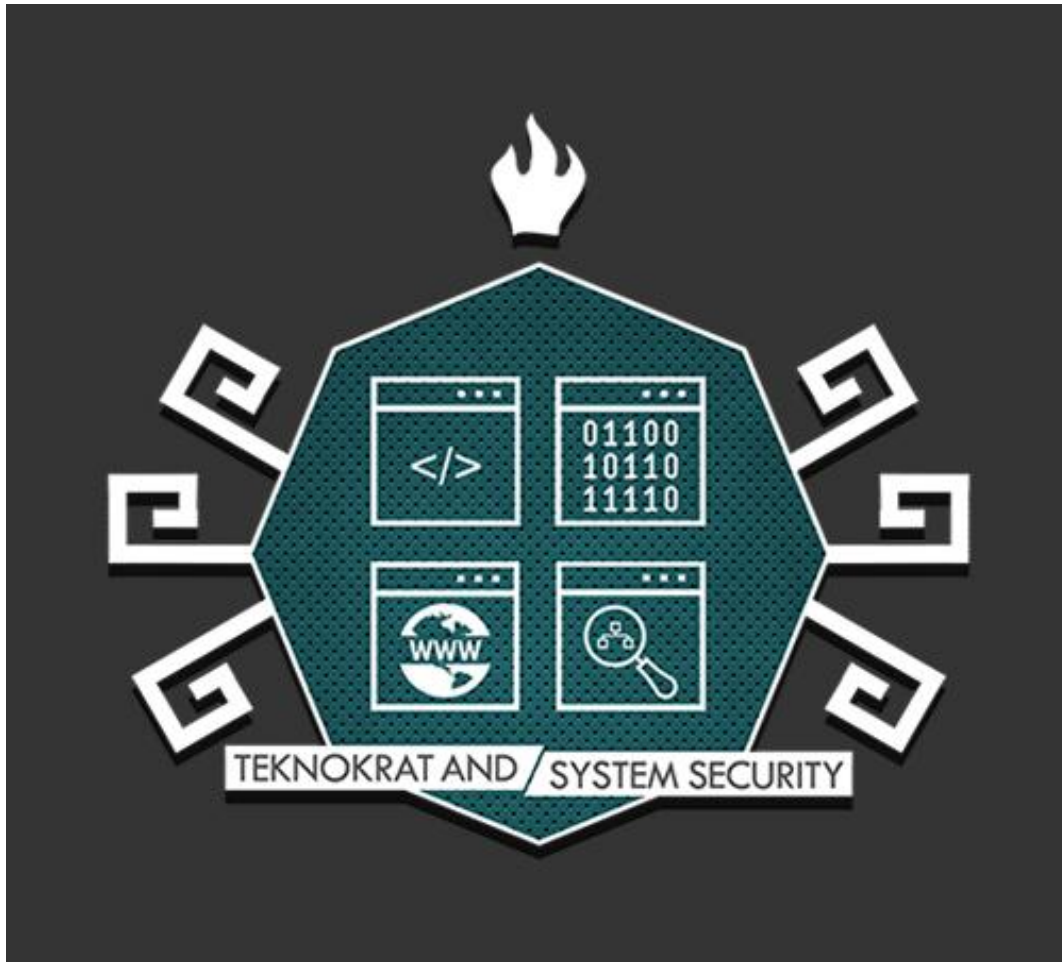


# Writeup UAS Tenesys

## Angkatan 2018



Rexy Fahrezi

## Aku adalah Raja(10)

-Miscellaneous-

Soal :

Diberikan flag yang sudah ter encode sebagai berikut :

CIAKBN{XMZSMVITSIV\_ISC\_ILITIP\_ZIRI\_KIMAIZ}

Solution :

Saya tau itu Caesar cipher karna dari soal nya sudah ada clue “Raja”, Lalu saya decode menggunakan <http://rumkin.com/tools/cipher/caesar.php> , dengan menggunakan geseran sebanyak 18, lalu didapatkan flagnya.

N: 18 ▼

CIAKBN{XMZSMVITSIV\_ISC\_ILITIP\_ZIRI\_KIMAIZ}

This is your encoded or decoded text:

UASCTF{PERKENALKAN\_AKU\_ADALAH\_RAJA\_CAESAR}

Flag : UASCTF{PERKENALKAN\_AKU\_ADALAH\_RAJA\_CAESAR}

## Pesan #1(10)

-Miscellaneous-

Soal :

Pecahkan Misteri ini : UASCTF{1 12 16 8 1 2 5 20 7 15 15 4}

Solution :

Diberikan pesan yang telah di encode dengan A1Z26 Cipher, lalu saya decode secara online menggunakan <https://planetcalc.com/4884/> dan didapatkan flagnya, lalu saya hapus spasinya dan dirubah ke lowercase, sesuai dengan hint soal (No Space & Lower case).

