# WRITE-UP WRECK-IT 2024 KUALIFIKASI

10 Agustus 2024

## *pertama kali ikut wreck it :)*

*(IPB University)*

» patsac «
» arai «
» aqua «

# Daftar Isi

# Forensic

## MyHeroComedya (100 pts)

Para Pahlawan Punya Cara Komunikasi sangat rentan, mereka bahkan mengirimkan compressed file yang sangat rahasia dengan cara yang tidak aman, Bisakah anda merecover semua file nya?

Hint: Hero butuh banyak data

Diberikan sebuah file packet capture setelah dilihat summary nya ada tcp, icmp, dan beberapa hasil record dari lalu lintas jaringan

```
araisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/hero_acadmia$ tshark -r herokom.pcapng -qz io

===================================================================
Protocol Hierarchy Statistics
Filter:

eth                                      frames:286 bytes:890558
  arp                                    frames:24 bytes:1224
  ip                                     frames:262 bytes:889334
    icmp                                 frames:144 bytes:7416
    udp                                  frames:14 bytes:3530
      ssdp                               frames:12 bytes:2616
      dhcp                               frames:2 bytes:914
    tcp                                  frames:104 bytes:878388
      data                               frames:46 bytes:874512
===================================================================
```

Setelah saya analisa ada file -file nya langsung saja saya coba extract dulu

`$ foremost herokom.pcapng`

Setelah itu saya coba extract data icmp dan didapat lah  data dan ternyata salah satu ny password zip

```
araisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/hero_acadmia$
araisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/hero_acadmia$ tshark -r herokom.pcapng -Y 'icmp.type == 0' -Tfields -e dat
a | tr '\n' ' ' | xxd -p -r
halllooooo6f6e65666f72616c6c5f616c6c666f726f6e65oneforalloneforalldoneeearaisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/he
ro_acadmia$ echo 6f6e65666f72616c6c5f616c6c666f726f6e65 | xxd -p -r
oneforall_allforonearaisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/hero_acadmia$
```

Password zip nya  mendapatkan beberapa file private dan public key. Yang ternyata private_key encrypted

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFNTBfBgkqhkiG9w0BBQ0wUjAxBgkqhkiG9w0BBQwwJAQQALOoQODLZ0Euqpm2
V0M6+QICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQMEASoEEBeAT3RA2N50Ymhl
rnzk0XYEggTQaUt9JGwqjHV+LeoCdTz5jgt+KLB7z+CTONFcadVPnkihd/yjSBX8
TMm0DwU3B42Y6Pp+Nok3NdcLjoKYEdo4paqr2HkCuSpfpxJ2U9x44JSkBPzu3EtM
6H66Zu2UlmBUAEJI4J6543MT0gejaaHVduK9Gvx7BD66m+Q4z2hAEjX1dG+29W7K
QIQyvH2ec3Ihoc0EFchl+7jj506rto/UmXndh25f7ofABnm2JIl1lK45deqWU1TN
+AfjctIkbAU+5mVNKyzLt69g9heeJ0Hx4790b75naOKVllAhBwC8OTgzQPHK0H31
xT9/l9nxtZMtKBF+/tv4XCk9Y3vEJX4oaUc2QRjJUlj2gaIxzEuKKXRZvcQw/VZC
msrsobtyI58EQ9gEsvKbt3vlIEi1EuzdJgxsTUoue3BqgLJ/4FVQfnY9nXlCYf0C
qKx18UlQR8rf27XD9mauNrREWu5g5BP/86ERrxml3RyHDCxgFev7zUBgXzXSUBn3
QTpoqHyqVsx2iLcMX8mFiC1pk4wOkaCX9qEkjBbmPi4i8MtWfPEKpBeQFB6Lj4Zy
U9QXdIpZK93JX+ZNLorAyYq/0cG5SDA4BAQiyoEz17nlK1GQ+iUqeDcxJz/5aTL3
VTHMr7+EXuPkvrtR6F0/o1Wt0N/1td1z4j3Xbo57XKtCq2+bgM9trwKyQSGXfBrn
+hBad1Wja71Xq4Fre89HBF6lW4HNngpBWH2/wz6P0TfwZoN1IxVixWlflZ7vn9qK
IdDRyl1ZnVC2FMR+RFVoOw5OAgvf9XQuX1Q9KqRlOWzH3zQLHOdkvSVLbM4Q8ui5
NwoO3XGM5Rqf+wWP62J6Ut5uDobJYU3wZq2+a3wHf+iobOvpLSwGbHDWOPBK8PHW
gBD3wHa0ltDBaJ1nb9TpUUKB7QYgr/SU9DZVggk6AjxDFWVM6v+E6B+TbAw71DTx
q1uCDFEjNqsBEUa43HE7z1rhgSqxHOue11YbYNa0pNaMn69UQsnrBCmdk36IvUDR
S2nbdDs8Uiwwn5NXouIjEWwx/PY+hd1j20lNreZjmPERuK6VLanvSwv8Dq+d5Nmt
UVibrxlvkhvcKB6kGFD9WiQ412LqtzWvRDSSGN5HSvWIBfFsH7ObI6WsWs55jj1c
s5iUyijL3HZ0FFnalTF6a1z3Kz90WGtb7KjFi+jvYZ33mfJi5pdRAiH2Mw7UaIRt
mMPm2UO3Pe73jvIJxNh1sOPlBRSLkYapZNjpvGQLMNjHfapQAH+448zbrUVRb973
wQAvURBXPDgxz23z2KsrWAyoFl2UB0+ACUSvGE+tWgMWHqzQFmihpF4ag10K/xL3
4lgSKHCU5+sRJ2rOkbSk0gMYepm7T8R0Xci6xQwhKwpju72Tsc4N2UpUKiPd9IgO
xqaXQNOG2ujBeo5qVumo2qLVhcEshW71rBPqEnqMZWWax7aT2TkYsO9c+a6V4U9E
SCzyPKSf/mFxiV6MJSJ158NZ1OQUcBzA0HAmtRl4bJmC9pvt07lPG4dE6is+1tXd
SJ7T6u4muSc3V/ljFXSbxCBzVauDn/CHWm7K1HYHgEJIsrGBIxgQbXYyorR34bAL
qD9cKshEC9xMkgWlIeCx8uiQwPQiz8KcVUuCeuS/FiwHSsgwRLAj6Ok=
-----END ENCRYPTED PRIVATE KEY-----
```

Dari sini setelah cukup lama coba cari bug rsa nya atau pun mencoba memahami soal ternya passphrase nya ada di icmp tadi yaitu oneforall

