“ATAQUES Y EVALUACIÓN DE VULNERABILIDADES (Parte III)”

Informe N°4

Laboratorio de Seguridad en Redes

Melanny Dávila
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
melanny.davila@epn.edu.ec

Alejandra Silva
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
alejandra.silva@epn.edu.ec

***Abstract*—En el siguiente documento se detallará el proceso llevado a cabo durante la sesión de laboratorio sobre la aplicación DVWA mediante la inflitración de código para poder acceder a bases de datos.**

***Index Terms*—Ataque, SQLMap, base de datos, Kali, DVWA.**

I. Introducción

Actualmente existe gran cantidad de herramientas que permiten realizar ataques mediante diferentes herramientas en este caso SQL que se vale de una vulnerabilidad informática para realizar operaciones sobre base de datos haciendo énfasis en estas herramientas también se evaluara los ataques mediante la aplicación DVWA que ayudan a los profesionales de la seguridad a poner a prueba sus habilidades y herramientas en un entorno legal y ayuda a mejorar la seguridad y protección de aplicaciones web.

II. Objetivos

- Explotar las vulnerabilidades de un equipo dentro de un entorno controlado.
- Realizar diversos ataques sobre la aplicación DVWA utilizando la técnica de SQL Injection.
- Utilizar técnicas de explotación manual como herramientas automáticas (SQLMap).

III. Cuestionario

A. Presente la configuración realizada en el laboratorio.

Para poder realizar la lectura de las bases de datos vulnerables se utiliza la herramienta SQLmap, para lo cual se debe tenerla instalada en kali y, posterior a esto, junto con el comando sqlmap se debe colocar la opción –headers seguido del agente de usuario y la opción -dB.
Se visualizó el contenido de varias bases de datos explorando algunas de las opciones que ofrece sqlmap como llegaria a ser la opción -dump que es usada para mostrar todo el contenido de la base de datos.
Esta herramienta puede ser usado para obtener información delicada como llegaría a ser las contraseñas de un grupo de usuarios alojadas en la base de datos. Este ataque se debe complementar con otros para poder ser completamente efectivo y explotar todas las vulnerabilidades tal y como se realizó en la sesión de laboratorio.

B. Presentar las capturas de pantalla, con la debida explicación de los resultados mostrados.

En la sesión de laboratorio como primera parte se realizó pruebas de conectividad entre las máquinas virtuales Kali, Metasploitable y la máquina física.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.191.136
PING 192.168.191.136 (192.168.191.136) 56(84) bytes of data.
64 bytes from 192.168.191.136: icmp_seq=1 ttl=64 time=1.43 ms
64 bytes from 192.168.191.136: icmp_seq=2 ttl=64 time=0.726 ms
64 bytes from 192.168.191.136: icmp_seq=3 ttl=64 time=0.257 ms
64 bytes from 192.168.191.136: icmp_seq=4 ttl=64 time=0.680 ms
64 bytes from 192.168.191.136: icmp_seq=5 ttl=64 time=0.482 ms
64 bytes from 192.168.191.136: icmp_seq=6 ttl=64 time=0.490 ms
64 bytes from 192.168.191.136: icmp_seq=7 ttl=64 time=0.245 ms
64 bytes from 192.168.191.136: icmp_seq=8 ttl=64 time=0.793 ms
```

Fig. 1. Prueba de conectividad Kali-Metasploitable

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.191.2
PING 192.168.191.2 (192.168.191.2) 56(84) bytes of data.
64 bytes from 192.168.191.2: icmp_seq=1 ttl=128 time=0.639 ms
64 bytes from 192.168.191.2: icmp_seq=2 ttl=128 time=0.347 ms
^C
--- 192.168.191.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1027ms
rtt min/avg/max/mdev = 0.347/0.493/0.639/0.146 ms
```

Fig. 2. Prueba de conectividad Kali-Máquina física

Posterior a eso, mediante el explorador de la máquina física se escribe como dirección web la siguiente dirección IP de Metasploitable: 192.168.191.136, tal como se presenta en la figura 35.

