

Author : Jayesh Jaiswal; Atharva Gawas.

Title : Aaj Wednesday Hai...

Category : Miscellaneous

Git-Hub Links :

<https://github.com/Jayesh-2003>

<https://github.com/ATHARVA-GAWAS>

Category : Miscellaneous

Description : oh my god EOF.

Flag : VishwaCTF{_sinclair_addams_barclay_petropolis_walker_galpin_thornhill_weems}

Writeup

1] We can see little bit text in image soo try changing its brightness and contrast.Inorder to see the text clearly.



We can see it like this



Text – “<https://t.me>” find other half of me also you may get 1st part of flag in image in image

soo we can get that the other half is in image, soo it is in the HEX data of image and also as the file name suggest check up to end of file soo check the ends in jpg

we can see that after the end of jpg file that is FFD9 the file doesn't end we can see a png image HEX data starts.

also scrolling to total end we can see half bot link i.e “/nachrai69_bot”

00021940	00	00	00	00	00	4C	08	60	00	00	00	00	00	00	80	09L`....ç.
00021950	01	0C	00	00	00	00	00	00	30	21	80	01	00	00	00	000!ç.....
00021960	00	00	26	04	30	00	00	00	00	00	00	C0	84	00	06	00	.&.0.....Lä..
00021970	00	00	00	00	00	98	08	59	5F	39	57	83	31	63	74	00ÿ.Y_9Wälct.
00021980	00	00	00	49	45	4E	44	AE	42	60	82	2F	6E	61	63	68	...IEND«B`é/nach
00021990	72	61	6A	36	39	5F	62	6F	74	+							raj69_bot

2] Concatenating the bot parts we get link as “https://t.me/nachraj69_bot” this link will not open in browser as its a telegram link so for converting it for browser by adding telegram in place of t in [t.me](https://t.me/nachraj69_bot)

Soo the link becomes “https://telegram.me/nachraj69_bot”

Now we know that 1st part of flag is in image so as we seen that at end of file that is FFD9 there is png file so extracting it by writing a python code for converting HEX to image after FFD9

```
import PIL.Image
import io
with open("ki.jpeg","rb") as f:
    content=f.read()
    offset=content.index(bytes.fromhex('FFD9'))

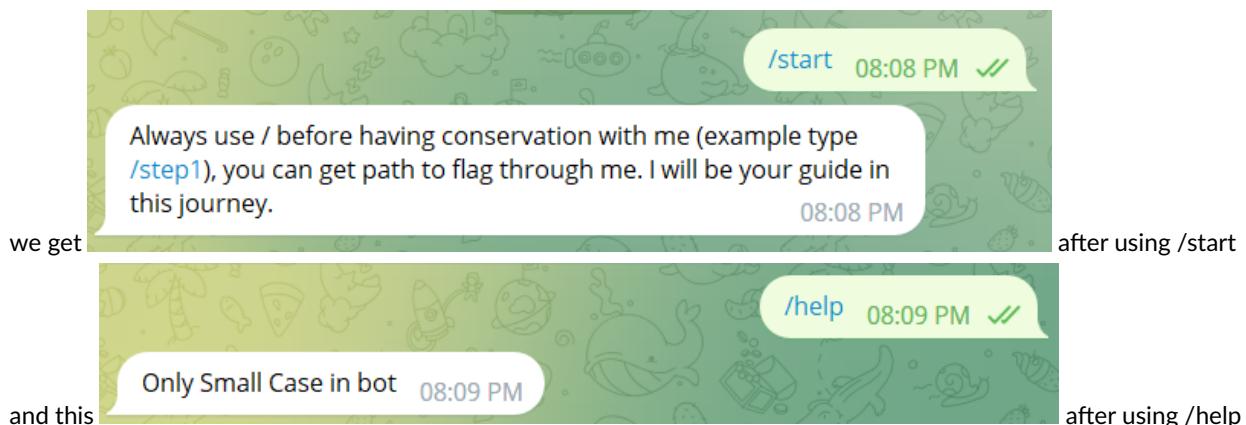
    f.seek(offset+2)
    new_img = PIL.Image.open(io.BytesIO(f.read()))
    new_img.save("new_image.png")
```

Congrats we got first part of flag “_sinclair_addams_barclay”

_sinclair_addams_barclay

3] Now moving towards Telegram bot

As we now basic commands that work on Telegram bots like /start and /help



4] as given after /start “Always use / before having conservation with me (example type /step1), you can get path to flag through me. I will be your

guide in this journey.”