```
araisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/hero_acadmia/output_Sat_Aug_10_17_40_11_2024/zip$ openssl rsa -in oneforal
l.pem
Enter pass phrase for oneforall.pem:
writing RSA key
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC7v1Syjkxnmguz
hXN6Rdn8yHSQT39TPBaeesKLi3AbVAfNjbbviZdu8/Tu3LnAXyYpeZHlLvzAE25j
oYOaZJ8JrvHojHUqjJaZHUtvzjOFrNvU3poQVQkpHu+SGC46rgEM6qkNqCHS/tml
2btMKbOXS5063F9vVWxmjAw36GKOyhVbqlD1MsQUmMxCUHjqAkpMV+yaFQSCm0AE
Zpk5cKn1BKpxlBhjhbXGMn3T5AlXX82+0ve8DbI3Vnsh3r2wWgz3TkTQxyzv964R
ml3xDOM5+6XAzJDqRH8bYcVy2zUUb85L+ZR2ti6emdEcH8prmUqT+fq1Nfe8zIac
mwd/65ZBAgMBAAECggEAB9IeixmWYTJvjUOb3doPDJKlGGXXXfZA0vU2KW3zi4/i
i1N97ViD8GFFMLYNHtBX3J5tz2g3qyCkFo5h1wqd/V9GQHOpZc5Zb6NiwxOJ3eWn
eqSTMl74dLgPLrzHIDajYJBd3m3Eiu+GzXvWa4PJMWI6+Hq5lv+t9k+bKrEJef0q
tXS/IIFhfcCBTLgzk4yJAg1wWs6yamZwDXBAbqGCJx9LmtvETHyO+n6O4iZGmjdV
AWJs3sDahllME4biNOcr9R0sFJM1WXKntOZny4PuqWk+AJKD6z8sPlEbLzN5TQDF
e2ZulBKGoPHEVoFT1ph3kIAYebrJry0ONFPmm3rzyQKBgQDu6/IqlDiOpS9zeEUe
QCZiqBD3n/syf+FLXX3fm2hiXZYp7A/nSsQwWK6wMDo1z07OylAqFzv3oAUph9bi
P5UWvgaRQsnWBG5dVjfjHreSh7Zbj/hZaPYhv06haPAIGndSvUHIpEDbnxT1jlNE
c4HquRkW1Czne5x3rrkA60wwuwKBgQDJKvDr70bqT4dxbjGV843VZQhHSVWIY8uK
40UygGfawX5gD8vpzjhJsIMch5xAoxRB136nRiJw9duACSfD1Gob5MdO3cNlHKxH
NXdrc0Xre7QvM5f38wtFZtNsBwsy7uYOw80trHhyXjFHjgSROqQ00Pht7duLecHW
6S809mATMwKBgDAZnFVqJcDCDL2IdxHSBGhUQaY4tQ/Dow3TMqYz2V4ETVj/R2xf
JwQ8tl6ONwniRJFpNZ5jsxT1SFTGHkLKXi+H7jaMZaoKllWAKBw3cOm1HMduQqdt
dC/zHddtEvXurhsgMwA74TrV2hhdoPHk90DUJvLroGayAhwuNtyyglJFAoGAO17v
B9LwrQqXwMRy4fylqYtN7CwakExTsEPvEj6PaCKfN56x4ek495aeu3bSiMkYm24M
NTYfyBLnm1wYXlV8k4rrv7z3hAn4VnPTMOUuh5dU0HF7snQKqYr1bvaNOZUEVOs4
zPgP/EEMbj/d3Tbfa68ZAuimWP2wVcswYYMtS70CgYEAsoHnzBPfvxiknewi6Rrw
png5faHiZmfB+H0ARKVsfina4te2ndVzhjLUPoIBd5SgatWvFqO6vnG/pNmDGOaa
PCEaVYSvLuk/09UidS25uzOLlVcZC8rWmOVBdfzIhZ224JRqOeDmVeKqomvtN1ch
GIPOMf5NzT8DYQekmlnPjN8=
-----END PRIVATE KEY-----
araisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/hero_acadmia/output_Sat_Aug_10_17_40_11_2024/zip$
```

Setelah itu kita decrypt private key nya dan di dapat lah pw untuk zip lain

```
araisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/hero_acadmia/output_Sat_Aug_10_17_40_11_2024/zip$ l
00000019.zip  00000039.zip  allforone.pem  b*  oneforall.pem  priv.pem
araisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/hero_acadmia/output_Sat_Aug_10_17_40_11_2024/zip$ openssl rsautl -decrypt
-inkey priv.pem -in b
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
tinggalsatulangkahlagimenjadiheronomorsatudidunia
```

Setelah di extract ternyata zip tersebut masih rusak dan harus kita recover kembali png nya.


`Flag : WRECKIT50{H4RusNy4_S1mple_And_B4S1c_Sm4sh}`

## The Magic of Word (410 pts)

Seorang kakek tua memberikanku file aneh ini, dia bilang akan menunjukan sebuah teknik rahasia yang dipelajarinya saat perang dunia pertama.

Author: aodreamer

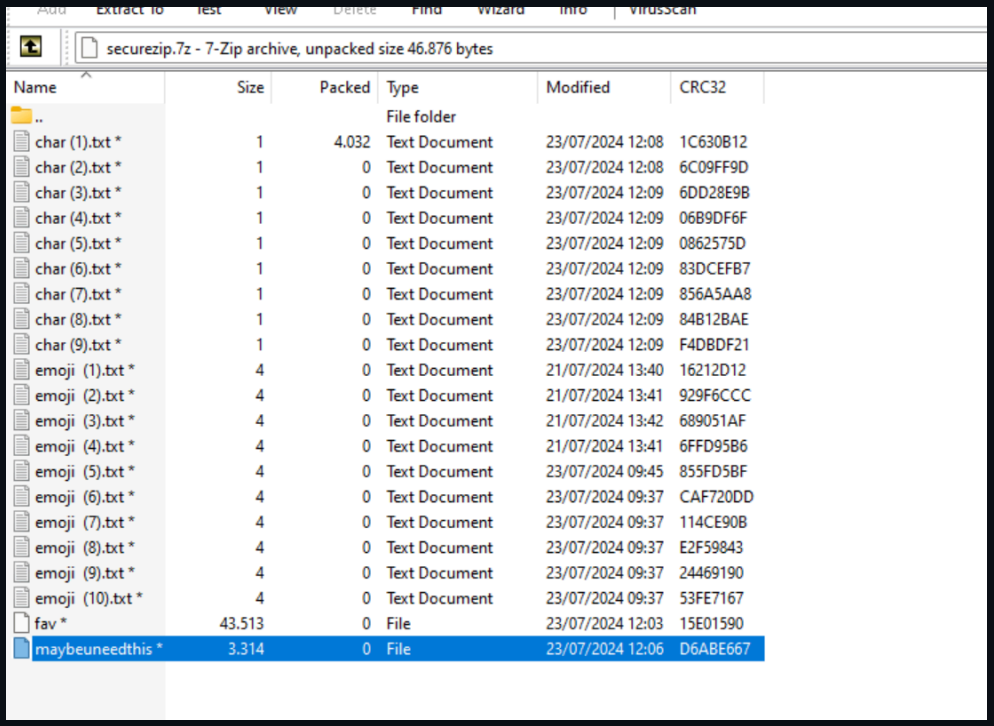
Terdapat file secret yg teridentified sebagai file documents karena file document saya befikir untuk extract mengugunakan unzip