## A1Z26 encoder/decoder

Text

1 12 16 8 1 2 5 20 7 15 15 4

Action

☐ Encode ☒ Decode

CALCULATE

Transformed text

alphabetgood

Flag : UASCTF{alphabetgood}

### Pesan #2(10)

### -Miscellaneous-

Soal :

Pecahkan Misteri ini : 85 65 83 67 84 70 123 107 117 95 116 97 104 117 95 105 110 105 95 104 97 110 121 97 95 100 101 99 105 109 97 108 125

Solution :

Diberikan pesan yang sudah di encode, lalu saya tau itu adalah decimal karna bentuknya hanya angka ,lalu saya decode secara online menjadi text menggunakan <https://v2.cryptii.com/decimal/text> dan didapatkan flagnya.

INTERPRET AS <b>DECIMAL</b> ▼		CONVERT TO <b>TEXT</b> ▼	
Separator		Transform	None
<pre> 85 65 83 67 84 70 123 107 117 95 116 97 104 117 95 105 110 105 95 104 97 110 121 97 95 100 101 99 105 109 97 108 125 </pre>		<pre> UASCTF{ku_tahu_ini_hanya_decimal} </pre>	

Flag : UASCTF{ku\_tahu\_ini\_hanya\_decimal}

### Pesan #3(10)

### -Miscellaneous-

Soal :

Pecahkan Misteri Ini :

5541534354467b616b755f68616e79616c61685f68657861643363696d616c7d

Solution :

Diberikan pesan yang telah di encode ke bentuk hexadecimal, lalu saya decode secara online menggunakan <http://string-functions.com/hex-string.aspx> dan didapatkan flagnya.

### Hex to string converter

Enter the hexadecimal text to decode, and then click "Convert!":

5541534354467b616b755f68616e79616c61685f68657861643363696d616c7d

Convert!

The decoded string:

UASCTF{aku\_hanyalah\_hexad3cimal}

Flag : UASCTF{aku\_hanyalah\_hexad3cimal}

## Camping(10)

## -Miscellaneous-

Soal :

Bercamping sambil pecahkan misteri ini :

VUFTQ1RGe2F5dWtfY2FtcGluZ19iYXJlbmdfYmFzZTY0fQ==

Solution :

Diberikan soal dengan bentuk base64, lalu saya decode menggunakan <https://www.base64decode.org/> dan didapatkan flagnya.

### Decode from Base64 format

Simply use the form below

VUFTQ1RGe2F5dWtfY2FtcGluZ19iYXJlbmdfYmFzZTY0fQ==

**i** For encoded binaries (like images, documents, etc.) upload your data via the [file decode form](#) below.

UTF-8

Source charset.

☐ Live mode OFF

Decodes in real-time when you type or paste (supports only unicode charsets).

**< DECODE >**

Decodes your data into the textarea below.

UASCTF{ayuk\_camping\_bareng\_base64}

Flag : UASCTF{ayuk\_camping\_bareng\_base64}

## Good Job(10)

## -Miscellaneous-

Soal :

Diberikan sebuah gambar yang tidak mencurigakan.



Solution :

Saya hanya meng-check metadata dari gambar tersebut menggunakan exiftool, lalu didapatkan flagnya

```
bio@bio:~/Downloads$ exiftool Good\ Job.jpg
ExifTool Version Number      : 11.16
File Name                    : Good Job.jpg
Directory                   : .
File Size                    : 143 kB
File Modification Date/Time   : 2019:01:06 09:05:59+07:00
File Access Date/Time        : 2019:01:06 09:06:40+07:00
File Inode Change Date/Time   : 2019:01:06 09:06:04+07:00
File Permissions              : rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                  : 1.01
Resolution Unit               : inches
X Resolution                  : 1
Y Resolution                  : 1
Exif Byte Order               : Big-endian (Motorola, MM)
Artist                       : UASCTF{Mantap gan good job}
XP Author                     : UASCTF{Mantap gan good job}
Padding                      : (Binary data 2060 bytes, use -b option to extract)
About                        : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Creator                      : UASCTF{Mantap gan good job}
Image Width                   : 400
```

Flag : UASCTF{Mantap\_gan\_good\_job}

**Troll(10)**

**-Miscellaneous-**

Ini free flag untuk mu , tapi bohong Hiya. Diberikan sebuah ascii art bergambar troll.

**Solution :**

Flag : UASCTF{TR0LL\_bikin\_semua\_happy}

Soal :

benerin trus dapet flag, simple. Diberikan sebuah zip rusak yang tidak bisa di extract.

Solution :

Saya check local file header pada zip tersebut , dan ternyata memang mengalami kesalahan di bagian CRC32 dan nama file didalamnya.