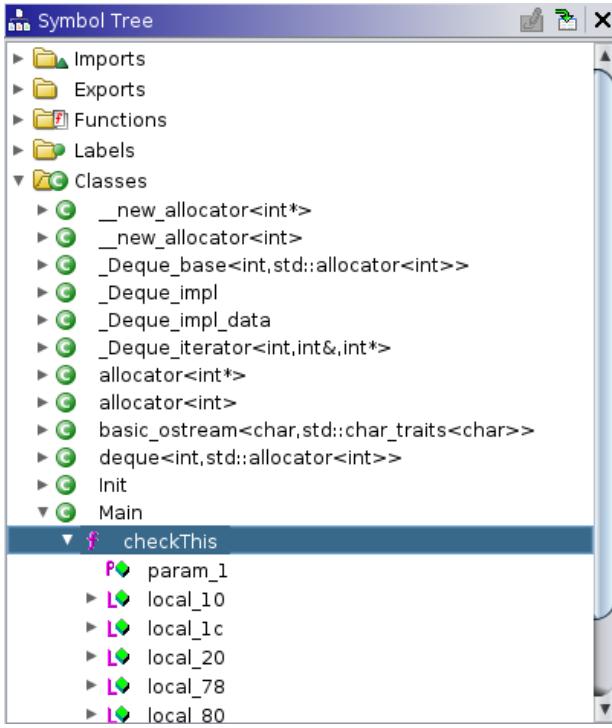
soo typing /step1 we get



opening this link “<https://shorturl.at/guEFY>”

we will get a CPP output executable, after running it we get “This is a coding question and Guess Its Name from Leetcode website,which concepts from english it checks? Type name of concept in bot.1”

5] Analyzing it with ghidra, opening main class and a function made in it



```

/* Main::checkThis(int) */

undefined8 __thiscall Main::checkThis(Main *this,int param_1)

{
    int iVar1;
    int *piVar2;
    undefined8 uVar3;
    int local_84;
    stack<int,std::deque<int,std::allocator<int>>> local_78 [88];
    int local_20;
    int local_1c;

    std::stack<int,std::deque<int,std::allocator<int>>>;
    stack<std::deque<int,std::allocator<int>>,void>(local_78);
    local_84 = param_1;
    iVar1 = param_1;
    if (param_1 < 0) {
        uVar3 = 0;
    }
    else {
        for (; local_1c = iVar1, local_84 != 0; local_84 = local_84 / 10) {
            local_20 = local_84 % 10;
            /* try { // try from 00101383 to 00101387 has its CatchHandler @ 0010143b */
            std::stack<int,std::deque<int,std::allocator<int>>>::push(local_78,&local_20);
            iVar1 = local_1c;
        }
        for (; local_1c != 0; local_1c = local_1c / 10) {
            piVar2 = (int *)std::stack<int,std::deque<int,std::allocator<int>>>::top();
            if (*piVar2 != local_1c % 10) {
                uVar3 = 0;
                goto LAB_0010142b;
            }
            std::stack<int,std::deque<int,std::allocator<int>>>::pop(local_78);
        }
        uVar3 = 1;
    }
LAB_0010142b:
    std::stack<int,std::deque<int,std::allocator<int>>>::~stack(local_78);
    return uVar3;
}

```

Doing some reversing techniques and analysing what is hapening with variables we can get that function is used to check the concept of palindrome from english. typing that concept in bot gives



we get a link "<http://shorturl.at/HKLOY>"

6] Opening this link we get a music file in which voice says “who is she, type her name in the bot once you find her also the second part of flag is in the picture also their are many secrets in audio”

using string we can get that something is in its metadata

```
LIST
INFOINAM"
Wednesday's child is full of woe
ICMTz
first name of person who is hyde in the Show uck.wav
one of dialogue of show is given as title or track name is the passphrase
ID3
vCOMM
TIT2
WXXX
https://youtu.be/z4t2\_6SFiPo
```

so checking mediainfo we get

MediaInfo v21.03

Details About

 you_suck.wav

General

Complete name	:	J:\CTF\you_suck.wav
Format	:	Wave
File size	:	2.09 MiB
Duration	:	49 s 600 ms
Overall bit rate mode	:	Constant
Overall bit rate	:	354 kb/s
Track name	:	Wednesday's child is full of woe
Comment	:	What is the first name of the person who plays Hyde in the show is the passphrase. / (Hint- one of the dialogues from the show that has been used as a title or track name)
URL	:	https://youtu.be/z4t2_6SFiPo