```
araisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/apawel$ tree
.
├── [Content_Types].xml
├── _rels
├── docProps
│   ├── app.xml
│   └── core.xml
└── word
    ├── _rels
    │   ├── document.xml.rels
    │   └── vbaProject.bin.rels
    ├── document.xml
    ├── endnotes.xml
    ├── fontTable.xml
    ├── footnotes.xml
    ├── numbering.xml
    ├── settings.xml
    ├── styles.xml
    ├── theme
    │   └── theme1.xml
    ├── vbaData.xml
    ├── vbaProject.bin
    └── webSettings.xml

5 directories, 16 files
```

Disitu terlihat ada vbaproject.bin ketika saya strings ternyata dapat link mega

```
!+[]+!+[]
msI^
myString
your_password_here
_B_var_your_password_here
ord is cID="{89E4EBCC-E098-4137-AE0D-7642C19E49D5}"
Document=ThisDocument/&H00000000
Module=Module1
Name="Project"
HelpContextID="0"
VersionCompatible32="393222000"
CMG="4A48B71C14201420142014201420"
DPB="A3A15EC7B6C8B6C8B6"
GC="FCFE01A203FA04FA0405"
[Host Extender Info]
&H00000001={3832D640-CF90-11CF-8E43-00A0C911005A};VBE;&H00000000
[Workspace]
ThisDocument=0, 0, 0, 0, C
Module1=32, 32, 1456, 651,
77 69 6e 64 6ThisDocument
Module1
2f 6d 65 67 61 2e 6e 7a 2f 66 69 6c 65 2f 51 6a 64 6a 32 5a 6a 4c 23 31 79 50 5f 70 70 45 38 57 34 54 58 57 4f 64 4b 52 51 6
6 4a 43 6c 56 4f 4c 51 47 6a 58 63 51 72 76 52 49 61 73 73 4b 6f 6d 5f 63 22 3b
!+[]+
 Unprotect the document if it's protected
wreckitaseqaseqjos'
Attribut
e VB_Nam
e = "
araisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/apaweh/word$ echo 2f 6d 65 67 61 2e 6e 7a 2f 66 69 6c 65 2f 51 6a 64 6a 32
 5a 6a 4c 23 31 79 50 5f 70 70 45 38 57 34 54 58 57 4f 64 4b 52 51 66 4a 43 6c 56 4f 4c 51 47 6a 58 63 51 72 76 52 49 61 73
73 4b 6f 6d 5f 63 22 3b | xxd -p -r
/mega.nz/file/Qjdj2ZjL#1yP_ppE8W4TXWOdKRQfJClVOLQGjXcQrvRIassKom_c";araisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/apaweh
/word$
```

Setelah di buka ada file mynotes.zip extract lagi ketemu file secure.7z. Disini bagian part sulit nya setelah beberapa saat mencoba saya menyadari ada bagian crc32 yg bisa diidentify karena hanya satau karakter per file txt




| Name | Size | Packed | Type | Modified | CRC32 |
|---|---|---|---|---|---|
| .. | | | File folder | | |
| char (1).txt * | 1 | 4.032 | Text Document | 23/07/2024 12:08 | 1C630B12 |
| char (2).txt * | 1 | 0 | Text Document | 23/07/2024 12:08 | 6C09FF9D |
| char (3).txt * | 1 | 0 | Text Document | 23/07/2024 12:09 | 6DD28E9B |
| char (4).txt * | 1 | 0 | Text Document | 23/07/2024 12:09 | 06B9DF6F |
| char (5).txt * | 1 | 0 | Text Document | 23/07/2024 12:09 | 0862575D |
| char (6).txt * | 1 | 0 | Text Document | 23/07/2024 12:09 | 83DCEFB7 |
| char (7).txt * | 1 | 0 | Text Document | 23/07/2024 12:09 | 856A5AA8 |
| char (8).txt * | 1 | 0 | Text Document | 23/07/2024 12:09 | 84B12BAE |
| char (9).txt * | 1 | 0 | Text Document | 23/07/2024 12:09 | F4DBDF21 |
| emoji (1).txt * | 4 | 0 | Text Document | 21/07/2024 13:40 | 16212D12 |
| emoji (2).txt * | 4 | 0 | Text Document | 21/07/2024 13:41 | 929F6CCC |
| emoji (3).txt * | 4 | 0 | Text Document | 21/07/2024 13:42 | 689051AF |
| emoji (4).txt * | 4 | 0 | Text Document | 21/07/2024 13:41 | 6FFD95B6 |
| emoji (5).txt * | 4 | 0 | Text Document | 23/07/2024 09:45 | 855FD5BF |
| emoji (6).txt * | 4 | 0 | Text Document | 23/07/2024 09:37 | CAF720DD |
| emoji (7).txt * | 4 | 0 | Text Document | 23/07/2024 09:37 | 114CE90B |
| emoji (8).txt * | 4 | 0 | Text Document | 23/07/2024 09:37 | E2F59843 |
| emoji (9).txt * | 4 | 0 | Text Document | 23/07/2024 09:37 | 24469190 |
| emoji (10).txt * | 4 | 0 | Text Document | 23/07/2024 09:37 | 53FE7167 |
| fav * | 43.513 | 0 | File | 23/07/2024 12:03 | 15E01590 |
| maybeuneedthis * | 3.314 | 0 | File | 23/07/2024 12:06 | D6ABE667 |

Dari crc32 kita cari output yg mirip dengan hasil crc32 nya,

```
from zlib import crc32
```

```
from binascii import hexlify

import string
import struct

def calc_crc32(data):
    crc = struct.pack(
        '>I', crc32(data.encode()) % (1<<32)
    )

    return hexlify(crc)

charset = string.ascii_letters + string.digits
for c in charset:
    print(c, calc_crc32(c))
```

Didapat lah hasil setelah di identify satu-satu
😘w😋r😕3😑c🙃k😶1😜t😎5🤭0😵
Lalu kita extract dan berhasil ternyata hamdalah wee
Dari hasil maybeuneedthis masih corrupt sehingga diperbaiki dulu

```
with open('maybeuneedthis', 'rb') as f:
        raw = f.read()

def restore(data):
        if len(data) == 4:
        return bytes([data[1], data[0], data[3], data[2]])
        else:
        return bytes([data[1], data[0]])

result = bytearray(
        b''.join(restore(raw[i:i+4]) for i in range(0, len(raw), 4))
)

with open('flag.png', 'wb') as f:
        f.write(result)
```

Dari hasil fav terdapat hint