FD theflag.zip	
Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000	50 4B 03 04 14 00 00 00 08 00 CA 42 26 4E CC FE PK.....ÊB&Nìp
00000010	55 17 49 00 00 00 48 00 00 00 0B 00 00 00 69 6E U.I...H.....in
00000020	69 66 6C 61 67 2E 74 78 74 CB 54 48 C9 CF 2B 51 iflag.txtÊTHÉÎ+Q
00000030	C8 CE CB 2F 57 28 CF C8 57 28 55 28 52 48 2A 2D ÈÎË/W(ÎËW(U(RH*-
00000040	51 28 C9 C8 2C 56 00 A2 92 8C 54 85 B4 9C C4 74 Q(ÊË,V.c'ËT...œÄt
00000050	85 50 C7 60 E7 10 B7 EA A8 CC 82 A0 D2 E2 C4 EC ...PÇ`ç.·ê`î, òâÄi
00000060	F8 E2 D4 82 D4 A2 92 CC F8 F8 A4 CC C4 E2 C4 5A œâÔ,Ôc'ÎœœÎÄÄZ
00000070	00 50 4B 01 02 1F 00 14 00 00 00 08 00 CA 42 26 .PK.....ÊB&
00000080	4E CC EF 55 71 48 00 00 00 48 00 00 00 0B 00 24 NîiUqH...H.....\$
00000090	00 00 00 00 00 00 00 20 00 00 00 00 00 00 74 .....t
000000A0	68 65 66 6C 61 67 2E 74 78 74 0A 00 20 00 00 00 heflag.txt.. ...
000000B0	00 00 01 00 18 00 EB EF EB 45 5E A5 D4 01 C9 86 .....ëiëE^¥Ô.É+
000000C0	B5 F1 5D A5 D4 01 C9 86 B5 F1 5D A5 D4 01 50 4B µñ]¥Ô.É+µñ]¥Ô.PK
000000D0	05 06 00 00 00 00 01 00 01 00 5D 00 00 00 71 00 .....]...q.
000000E0	00 00 00 00  ....

Lalu saya edit dan sesuaikan dengan CRC32 & nama file aslinya yaitu theflag.txt

FD theflag.zip	
Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000	50 4B 03 04 14 00 00 00 08 00 CA 42 26 4E CC EF PK.....ÊB&Nîi
00000010	55 71 49 00 00 00 48 00 00 00 0B 00 00 00 74 68 UqI...H.....th
00000020	65 66 6C 61 67 2E 74 78 74 CB 54 48 C9 CF 2B 51 eflag.txtÊTHÉÎ+Q
00000030	C8 CE CB 2F 57 28 CF C8 57 28 55 28 52 48 2A 2D ÈÎË/W(ÎËW(U(RH*-
00000040	51 28 C9 C8 2C 56 00 A2 92 8C 54 85 B4 9C C4 74 Q(ÊË,V.c'ËT...œÄt
00000050	85 50 C7 60 E7 10 B7 EA A8 CC 82 A0 D2 E2 C4 EC ...PÇ`ç.·ê`î, òâÄi
00000060	F8 E2 D4 82 D4 A2 92 CC F8 F8 A4 CC C4 E2 C4 5A œâÔ,Ôc'ÎœœÎÄÄZ
00000070	00 50 4B 01 02 1F 00 14 00 00 00 08 00 CA 42 26 .PK.....ÊB&
00000080	4E CC EF 55 71 48 00 00 00 48 00 00 00 0B 00 24 NîiUqH...H.....\$
00000090	00 00 00 00 00 00 00 20 00 00 00 00 00 00 74 .....t
000000A0	68 65 66 6C 61 67 2E 74 78 74 0A 00 20 00 00 00 heflag.txt.. ...
000000B0	00 00 01 00 18 00 EB EF EB 45 5E A5 D4 01 C9 86 .....ëiëE^¥Ô.É+
000000C0	B5 F1 5D A5 D4 01 C9 86 B5 F1 5D A5 D4 01 50 4B µñ]¥Ô.É+µñ]¥Ô.PK
000000D0	05 06 00 00 00 00 01 00 01 00 5D 00 00 00 71 00 .....]...q.
000000E0	00 00 00 00  ....

Lalu saya extract dan berhasil mendapatkan flagnya.



```
%.....b..ny
...teC b'n'0...{..SP.9...i...I...m'...}...lW.P.5r'...OVR?...w...n3\..w...9...x]
...1...l...S...uBt...e.4.a...V...&K%...A.N...J...m'...}...lW.P.5r'...OVR?...w...n3\..w...9...x]
pt].0...l...3...s.8D.s)...OS...Zc...L...V...jxV...r...w...e...A...m'...{...7s.0...z...qAC...[K.
4"........%,%g2j.U?K...e...o%...U...[...D...D...J...K...%1.f.@...c...b.?E...vgK...
7...-...Z...W...l...r...e...9...g[.3...~...xv...A...~...S).P...[
...+...&M'...D].x...=...3w...h...s.na...8qwf...c...s.J...[.M...l...Gb...j4...[...
[w...m'...4"...?E]...mH...o.C...r
...f.g\...j.K...R...$.H...&...2...I.R...W...j.g...j.../?C...
...P.D.E...@V...MX...q...q...lS...lr..."K"...l
...B...lt...A...G].J...m'B...G.K.EB...w...W...v...
...Q...z...z...u...x...Ov...lK...G...Qn.1j.G...N'.<n.B...Mw...qmK...[...jG...o.PU.
{...P.E...x...b...k...Uq...+
.w...P...#3.0..POST /part/profile/reset-team.php HTTP/1.1
Host: ctf.tenesisys.id
Connection: keep-alive
Content-Length: 60
Accept: */*
Origin: http://ctf.tenesisys.id
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://ctf.tenesisys.id/profile.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,id;q=0.8
Cookie: PHPSESSID=2coj4mcvc32iokeko9vs2r2r42

password-reset-&team-reset-UASCTFX8Sniffing_Is_Very_3asy%7DHTTP/1.1 200 OK
Date: Sat, 05 Jan 2019 18:20:23 GMT
Server: Apache
X-Powered-By: PHP/5.6.38
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Type: text/html; charset=UTF-8
Content-Length: 140
Connection: Keep-Alive
Content-Encoding: gzip

Packet 414, 19 client packets, 46 server packets, 37 turns(s). Click to select.
Entire conversation (50 KB) Show and save data as ASCII Stream 5
Find: UAS Find Next
```

