instala siempre los parches de seguridad y actualizaciones para bases de datos, frameworks y aplicaciones, ya que corrigen vulnerabilidades conocidas.
3. **Limitar los permisos en la base de datos**: El usuario que ejecuta las consultas en la base de datos debe tener solo los permisos estrictamente necesarios(mínimo privilegio).
4. **Auditar y monitorear la base de datos**: Activa los registros de auditoría para detectar cualquier actividad sospechosa en las consultas SQL y configura alertas automáticas si se detectan patrones anormales.
5. **Hacer revisiones periódicas del código**: Implementa auditorías de código, tanto manuales como automáticas, para identificar y corregir posibles puntos de inyección SQL.

Conclusión

Es crucial abordar este tipo de vulnerabilidades de inmediato para evitar posibles daños a la seguridad de la base de datos y poder cumplir con CIA(confidencialidad, integridad y disponibilidad). Es fundamental realizar una revisión exhaustiva del sistema para detectar posibles brechas adicionales y fortalecer la seguridad general, con el objetivo de prevenir futuros ataques.