```
(c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (c^_^o)+ (ﾟДﾟ)[ﾟ
εﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+
(ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (o^_^o))+ (c^_^o)+ (ﾟДﾟ)[ﾟ
εﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟ
εﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+
((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o)
+(o^_^o))+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟ
Θﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟ
Θﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ ((o^_^o)
+(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟ
Θﾟ))+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (o^_^o))+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟoﾟ]) (ﾟ
Θﾟ)) ('_');
```

aadecode

```
alert(`Follow these steps:

1. Go to canva.com and create an image with the size of 300x300 pixels with a white background.
2. Add text with the font Open Sans, size 14.9.
3. Insert this text:

sdAsWadaRkjda5jh&Ss{2hB8_kln8A9bdjEeliGjAoCj_owS}laKnckasITklas6lkfj4Afja56v0mk}
nS{jtqhwpEihrkqugfjkadnckasnckalscnjabfjkbau;WHDaiosn1scbnjk;asbk;hduihawn_dksndklansfjUbvdv;akjdbv;aAi
bidfniawWnibfwibfawnflk_nsknasjk;bajsbfjasUfjbfjkwb;iabfjXsbkfnajeubfjabwfkaNflkjaeilfhasdjfb0ksnfl{}
wjkflhdfqwhweurhahkasdjs3ncjdcd1jf6has2d3

4. Place the text exactly in the center, both horizontally and vertically.
5. Align the text as justified.
`);
```

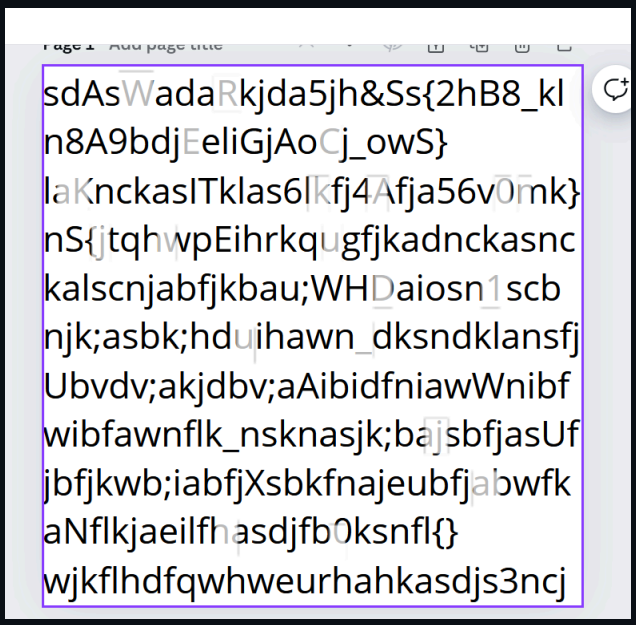
Ada hint seperti ini

1. Go to canva.com and create an image with the size of 300x300 pixels with a white background.
2. Add text with the font Open Sans, size 14.9.
3. Insert this text:

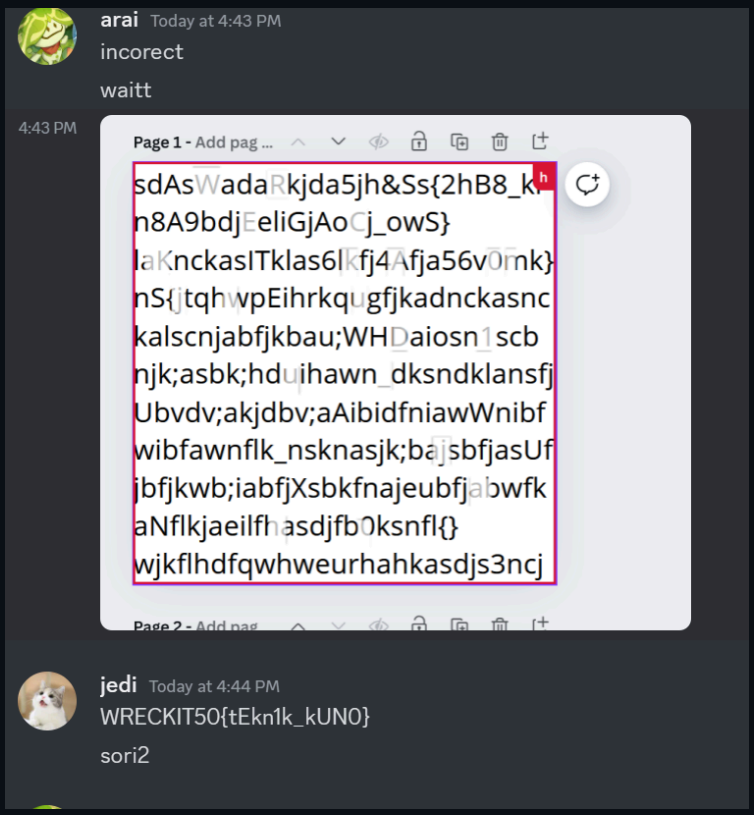
sdAsWadaRkjda5jh&Ss{2hB8_kln8A9bdjEeliGjAoCj_owS}laKnckasITklas6lkfj4Afja56v0mk}nS{jtqhwpEihrkqugfjkadnckasnckalscnjabfjkbau;WHDaiosn1scbnjk;asbk;hduihawn_dksndklansfjUbvdv;akjdbv;aAibidfniawWnibfwibfawnflk_nsknasjk;bajsbfjasUfjbfjkwb;iabfjXsbkfnajeubfjabwfkaNflkjaeilfhasdjfb0ksnfl{}wjkflhdfqwhweurhahkasdjs3ncjdcd1jf6has2d3

4. Place the text exactly in the center, both horizontally and vertically.
5. Align the text as justified.

Lalu setelah saya mikir dengan dalam  ternyata pake canva abis itu masukin image nya ke canva supaya keliatan flag nya




Saya tanya ke temen karena saya ga keliatan




`Flag : WRECKIT50{tEkn1k_kUN0}`

# Cryptography

## m4K c0MbL4n6 (100 pts)

**Deskripsi**

aku lagi jomblo. tolong carikan aku jodoh

Thanks to hash designer & attacker: @hakim01a (IG) & @yudik_suta (IG)

Connected to : nc 188.166.247.108 6969
alt: nc 13.212.238.29 6969

Author : ac3

**Attachment**

*propietary.py*

```python
import math

... # truncated
def convert_to_32bit_hex(input_hex):
    input_int = int(input_hex[:8], 16)  # Ambil 8 digit pertama jika lebih panjang dari 8 digit
    bit_string = format(input_int, '032b')  # Konversi integer ke 32 bit biner dengan leading zeros

    return bit_string


# Fungsi hash HORTEX
def HORTEX(input_hex):
    X_bin = convert_to_32bit_hex(input_hex)
    pad_len = (64 - (len(X_bin) % 64)) % 64
    X_padded = X_bin + '1' + '0' * (pad_len - 1)

    r, c = 64, 192
    state = '0' * (r + c)

    state_int = int(state[:r], 2)
    block_int = int(X_padded, 2)
    updated_state = format(state_int ^ block_int, '064b') + '0'*c
    after_abs = transform_f(updated_state)

    s0 = transform_f(after_abs)
    h1 = s0[:r]
    state = transform_f(s0)
    h2 = state[:r]

    h1_hex = format(int(h1, 2), '016x')
    h2_hex = format(int(h2, 2), '016x')
    return h1_hex + h2_hex
```

*chall.py*