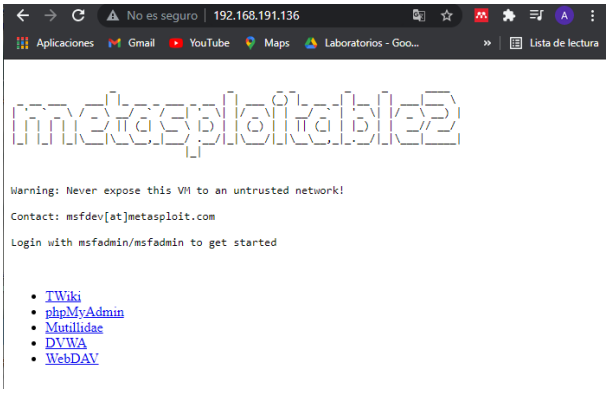

Fig. 3. Página web de Metasploitable

Una vez que se llega a la opción DVWA, se debe ingresar las respectivas credenciales

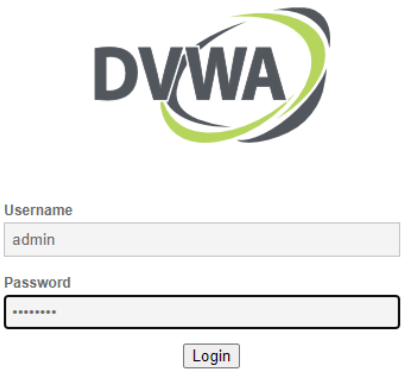

Fig. 4. Acceso a DVWA

De esta manera se configurará la seguridad de DVWA tal y como se presenta en la figura 5, es decir un nivel de seguridad bajo.

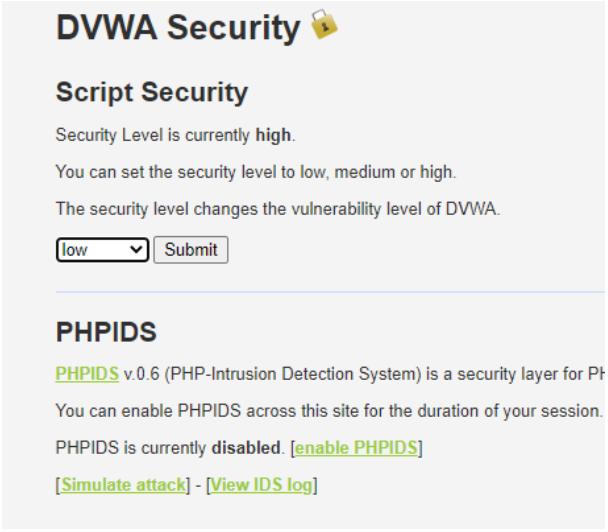

Fig. 5. Selección nivel de seguridad

Fig. 6. Nivel de seguridad establecido

Para proceder a realizar la inyección SQL se procede a la ventana SQL Injection.

Fig. 7. Vulnerabilidad SQL Injection

El User ID es un contenedor que lista nombre de usuario que este en una pagina web de alguna empresa y realiza una búsqueda de tal manera que muestra ID de usuarios y bot el usuario como se ilustra a continuación.

Fig. 8. Prueba User ID

Se coloca una comilla y si responde la base de datos responde, significa que se puede hacer pruebas de ejecución.

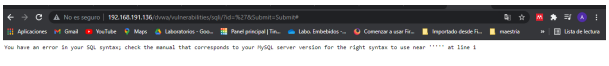

Fig. 9. Prueba vulnerabilidad

Como se presenta en la figura 9, con lo que se concluye que el sitio es vulnerable.

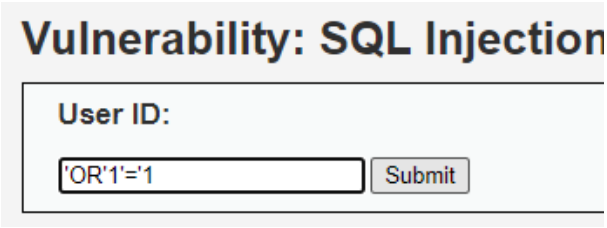

Fig. 10. Vulnerabilidad de un sitio

Resultados devueltos por el comando ingresado anteriormente, dado a que dicha sentencia que se usó indica que cuando el ID sea igual a cualquier cosa o 1=1 se devolverán todos los resultados de la tabla.