Audio

Format	:	PCM
Format settings	:	Little / Signed
Codec ID	:	1
Duration	:	49 s 600 ms
Bit rate mode	:	Constant
Bit rate	:	352.8 kb/s
Channel(s)	:	1 channel
Sampling rate	:	22.05 kHz
Bit depth	:	16 bits
Stream size	:	2.09 MiB (100%)

[Save to text file](#)

OK

as we can see in comment

"first name of person who is hyde in the Show / one of dialogue of show is given as title or track name is the passphrase"

soo the title which is "Wednesday's child is full of woe" is dialogue of Wednesday Webseries and the first name of hyde is tyler and using steghide extract the hidden text.

```
└─[krish㉿kali]-[~/Desktop]
$ steghide extract -sf you_suck.wav
Enter passphrase:
the file "2ndPart.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "2ndPart.txt".
```

7] After doing some research about text we can get its a base64 form of image(also as indicated that there is a image in audio somewhere) so after converting it we get

Base64 to Image

 Add to Fav

Enter Base64 String

Op4+7970QY4uWs7F3qUbQsTM0i0B79rWuHwtaK21790DLbzHFjtaOgCSM0Wyxy
/Dy7x3JNjaPnPnFoL3SxSF3udwselU1JpebB4l0PZKGSRPGyaJ/RknqPS1cfIw42+HNTNfkavv
/AJtXlXhnWZ9H1SN0YD4pnCOWJx4e0n+vusuTMoZEVT0qj4zyYG1
/ZM2eteDHeF8P8Rh5DsvRctwilik5fISn8pPqr3HoVloHB104Ag0V69Jp8eZp2bgyOf5f
/SJHUjgj7LyGfCGHm5EakL/AC5C3cR15QmlB
/XwHFKWRPv5LWTEfihzZWg1yKwC1IGMEbrUt+rJD8LXGunKqdSlc4G0MuWPQt42CSnb8FLlvtxEEmyp
GS74ioxK4s3bPQRVi5GjbSGwWpDBQQiIMi3gJS4BN7WhPcrLoSjnyWmA2mE2U4Ktx6CMNlzHIDUvleLF