```
from propietary import *
def print_diagram():
    diagram = """
    Sistem Penjodohan oleh Mak Comblang. Semoga cocok :)
    """

    print(diagram)

if __name__ == "__main__":
    print_diagram()



while True:
       X_hex = input('choose your man (hex): ')
       Y_hex = input('choose your woman (hex): ')

       hash_value1 = HORTEX(X_hex)
       hash_value2 = HORTEX(Y_hex)

       if hash_value1 == hash_value2 and X_hex != Y_hex:
              print("New couple is matched :). Here your flag WRECKIT50{REDACTED}")
              break
       else:
              print("Try again")
              break
```

**Solution**

Ketika menyelesaikan challenge ini, file pertama yang dibaca adalah *chall.py*. Sekilas untuk mendapatkan flag, kita harus membuktikan adanya *hash collision* pada fungsi hash HORTEX. Namun ketika diperhatikan input dalam bentuk hex dan ketika pengecekan tidak dilakukan sanitasi seperti pengecekan nilai hex, maka hal ini dapat dieksploitasi. Jika nilai X_hex adalah “00” dan nilai Y_hex adalah “0000”, maka hasil perhitungan hex akan sama, karena keduanya adalah null bytes. Hal ini terjadi karena pada fungsi hash HORTEX, langkah pertama yang dilakukan adalah meng-konversi nilai menjadi bentuk 32bit hexdigit. Maka nilai “00” dan “0000” akan menghasilkan nilai yang sama ketika masuk ke dalam fungsi convert_to_32bit_hex(). Nilai di awal sudah sama, maka hasil akhir akan menjadi sama.

Proof of Concept

```
Python 3.11.2 (main, May  2 2024, 11:59:08) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> from propietary import HORTEX
>>> HORTEX("00")
'b8942df66d70d949ea90c5b39bfce674'
>>> HORTEX("0000")
'b8942df66d70d949ea90c5b39bfce674'
>>>
```

Screenshot

```
patsac ~/ctf/2024/wreckit/qual/cry/makcomblang
➜ ./nc.sh

    Sistem Penjodohan oleh Mak Comblang. Semoga cocok :)

choose your man (hex): 00
choose your woman (hex): 0000
New couple is matched :). Here your flag WRECKIT50{fUnCt10n_Sh0uLd_nOt_13Ij3cT1On}
patsac ~/ctf/2024/wreckit/qual/cry/makcomblang
➜
```

Flag : WRECKIT50{fUnCt10n_Sh0uLd_nOt_13Ij3cT1On}

# Web

## Oshiku 100

Challenge Sederhana. iya kan?

137.184.250.54:7012

mirror : 146.190.104.208:7012

Author: ZeroEXP

DIberikan sebuah web service whitebox, setelah saya teliti ternyata session nya stored tidak randomly alias dalam string saja syaa langsung ketawa

```
app = Flask(__name__)
app.secret_key = 'os.urandom(8)'

# Database connection
```

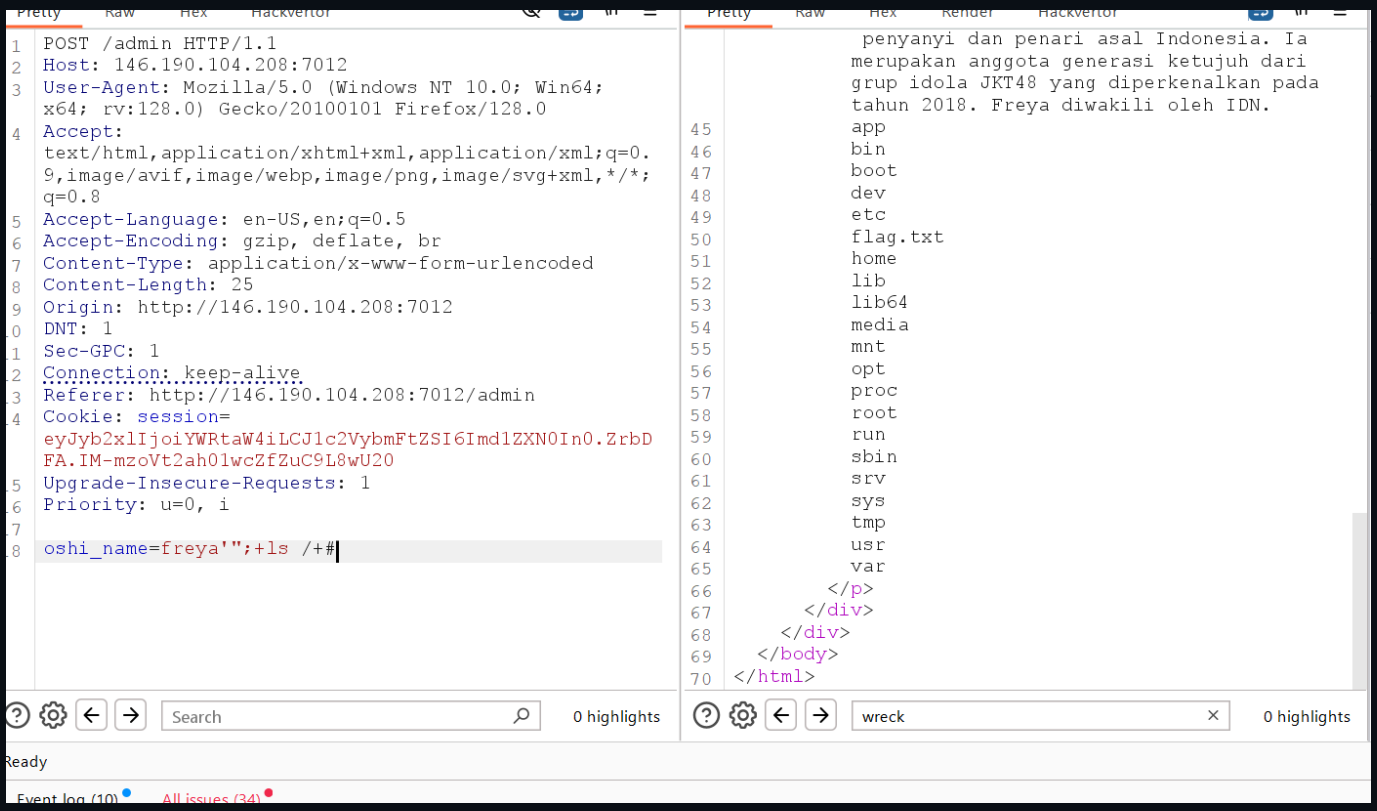
Langsung aja saya sign key dengan role admin

```
araisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/secrets_magic_word/MyNotes/securezip$ flask-unsign --sign --cookie "{'role
': 'admin', 'username': 'guest'}" --secret 'os.urandom(8)'
eyJyb2xlIjoiYWRtaW4iLCJ1c2VybmFtZSI6Imd1ZXN0In0.Zrdi1g.tyR9hR3EmMV0gWw8n1j_60z0A4U
araisantai@LAPTOP-50Q5ECGM:~/Private/ctfs/wreckit/secrets_magic_word/MyNotes/securezip$
```

Setelah itu saya lihat ada  bug sql injection dan command injection