Dan didapatkan flagnya, lalu saya ubah dari UASCTF%7BSniffing\_Is\_Very\_3asy%7D menjadi UASCTF{Sniffing\_Is\_Very\_3asy}

Flag : UASCTF{Sniffing\_Is\_Very\_3asy}

## Black (60)

## -Digital Forensic-

Soal :

Ku Berikan Sebuah Free Flag dengan cuma cuma Link, diberikan sebuah gambar yang mencurigakan dan temukan flagnya.



Solution :

Saya analisis gambar tersebut menggunakan image forensic online, dan saya atur Principal Component Analysis nya menjadi 3 component , dan didapatkan 7 buah barcode.



Lalu saya coba scan barcode qr tersebut satu persatu dan didapatkan flagnya.

Flag : UASCTF{Barc0d3\_QR\_D3ngan\_Kekuatan\_Super\_5ecr3t}

## Look Up Inside(70)

## -Digital Forensic-

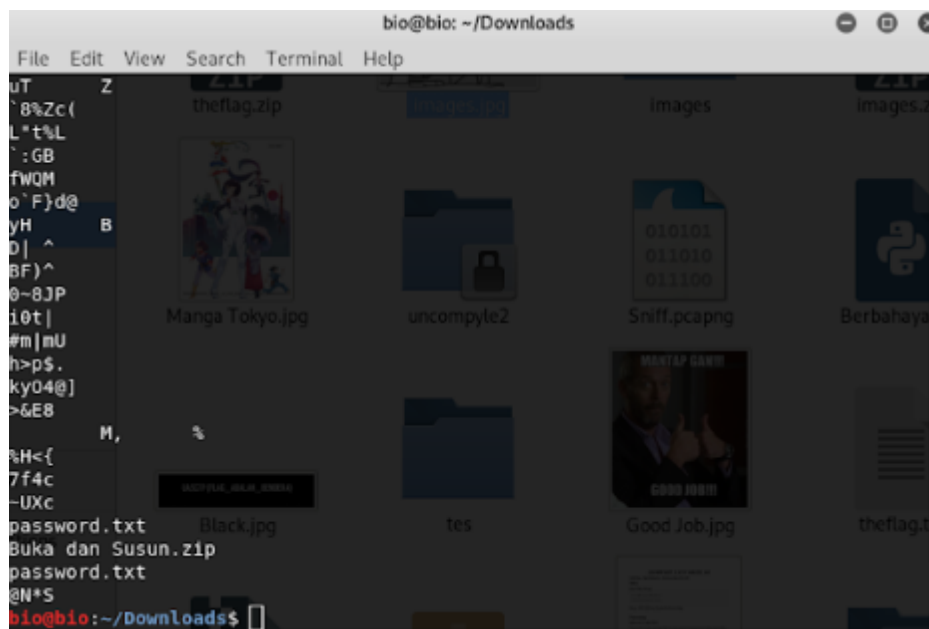
Soal :

Lian berkata "Jika melihat sesuatu janganlah sekedar melihat depannya saja namun lihatlah sampai kedalamnya juga" Link

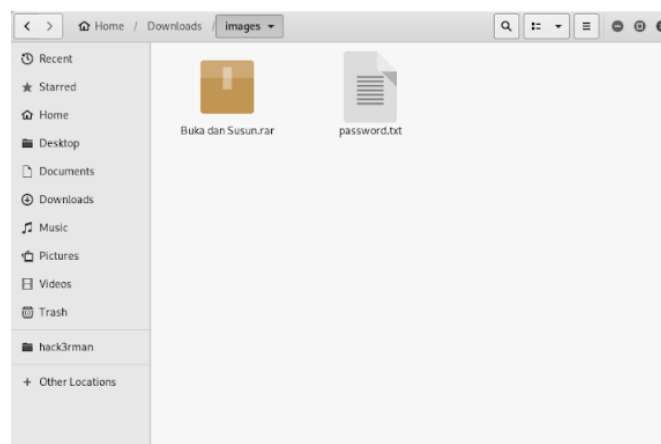
Hint : Kakak Lian diganti kakak hasan

Solution :

Pertama saya coba melihat isi string didalam gambar tersebut, dan ternyata ditemukan file bernama password.txt.