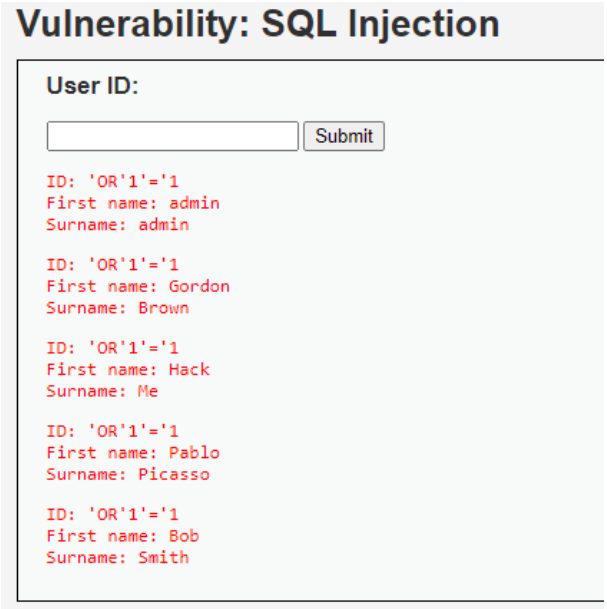

Fig. 11. Datos de la tabla

Cuando se revisa en View Source, se observa la petición legal que se mandó. Así se realizaría un ataque de inyección super básico.

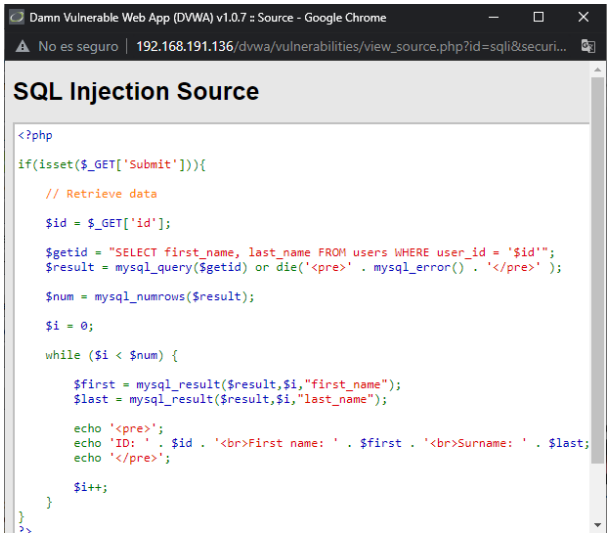

Fig. 12. Petición enviada

Se realizará el primer ataque, mediante el uso del comando union select database(),versión()#.

Unión permite ejecutar otra sentencia SQL y el MySQL seleccionar por método database el nombre de la base de datos

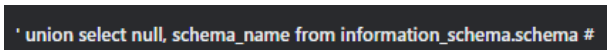

Fig. 13. Comando utilizado

Mediante el uso del comando mostrado en la figura 14, se tiene:

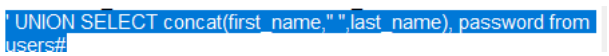

Fig. 14. Comando por utilizar

Resultados obtenidos en base al comando mostrado anteriomente

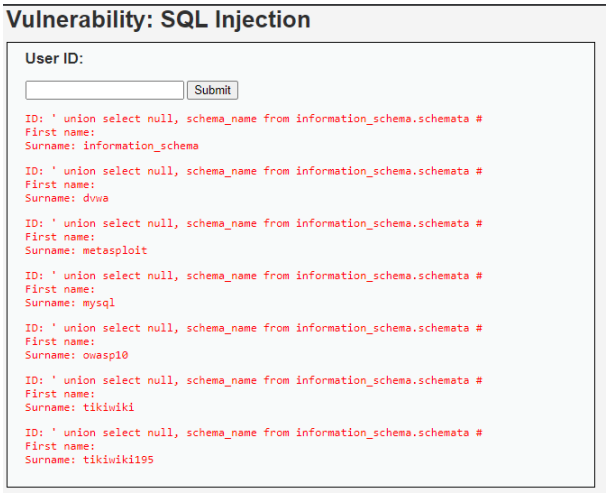

Fig. 15. Resultados del comando

Al utilizar el comando mostrado a continuación:

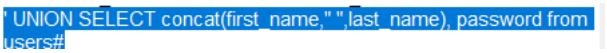

Fig. 16. Comando

En la figura 17, se ordena que se ingrese el nombre de la tabla, el nombre de la columna y que se haga la consulta. Se visualiza lo siguiente:

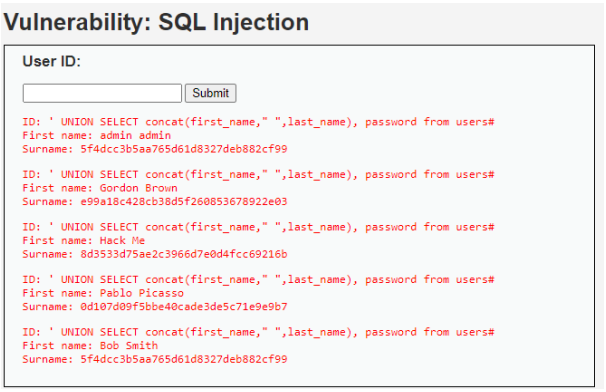

Fig. 17. Resultados

En la figura 18, se muestra la página que se utiliza para decriptar las contraseñas.

Fig. 18. Página para decriptar

En la figura 19, se muestra el resultado de la búsqueda de HASH, que corresponde a charley.

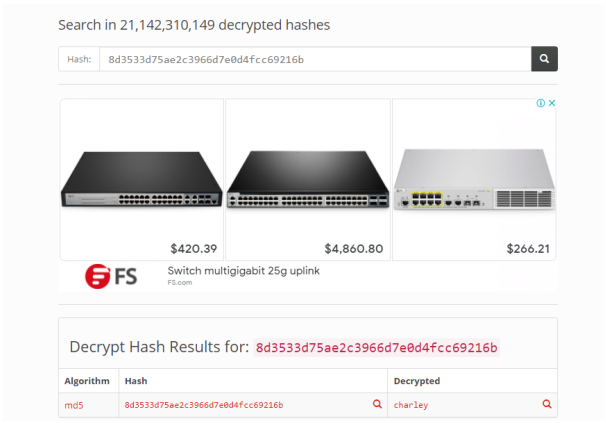

Fig. 19. HASH “decriptado”

Se obtuvo la información de las claves de los usuarios, la misma que fue decriptada mediante una paǵina.

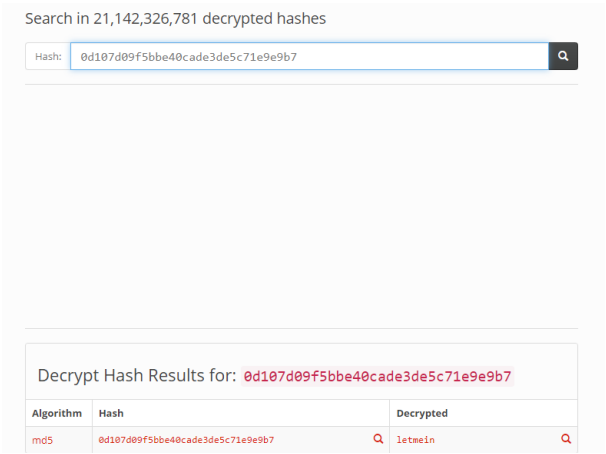

Fig. 20. Resultado HASH “decriptado”

Así se presenta el resultado final, cuyo HASH es: “230ca5bf6c311e7a9500cad0880a86da”

