Reporte del incidente de la vulnerabilidad de inyección SQL

Introducción

El objetivo de este informe es identificar, explotar y reportar una vulnerabilidad de inyección SQL encontrada en una aplicación web de prueba denominada Damn Vulnerable Web Application (DVWA).

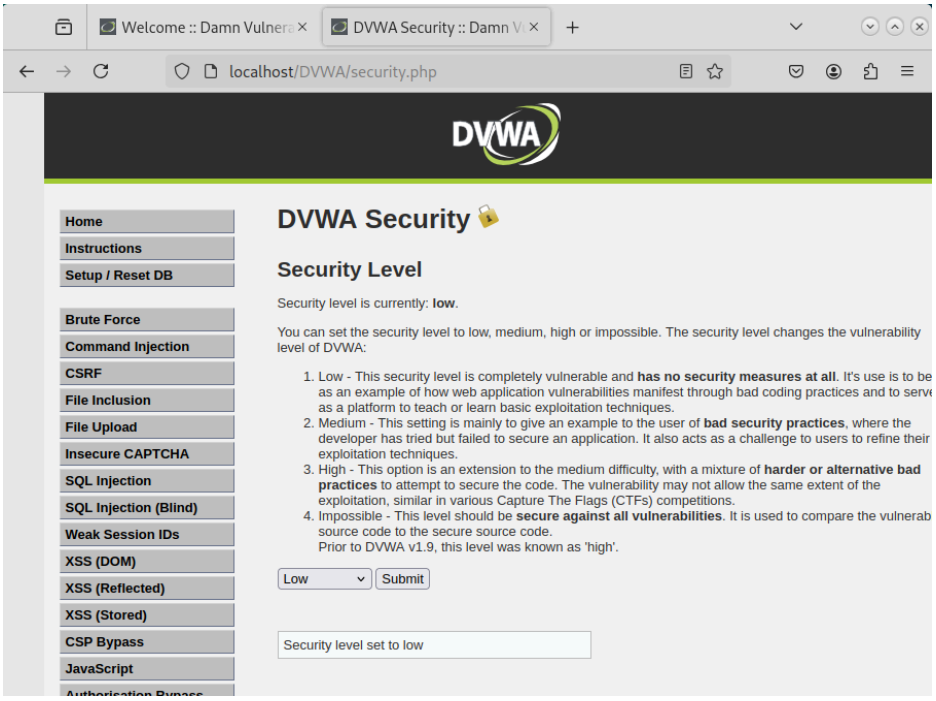
Por otra parte, la realización y explotación de la vulnerabilidad se realizó en la máquina virtual Debian para así tener controlada la vulnerabilidad.

Descripción del Incidente

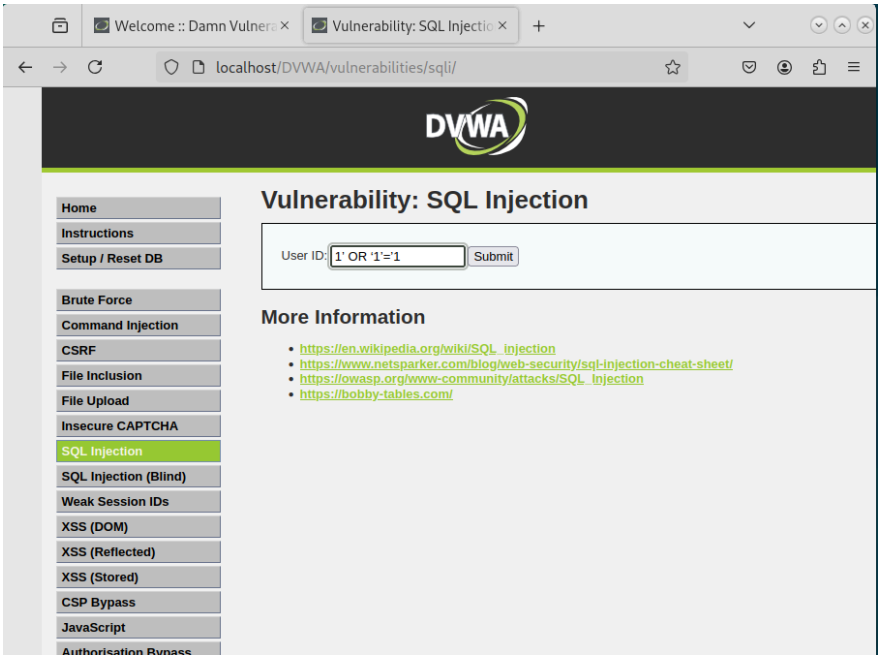
Se ha descubierto que la web DVWA es vulnerable a ataques de inyección SQL en el módulo de "SQL Injection". Este tipo de vulnerabilidades permite a un atacante inyectar consultas SQL maliciosas a través de los campos de entrada de la aplicación web. De esta forma los atacantes pueden manipular la base de datos de la web a través de entradas de usuarios inseguras, y como consecuencia se compromete la integridad y confidencialidad de los datos almacenados en la base de datos.