Lalu saya extract gambar tersebut dan didapatkan 2 file, yaitu "Buka dan Susun.zip" dan "password.txt"



Lalu saya coba buka file “buka dan susun.rar” ternyata sudah di password, dan saya buka password.txt ,isinya adalah sebuah base64 ,lalu saya coba decode

**Decode from Base64 format**  
Simply use the form below

---

VUdGemMzZHjpbVJ1ZVdFZ09pQnJZV3RoYTJ4cFIXNTBZVzEyWVc0NmRnPT0=

**1** For encoded binaries (like images, documents, etc.) upload your data via the [file decode form](#) below.

UTF-8

Source charset.

☐ Live mode OFF

Decodes in real-time when you type or paste (supports only unicode charsets).

**< DECODE >**

Decodes your data into the textarea below.

**Organize Pics and Vids**

1 Save, share and playback free with Plex. Download to start sharing now plex.tv

**OPEN**

UGFzc3dvcmRueWEgOiBrYWtha2xpYW50YW12YW46dg==

Dan ternyata hasilnya adalah base64 juga, lalu saya decode lagi

UGFzc3dvcmRueWEgOiBrYWtha2xpYW50YW12YW46dg==

**1** For encoded binaries (like images, documents, etc.) upload your data via the [file decode form](#) below.

UTF-8

Source charset.

☐ Live mode OFF

Decodes in real-time when you type or paste (supports only unicode charsets).

**< DECODE >**

Decodes your data into the textarea below.

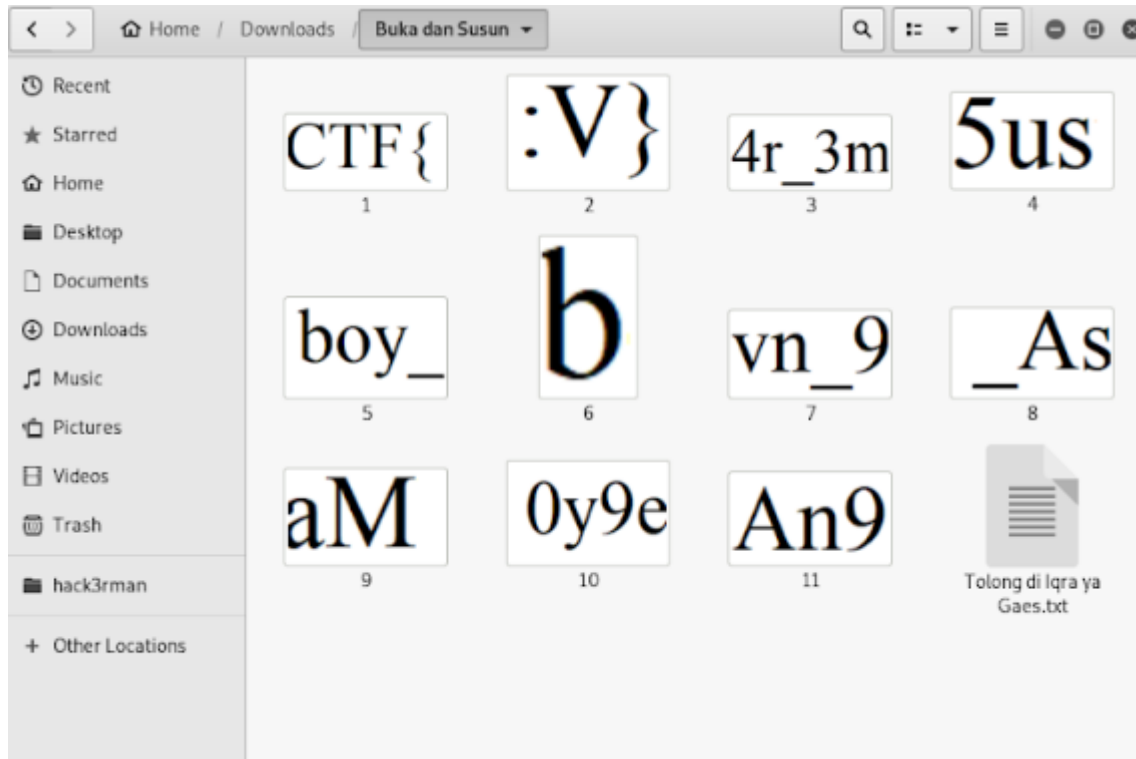
**Organize Pics and Vids**

1 Save, share and playback free with Plex. Download to start sharing now plex.tv

**OPEN**

Passwordnya : kakakliantamvan:v

Dapat passwordnya : kakakliantamvan:v, lalu sesuai hint tadi , jadi saya ganti menjadi kakakhasantamvan:v , dan saya berhasil meng extract rar tadi.