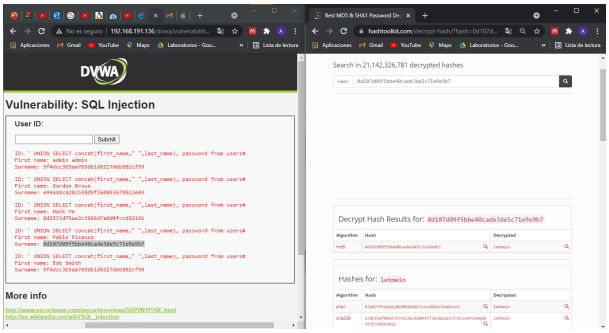

Fig. 21. Resultado HASH

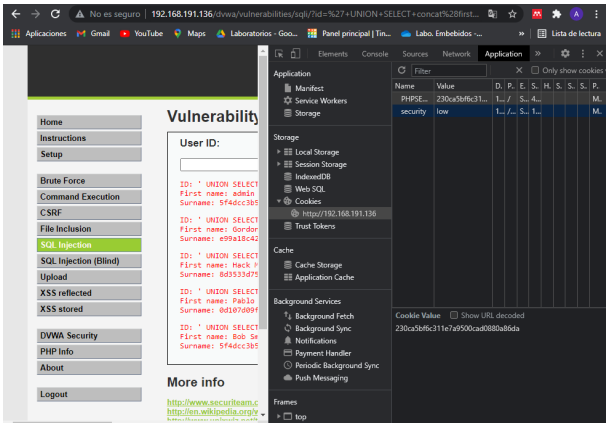

Fig. 22. Resultado final

Para resolver las credenciales, se hace uso de la página web mostrada en 23, donde el primer dato que se necesita es el valor de HASH que ya se mostró anteriomente.

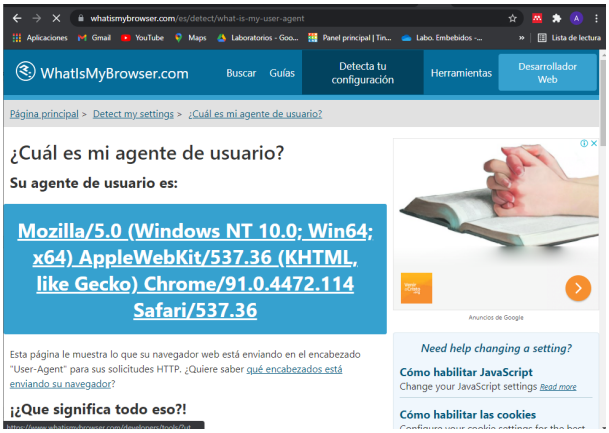

Fig. 23. Página web utilizada

Posterior a eso, se obtuvo como resultado el siguiente agente de usuario: “Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36”

En la figura 24, se muestra el inicio de SQLmap y que se prueba la conexión con el URL de la víctima.

Fig. 24. Inicio de SQLmap junto a pruebas de conexión

Luego de definir la petición a sqlmap para que muestre las bases de datos, se mostrarán los resultados en la figura 25.

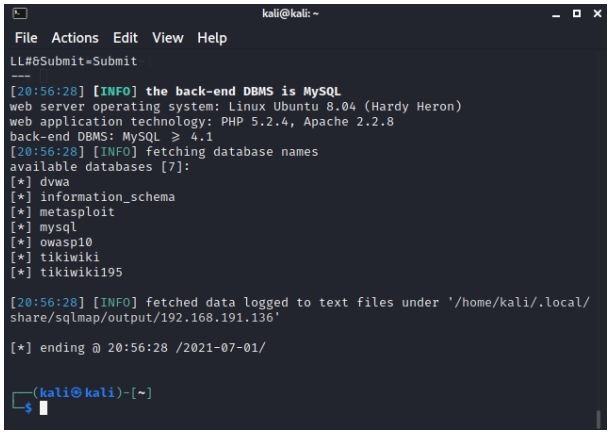

Fig. 25. Resultados

Para obtener la información de las bases de datos se usa la opción -dbs -D “nombre de la base de datos” -T “tabla que se desea ver”, y los resultados se muestran en la figura 26 y 27.