```
DATABASE = "database.db"
def query_database(name):
    query = 'sqlite3 database.db "SELECT biography FROM oshi WHERE name=\'' + str(name) +'\'\"'
    result = subprocess.check_output(query, shell=True, text=True)
    return result

@app.route("/")
```

Saya kira awalnya harus union ternyata langsung aja lewat command injection dari bantuan temen saya patsac


Dapet flask session langsung sqli ternyata command injection

**Flag : WRECKIT50{oshikucumansatukok_satujkt}**

# Reverse Engineering

## Its About Time (100 pts)

**Description :**

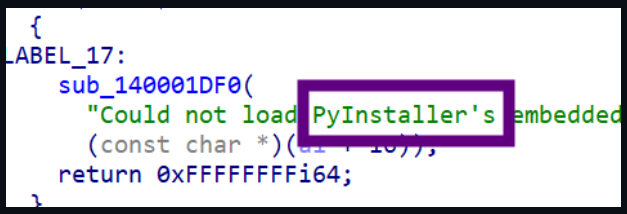
A very usefull app

Author: rafliher

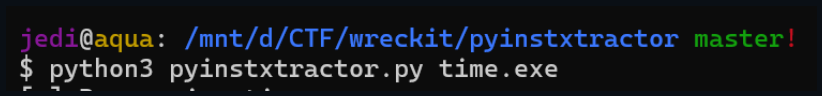
chall.exe

**Solution :**

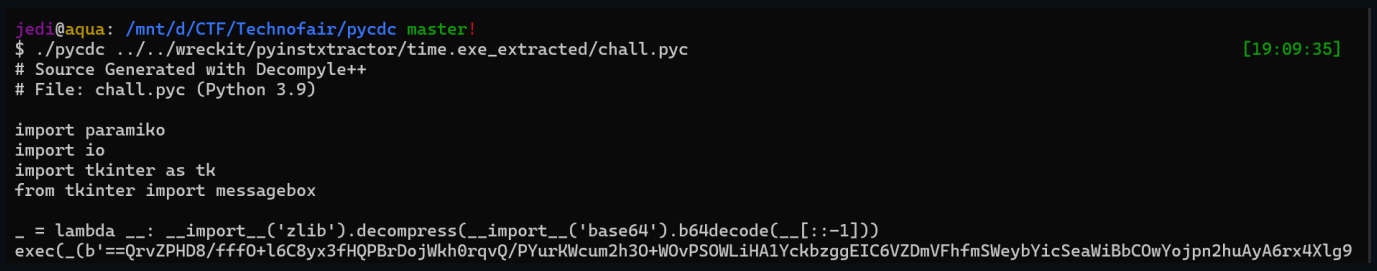
Diberikan suatu file chall.exe. Ketika dibuka dengan ida, saya melihat ada string yang menyebut PyInstaller di dalamnya.



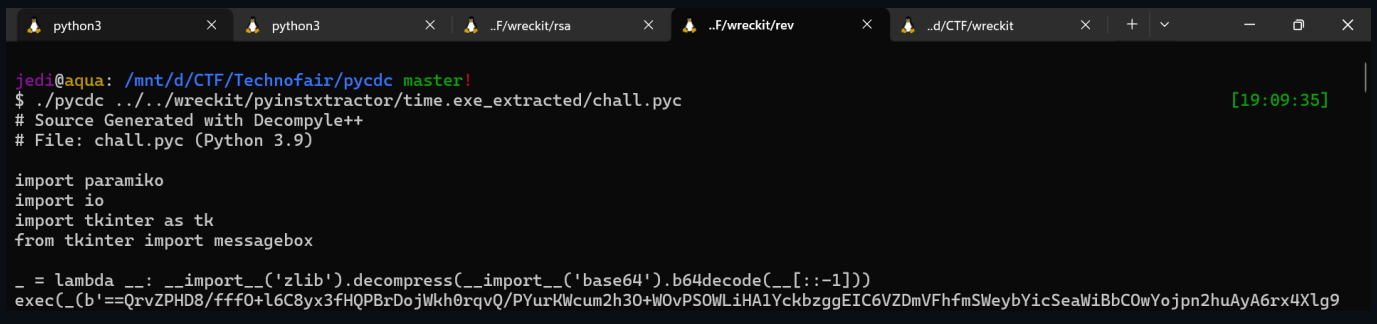

Berarti, kita bisa gunakan pyinstxtractor untuk mengekstrak isinya




Didapatkan suatu file bernama chall.py. Kita gunakan pycdc untuk decompile file tersebut




Ternyata, ada base64 yang di-compress dan dijalankan dengan exec. Kita coba dulu ganti exec dengan print




Dan ternyata isinya adalah kode lain. Saya curiga bahwa kita harus menjalankan kode ini berulang kali sampai ditemukan base code. Jadi saya coba lakukan iterasi sampai tidak ada kode base64

*decode_base64.py*

```
import base64
import zlib
import re

def decode_and_print(encoded_string):
    _ = lambda __: zlib.decompress(base64.b64decode(__[::-1]))
    result = encoded_string
    iteration = 1

    while True:
        try:
            result = _(result)
            match = re.search(rb"b'([^']*)'", result)
            if match:
                result = match.group(1)

            print(f"Iteration {iteration}: {result}")
            iteration += 1
        except:
            print(f"Decoding completed after {iteration - 1} iterations.")
            break

encoded_string = # the base64 code
```

Dan kita mendapatkan ini :

```
1  import paramiko
2  import io
3  import tkinter as tk
4  from tkinter import messagebox
5
6  hostname = "137.184.250.54"
7  port = 7031
8  username = "mack"
9  private_key = """
10 -----BEGIN OPENSSH PRIVATE KEY-----
11 b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
12 NhAAAAAwEAAQAAAgEA24NwXSVAsXP3rmwWL/TspeKDxYzcK1Z6Q38okkjrZbdw031hSLxR
```

Kita bisa melakukan koneksi menggunakan credential yang telah ada di kode (probset menyediakan ip mirror : 13.212.238.29)

Di situ, kita menemukan file flag.txt. Kita tidak bisa menggunakan command “cat” karena permission dari flag.txt 400. Sehingga, saya gunakan base64 untuk membaca filenya (ketika writeup ini ditulis, sepertinya permissionnya sudah diubah karena saya ternyata agak bodoh gak mencoba melakukan pergantian file access permission menjadi 777 atau semacamnya hehe)