Ternyata isinya adalah flag yang sudah di pecah belah dan harus disusun ulang--

Saya coba buka file txt tersebut dan terdapat clue berupa urutan angka,lalu saya berfikir jika awalnya CTF{ (no1) maka harusnya akhirnya akan :V} (no 2) karna format flag adalah CTF{FLAG} / UASCTF {FLAG} , lalu saya dapatkan urutan tersebut, dan saya susun, dan dapat flagnya.



Flag : CTF{5usvn\_9aMb4r\_3mAn9\_As0y9eboy\_:V}

## Berbahaya (60)

## -Cryptography-

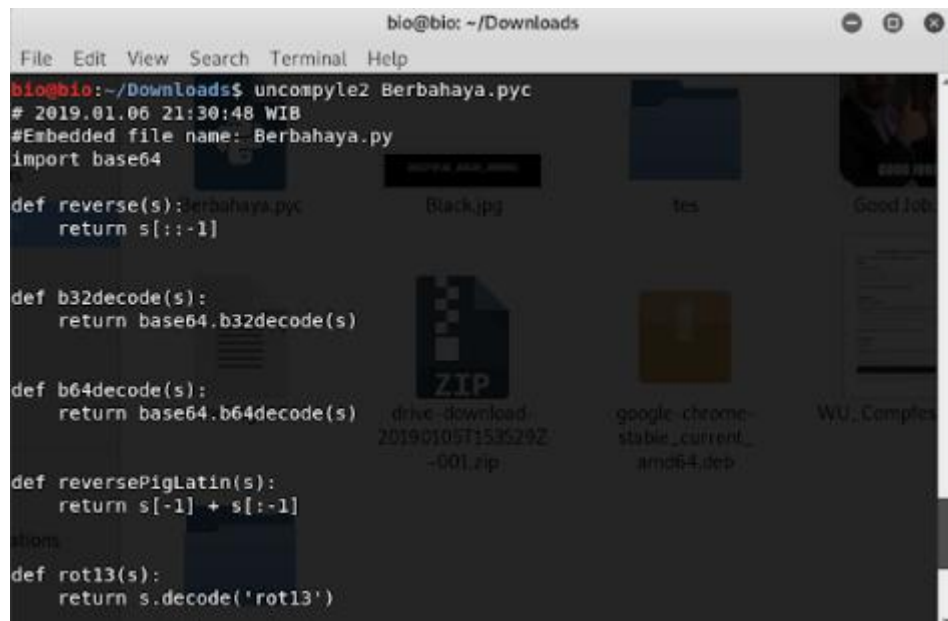
Soal :

Ini adalah File Berbahaya harap berhati hati ! Link

Hint : Decompiler me !

Solution :

Pertama saya decompile dulu file .pyc yang sudah diberikan di soalnya menggunakan uncompyl2



```
bio@bio: ~/Downloads
File Edit View Search Terminal Help
bio@bio:~/Downloads$ uncompyl2 Berbahaya.pyc
# 2019.01.06 21:30:48 WIB
#Embedded file name: Berbahaya.py
import base64

def reverse(s):
    return s[::-1]

def b32decode(s):
    return base64.b32decode(s)

def b64decode(s):
    return base64.b64decode(s)

def reversePigLatin(s):
    return s[-1] + s[:-1]

def rot13(s):
    return s.decode('rot13')
```

Lalu didapatkan sebuah script python berupa pesan yang telah di enkripsi sebanyak 4x

```
bio@bio: ~/Downloads
File Edit View Search Terminal Help

def reversePigLatin(s):
    return s[-1] + s[:-1]

def rot13(s):
    return s.decode('rot13')

def main():
    print 'WARNING!! Ini Sangat Berbahaya !'
    return '===2T6EITKOMUWJMMMD2ETMZGVZRGGTJLOTWET4QNED2UVZALVD60EHFGSS6EGWJJTBVOD
HFGSKUUVVRK'

if __name__ == '__main__':
    s = main()
    print s

+++ okay decompiling Berbahaya.pyc
# decompiled 1 files: 1 okay, 0 failed, 0 verify failed
# 2019.01.06 21:36:20 WIB
bio@bio:~/Downloads$ echo "===2T6EITKOMUWJMMMD2ETMZGVZRGGTJLOTWET4QNED2UVZALVD60EH
FGSS6EGWJJTBVODHFGSKUUVVRK" | rev | base32 --decode | base64 --decode
NFPGS{0reo4u4ln_vav_vfv_pnzchen}Hbio@bio:~/Downloads$
```

Jadi saya copy string yang sudah di enkripsi tersebut di bagian return, lalu saya menggunakan command

```
echo "pesan" | rev | base32 --decode | base64 --decode
```

dimana rev adalah untuk membaca string tersebut secara terbalik ,karna pesan itu sudah dibalik, maka kita harus membalikannya lagi ke awal, lalu setelah pesan tersebut urutannya sudah benar ,kita akan mendapatkan enkripsi base32, setelah itu kita decode ke base64 dan didapatkan sebuah enkripsi ROT13

jadi urutannya :