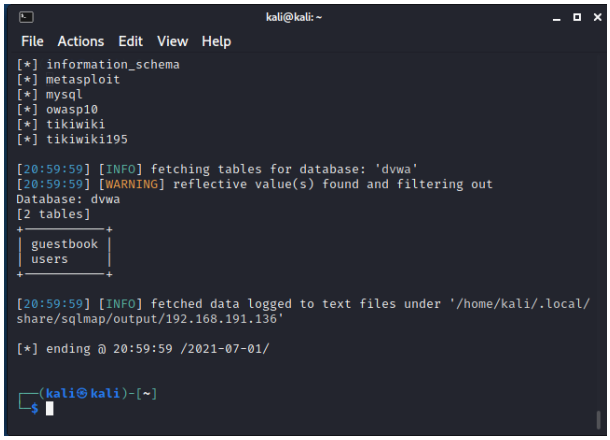

Fig. 26. Resultados

Para poder visualizar todo el contenido de una base de datos se usa el comando -dump al final del pedido como se evidencia en la figura 27.

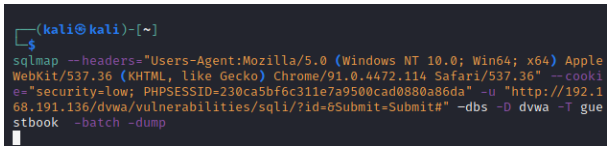

Fig. 27. Visualización sencilla de una base de datos

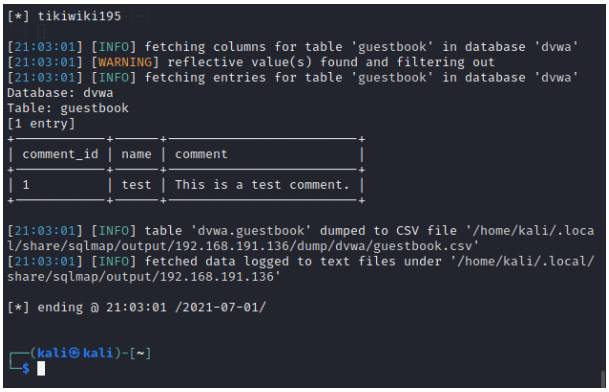

Fig. 28. Base de datos con todos sus campos mostrados

Luego, para obtener las contraseñas de los distintos usuarios de la base de datos se ejecuta el comando de visualización de la base de datos más la opción -dump que es para que muestre todo lo que se encuentra en la base de datos para la base de datos llamada users. Los resultados se muestran en la figura 29.

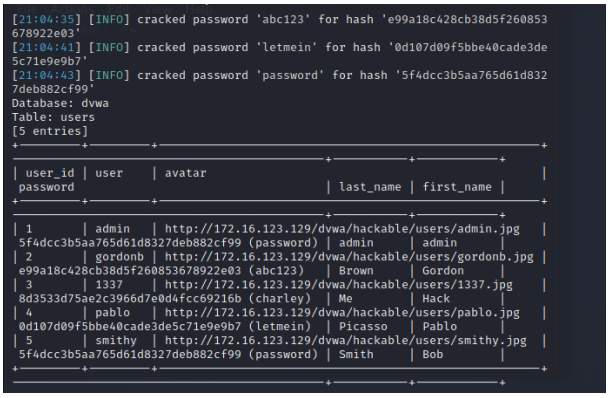

Fig. 29. Contraseñas de los distintos usuarios

C. Modifique la base de datos agregando un nuevo usuario con su nombre por medio de una inyección SQL.

El primer paso para agregar un nuevo usuario es una conexión remota mediante el comando telnet a la IP del metasploitable como se indica en la siguiente figura.

Fig. 30. Telnet a la IP de metasploitable.

Ahora lo que se tiene que utilizar el gestor el SQL de la maquina.

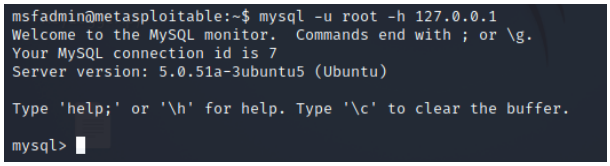

Fig. 31. Gestor SQL.

Luego se verifica las bases de datos que se tiene.