Proceso de Reproducción

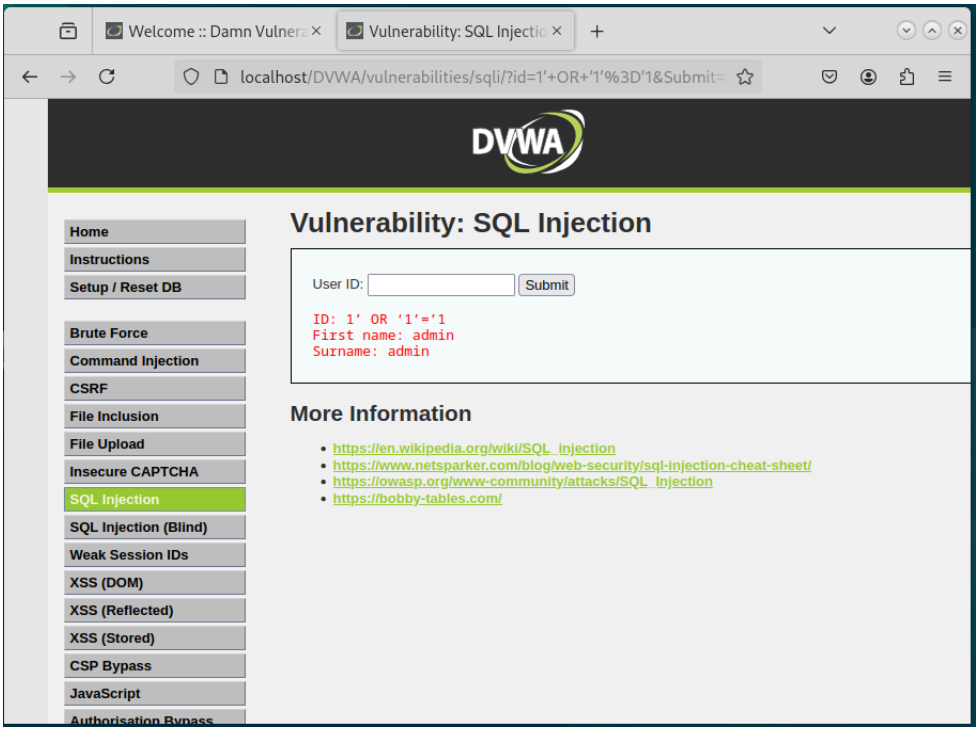
Para poder reproducir esta vulnerabilidad primero se ha accedido a la web http://localhost/DVWA y se ha cambiado el nivel de seguridad a bajo de DVWA:



A continuación se ha introducido el payload ***1' OR '1'='1*** en el campo "User ID" del apartado SQL Injection del DVWA.



Se ha podido realizar la inyección SQL ya que los resultados de la inyección nos muestran datos de la base de datos:



Impacto del Incidente

Esta vulnerabilidad es un riesgo ya que permite a los atacantes extraer información confidencial de la base de datos de forma sencilla y sin tener que necesitar credenciales de autenticación para acceder a la base de datos. En resumen, compromete la confidencialidad e integridad de los datos almacenados en la base de datos.

Recomendaciones

Es recomendable aplicar las siguientes medidas para mejorar la seguridad de la web:

1. Implementar validación de entrada en el servidor para evitar que se introduzcan comandos de SQL maliciosos y para que se verifiquen todas las entradas de la base de datos.
2. Crear usuarios nominales para la administración del servidor y concederles los mínimos permisos necesarios (principio de menor privilegio). Se tendría que eliminar el usuario genérico “root” o “admin”.
3. Mantener la base de datos y los servidores actualizados
4. Realizar formaciones a los trabajadores para que empiecen aplicar desarrollo seguro en las aplicaciones y sean conscientes de los peligros de no aplicar estas prácticas seguras.
5. Realizar auditorías o pentest de forma regular para detectar estos fallos en la infraestructura de la empresa.

Conclusión

La realización de inyección SQL en DVWA demuestra que la web tiene una vulnerabilidad grave que pone en peligro sus datos confidenciales de la base de datos y que en la vida real podría repercutir negativamente en las ventas de un negocio y en su reputación.

Esto demuestra que es esencial aplicar las medidas de ciberseguridad para desarrollar una web segura y también poder mantener su nivel de seguridad a lo largo del tiempo.