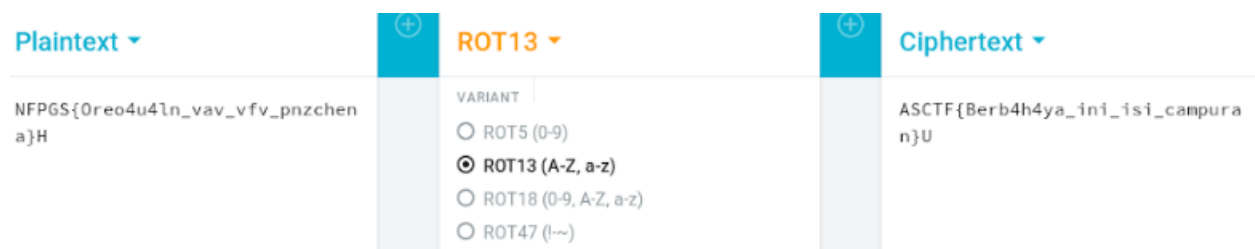
Pertama di reverse string

Kedua di decode base32

Ketiga di decode base64

Keempat di decode ROT13

Dan didapatkan flagnya.



Flag : UASCTF{Berb4h4ya\_ini\_isi\_campuran}

## Raja Berbeda (80)

## -Cryptography-

Soal :

Entah Kenapa Sang Raja mulai berbeda , mari bantu untuk mengembalikan raja kembali Link

Hint : -

Solution :

Pertama kita diberikan sebuah script python untuk meng encode pesan



```
import string

huruf = string.printable

def enkripsi (pesan) :
    global huruf

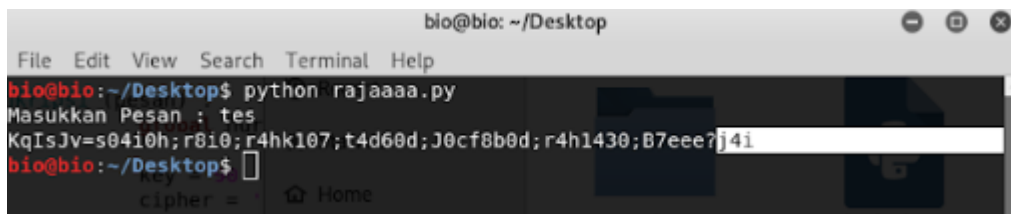
    key = 98
    cipher = 'KqIsJv=s04i0h;r8i0;r4hk107;t4d60d;J0cf8b0d;r4h1430;B7eee?'
    for i in pesan:
        if i in huruf:
            j = huruf.find(i)
            j = (j + key)%100
            cipher = cipher+huruf[j]
        else:
            cipher = cipher + i

    return cipher

if __name__ == '__main__':
    pesan = raw_input('Masukkan Pesan : ')
    print(enkripsi(pesan))

else:
    print(" Mau Flag ya ?")
```

Lalu ketika saya coba jalankan pythonnya , dan memasukan pesan “tes” , pesan tersebut akan ter enkripsi menjadi “j4i”



```
bio@bio: ~/Desktop
File Edit View Search Terminal Help
bio@bio:~/Desktop$ python rajaaaa.py
Masukkan Pesan : tes
KqIsJv=s04i0h;r8i0;r4hk107;t4d60d;J0cf8b0d;r4h1430;B7eee?j4i
bio@bio:~/Desktop$
```

Dan disini kita harusnya mendecode pesan yang ada didalam variable cipher tersebut, jadi script nya saya rubah menjadi seperti ini





```
import string

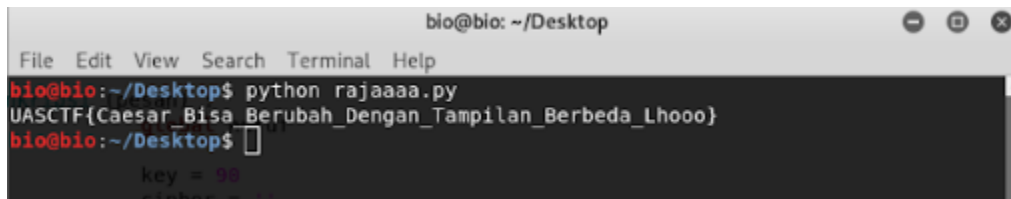
huruf = string.printable

def enkripsi (pesan) :
    global huruf
    key = 98
    cipher = ''
    for i in pesan:
        if i in huruf:
            j = huruf.find(i)
            j = (j - key)%100
            cipher = cipher+huruf[j]
        else:
            cipher = cipher + i
    return cipher

if __name__ == '__main__':
    pesan = ('KqIsJv=s04l0h;r8l0;r4hk107;t4d00d;J0cf8b0d;r4h1430;B7eee?')
    print(enkripsi(pesan))

else:
    print(" Mau Flag ya ?")
```