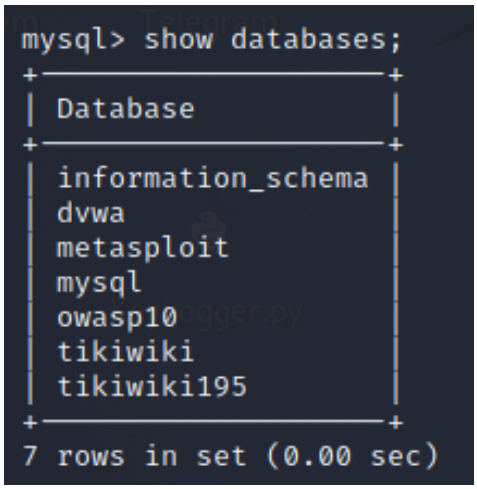

Fig. 32. Base de datos existentes.

Ahora se procede a escoger la base de datos que queremos desplegar y añadir otro usuario tal como se indica a continuación y se despliega la información de usuario y las contraseñas que posee cada uno de estos.

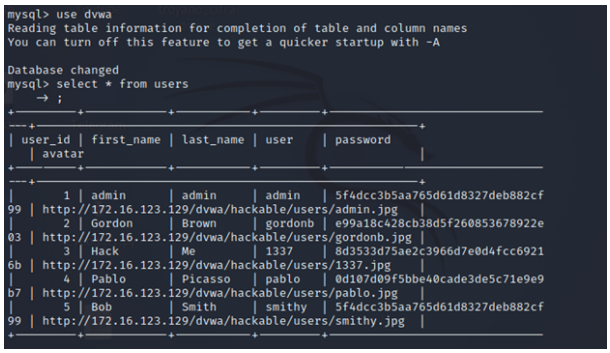

Fig. 33. Base de datos DVWA.

Ahora finalmente se coloca el código para insertar el nuevo usuario, tomando en cuenta los parámetros que constan en la visualización de la tabla anterior, first_name,last_name.user y contraseña.

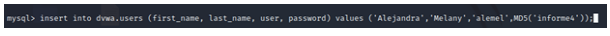

Fig. 34. Comando para agregar un nuevo usuario.

A continuación se indica como queda la nueva tabla al agregar el usuario pedido.

Fig. 35. Nuevo usuario agregado.

D. Conclusiones

- Se identificó que SQL injection posee varios métodos que ayudan obtener información desde un navegador web como tal. También, este mismo ataque, puede ser realizado desde una conexión telnet que permite no solo tener la visualización de las bases datos que posee dicha maquina, sino también poder añadir otro tipo de usuario creando así una vulnerabilidad muy fuerte.
- Como se pudo comprobar en esta sesión de laboratorio, SQLMap permite realizar pruebas de penetración de código abierto que automatiza el proceso de detección y explotación de fallas de inyección SQL.
- Un ataque "SQL injection" se vale de malas interpretaciones que se dan por el uso de MySQL, en algunos casos, este ataque puede hacer un bypass en la página de login de algún servidor, por lo que una seguridad puede ser saltada.
- Los ataques de inyección SQL pueden llevar a que un atacante extraiga información privada como númerosamos? lo jade tarjetas de crédito, contraseñas o registros sensibles de los usuarios. Asimismo no solo se puede extraer la información, sino también destruirla con los comandos de la base de datos.

E. Recomendaciones

- Se debe verificar que la información guardada no se encuentre en texto plano ya que es muy fácil acceder a ella debido a que no poseen una clave de encriptación.
- Es importante hacer pentesting a los servidores que se tienen funcionando dentro de una empresa ya que así se pueden explorar las vulnerabilidades de la misma.
- Comprende previamente el uso y suntaxis de comandos como union y concat con el fin de evitar inconvemientes en el desarrollo de la práctica de laboratorio.

REFERENCES

[1] J. G. & WEBPerfil, "Concatenar columnas y texto en SQL — CONCAT SQL". https://www.srcodigofuente.es/aprender-sql/funcion-concat (accedido jun. 29, 2021).

[2] "SQLmap". https://tools.kali.org/vulnerability-analysis/sqlmap (accedido jun. 29, 2021).

[3] "Important SQLMap commands", Infosec Resources. https://resources.infosecinstitute.com/topic/important-sqlmap-commands/ (accedido jun. 29, 2021).