```
mack@2b9a14d33fc5:~$ sudo base64 flag.txt
V1JFQ0tJVDUwe3NpYXBheWFuZ3RhdWJlZGFueWFwdWJsaWNrZXlzYW1hcHJpdmF0ZWtleX0=
mack@2b9a14d33fc5:~$ echo V1JFQ0tJVDUwe3NpYXBheWFuZ3RhdWJlZGFueWFwdWJsaWNrZXlzYW1hcHJpdmF0ZWtleX0= | base64 -d
WRECKIT50{siapayangtaubedanyapublickeysamaprivatekey}mack@2b9a14d33fc5:~$
```

**Flag : WRECKIT50{siapayangtaubedanyapublickeysamaprivatekey}**

# Aplikasi Berbasis Objek (140 pts)

**Description :**

Cukup berbeda dari 4.0

Author: aodreamer Download

Pass: wreckit50sanapati

**Solution :**

Diberikan suatu file ABO.apk. Kita gunakan apktool untuk mengektraksi isi dari file apk tersebut

```
jedi@aqua: /mnt/d/CTF/wreckit/rev/ABO
$ apktool d ABO.apk
I: Using Apktool 2.9.3 on ABO.apk
```

Lalu saya menemukan bahwa apk ini dikembangkan menggunakan framework flutter ketika saya buka dengan jadx

```
package com.difrancescogianmarco.example;

import io.flutter.embedding.android.FlutterActivity;
import kotlin.Metadata;

/* compiled from: MainActivity.kt */
@Metadata(d1 = {"\u0000\f\n\u0002\u0018\u0002\n\u0002\u0018\u00
/* loaded from: classes6.dex */
public final class MainActivity extends FlutterActivity {
```

Menurut referensi ini :

https://stackoverflow.com/questions/53666487/flutter-debug-apk-decompile-to-get-the-source-code

Kita bisa mendapatkan source codenya dengan melakukan strings pada kernel_blob.bin. Saya lalu lakukan hal tersebut

```
jedi@aqua: /mnt/d/CTF/wreckit/rev/ABO/ABO
$ strings assets/flutter_assets/kernel_blob.bin > extracted.dart
```

Pada file dart tersebut, ditemukan suatu fungsi dekripsi

```
484259  import 'remote_object.dart';
484260  class Aesenc extends StatefulWidget {
484261    final String passkey;
484262    const Aesenc({super.key, required this.passkey});
484263    @override
484264    State<Aesenc> createState() => _AesencState();
484265  class _AesencState extends State<Aesenc> {
484266    String decryptedText = '';
484267    @override
484268    void initState() {
484269      super.initState();
484270      _decryptText();
484271    void _decryptText() {
484272      final ciphertext = 'UYQ6Ym1peaw1wppjjhm5dhMdZCKHSIKqN3/kVgMHuZW0o7iHCzwIrRky8rDiASkRnFsRBvV9utO
484273      final key = enc.Key.fromUtf8(widget.passkey);
484274      final iv = enc.IV.fromBase64("bmV1ZGd1ZXNzdGhla2V5eQ==");
484275      final encrypter = enc.Encrypter(enc.AES(key, mode: enc.AESMode.cbc, padding: 'PKCS7'));
484276      setState(() {
484277        decryptedText = encrypter.decrypt(enc.Encrypted.fromBase64(ciphertext), iv: iv);
484278      });
```

Dan key-nya didapatkan dari kode bagian ini :

```
class _ProtectedState extends State<Protected> {
  final TextEditingController _passkeyController = TextEditingController();
  String _message = "";
  void _checkPasskey() {
    String passkey = _passkeyController.text;
    print(passkey);
    bool isValidPasskey() {
      if ((passkey[4] != 'r') && (passkey[9] != 'r')) return false;
      if (passkey[11] != '1') return false;
      if (passkey[13] != '3') return false;
      if ((int.parse(passkey[13]) - int.parse(passkey[11])) != 2) return false;

      if (passkey.length != 32) return false;
      if((passkey[3]!='u') && (passkey[6] != 'u')) return false;

      if((9 - int.parse(passkey[15]))!= int.parse(passkey[14])) return false;
      if (passkey.substring(0, 16) != passkey.substring(16)) return false;
      if ((passkey[0] != 's') && (passkey[7] != 's')) return false;
      if (passkey[passkey.length - 1] != '5') return false;
      if((passkey[1] != 'e') && (passkey[5] != 'e') &&(passkey[8] != 'e')) return false;
      if (passkey[2] != 'c') return false;
      if (passkey[16] != 's') return false;
      if (passkey[12] != '2') return false;
      if(passkey[10] != '\$') return false;
      return true;
```

Sehingga, kita bisa reverse kodenya untuk mendapatkan keynya dan melakukan dekripsi

*decode.py*

```python
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad
import base64

def find_passkey():
    passkey = [''] * 32
```

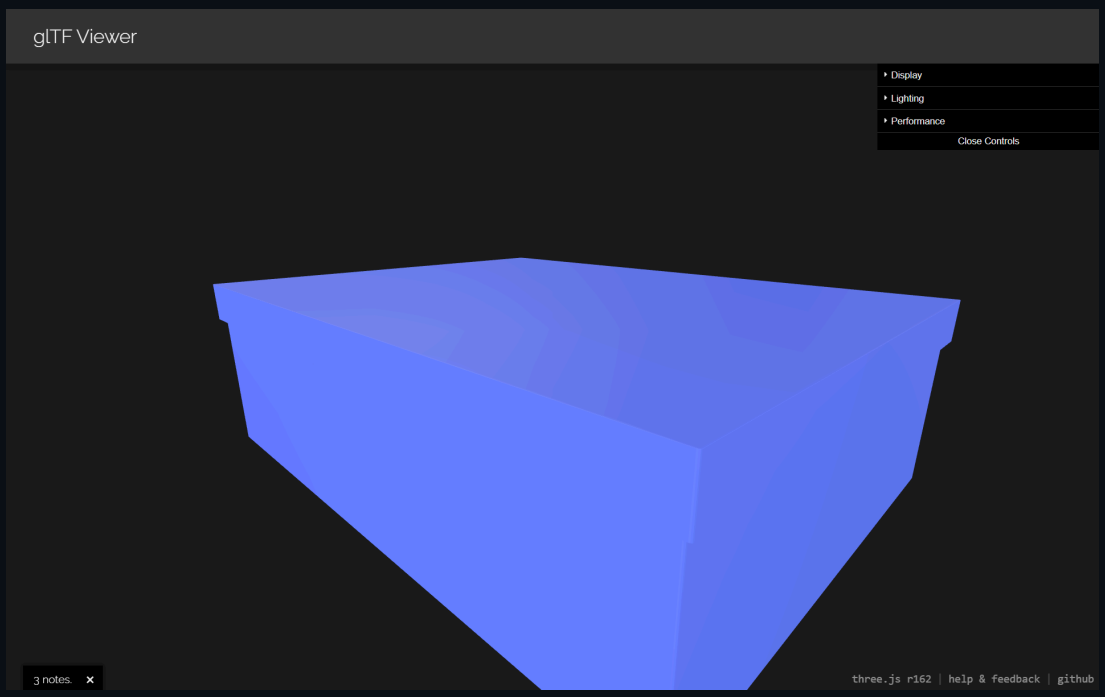
```
    passkey[4] = passkey[9] = 'r'
    passkey[11] = '1'
    passkey[13] = '3'
    passkey[14] = '4'
    passkey[15] = '5'
    passkey[3] = passkey[6] = 'u'
    passkey[0] = passkey[7] = passkey[16] = 's'
    passkey[31] = '5'
    passkey[1] = passkey[5] = passkey[8] = 'e'
    passkey[2] = 'c'
    passkey[12] = '2'
    passkey[10] = '$'