Lalu saya jalankan pythonnya dan mendapatkan flagnya



```
bio@bio: ~/Desktop
File Edit View Search Terminal Help
bio@bio:~/Desktop$ python rajaaaa.py
UASCTF{Caesar_Bisa_Berubah_Dengan_Tampilan_Berbeda_Lhooo}
bio@bio:~/Desktop$
```

Flag : UASCTF{Caesar\_Bisa\_Berubah\_Dengan\_Tampilan\_Berbeda\_Lhooo}

## Admin Login Dalam Kulit Kacang (40)

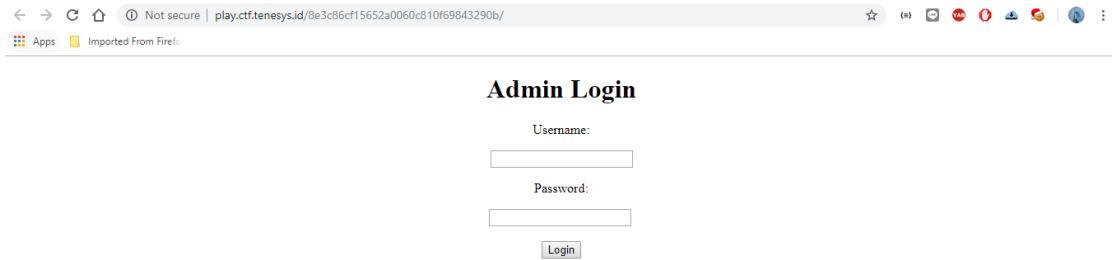
## -Web Exploitation-

Soal :

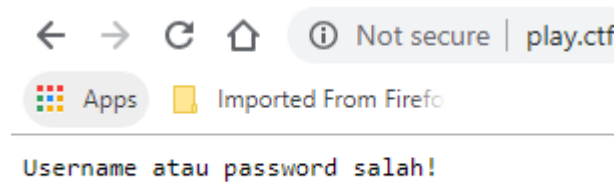
Akses web dan Dapatkan Flagnya

Solution :

Pertama kita diberikan sebuah website untuk login dengan memasukan parameter username dan password



Lalu saya mencoba memasukan username dan password “tes” dan muncul peringatan bahwa data yang dimasukkan salah



Lalu saya coba untuk melakukan sql injection pada form login tersebut dengan menggunakan ini  
username : a  
password : ' or 1=1 limit 1 -- --+

Lalu saya berhasil membypass nya dan mendapatkan flagnya

# Welcome Admin!

**Ini Flag kamu!**

UASCTF{Eeeeeeeeeeeeeeasy\_\_SQLInjection}

Flag : UASCTF{Eeeeeeeeeeeeeeasy\_\_SQLInjection}

## Agent JS (45)

## -Web Exploitation-

Soal :

Akses web hanya dan hanya melalui "Tenesys Computer" untuk mendapatkan flag.

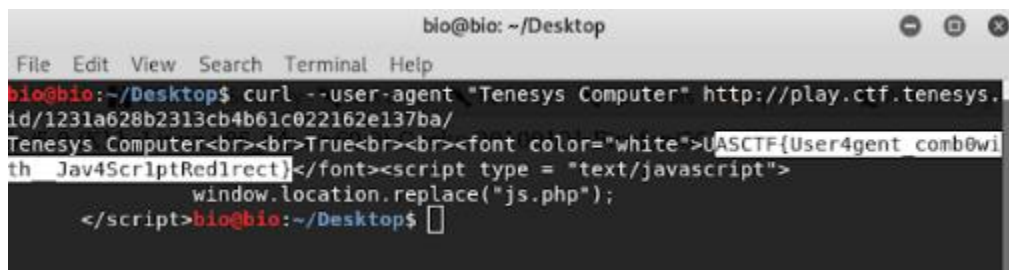
Hint : -

Solution :

Pertama kita diberikan sebuah link website, lalu saat saya buka muncul seperti ini

```
Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0  
False
```

Saya baru mengerti setelah melihat kembali Nama dan Deskripsi soal ,kita diberikan clue yaitu "Agent" dan "Tenesys Computer" ,jadi saya mencoba mengubah user agent nya menjadi tenesys computer menggunakan curl dan saya mendapatkan flagnya.

A screenshot of a terminal window titled 'bio@bio: ~/Desktop'. The terminal shows a curl command being executed: 'curl --user-agent "Tenesys Computer" http://play.ctf.tenesys.id/1231a628b2313cb4b61c022162e137ba/'. The output of the command is displayed in a monospaced font, showing the user agent string 'Tenesys Computer' and a flag 'UASCTF{User4gent\_comb0with\_Jav4Scr1ptRed1rect}' in white text on a black background. The terminal also shows a JavaScript snippet: 'window.location.replace("js.php");'.

Flag : UASCTF{User4gent\_comb0with\_Jav4Scr1ptRed1rect}