Size : 46.71 KB, 47828 chars

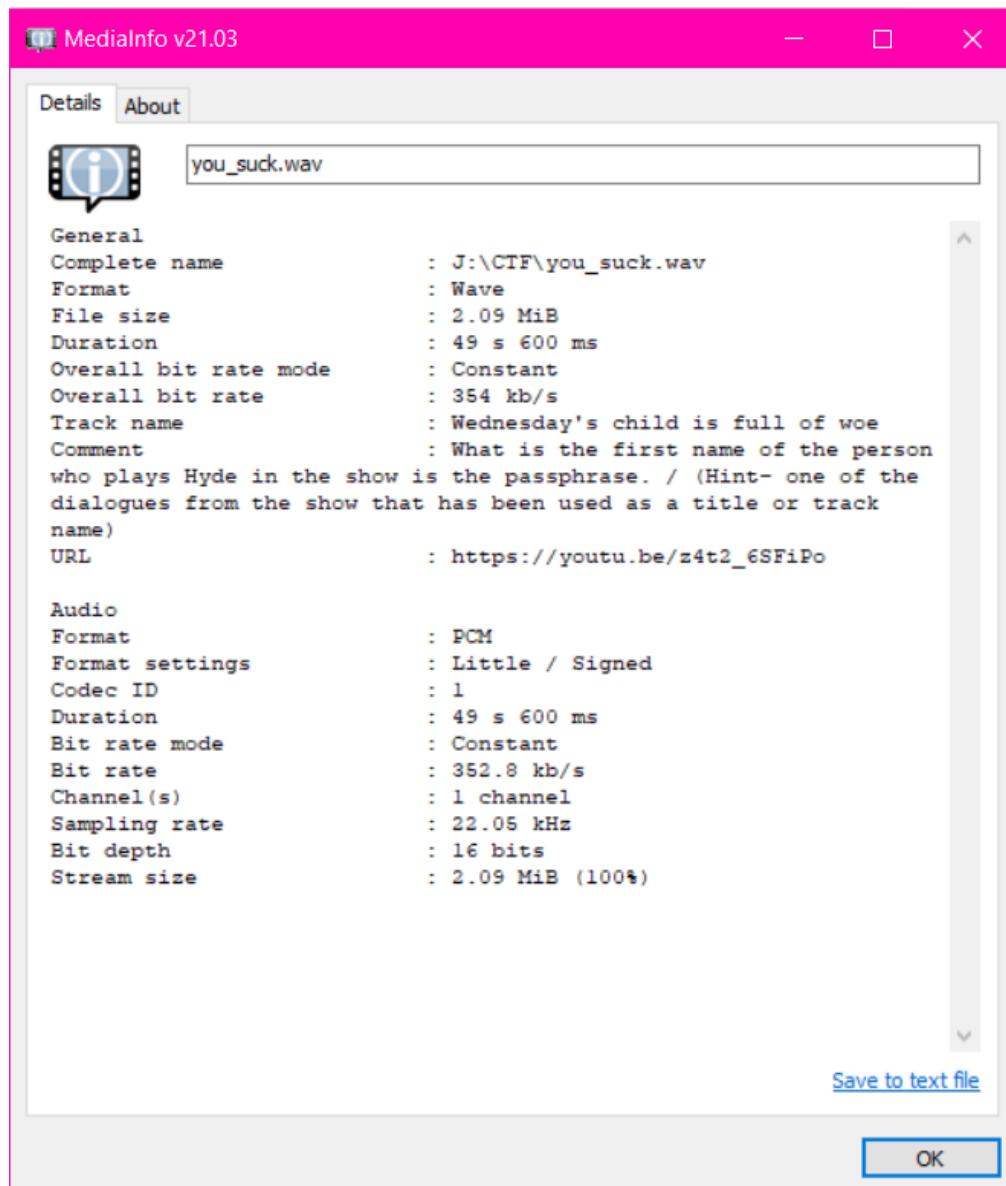


[Download Image](#)

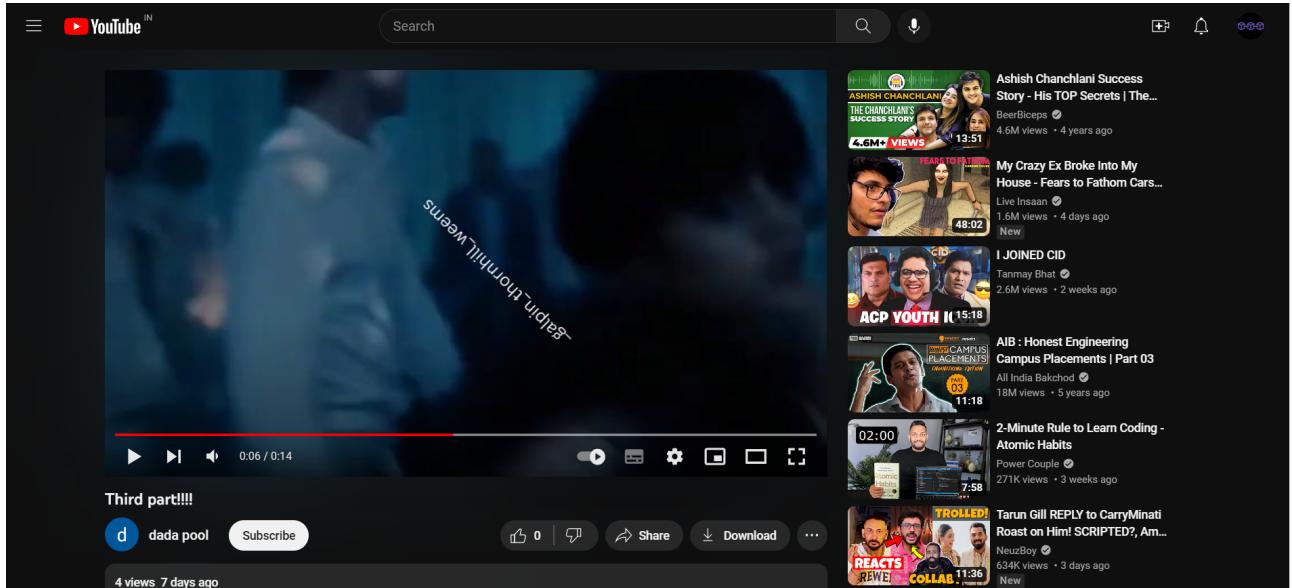
After some research we can find that her name is good.

See typing that in bot we get 2nd part of flag “*poteropelus_walker*”

8] Now also as said in audio contain many secrets and we can see a link in mediainfo which is "https://youtu.be/z4t2_6SFiPo"



going on that link we get a video whose name is 3rd part and in that for a fraction of second we get the 3rd flag as "_galpin_thornhill_weems"



9] Finally Concatenating part of flag we get flag as
VishwaCTF{_sinclair_addams_barclay_petropolis_walker_galpin_thornhill_weems}