    passkey[16:] = passkey[:16]

    return ''.join(passkey)

def decrypt_text(passkey):
    ciphertext =
'UYQ6Ym1peawlwppjjhm5dhMdZCKHSIKqN3/kVgMHuZW0o7iHCzwIrRky8rDiASkRnFsRBvV9utOl5P6Mn1BmK
w=='
    key = find_passkey().encode()
    iv = base64.b64decode("bmVlZGd1ZXNzdGhla2V5eQ==")

    cipher = AES.new(key, AES.MODE_CBC, iv)
    encrypted = base64.b64decode(ciphertext)
    decrypted = unpad(cipher.decrypt(encrypted), AES.block_size)

    return decrypted.decode('utf-8')

passkey = find_passkey()
print(f"The passkey is: {passkey}")

try:
    decrypted_text = decrypt_text(passkey)
    print(f"Decrypted text: {decrypted_text}")
except Exception as e:
    print(f"Decryption failed: {str(e)}")
```

```
jedi@aqua: /mnt/d/CTF/wreckit/rev/ABO
$ python3 hah.py
The passkey is: secureuser$12345secureuser$12345
Decrypted text: https://github.com/aodreamer/JustADumpRepo/raw/main/f/mod.glb
```

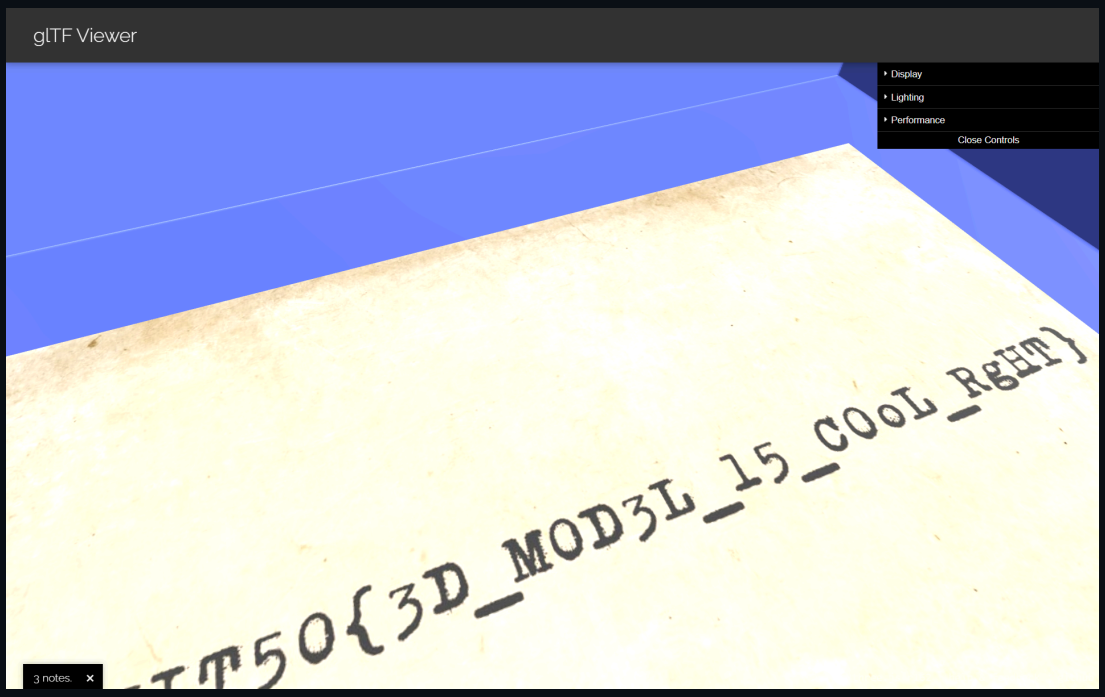
Didapatkan suatu file bernama mod.glb. Ketika dicari tahu, ternyata file ini adalah file glTF yang terkait dengan model 3D

```
jedi@aqua: /mnt/d/CTF/wreckit/rev
$ file mod.glb
mod.glb: glTF binary model, version 2, length 209340 bytes
```

Sehingga, saya coba gunakan gltf viewer berikut : https://gltf-viewer.donmccurdy.com/



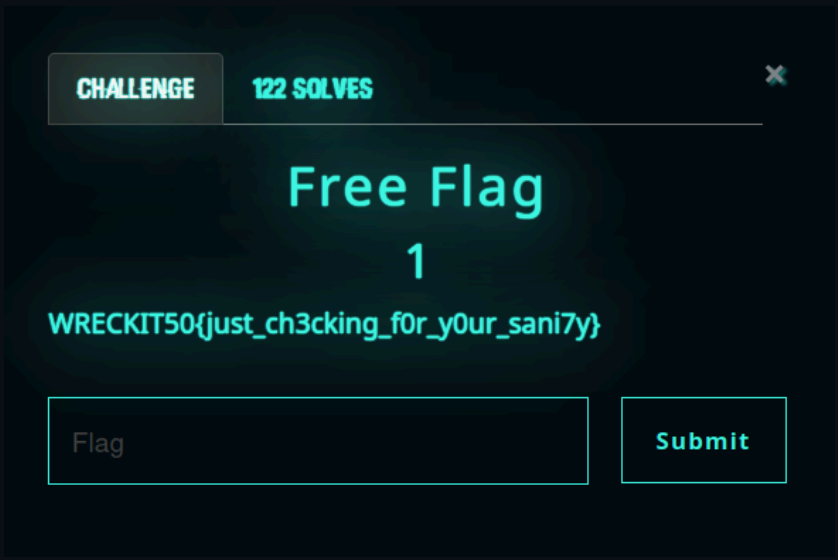

Saya curiga bahwa flag tersebut ada di dalam box, sehingga kita bisa zoom, dan benar saja, ada flag di dalamnya




**Flag : WRECKIT50{3D_M0D3L_15_C0oL_RgHT}**

# Misc

## Free flag (1 pts)




Flag : WRECKIT50{just_ch3cking_f0r_y0ur_sani7y}