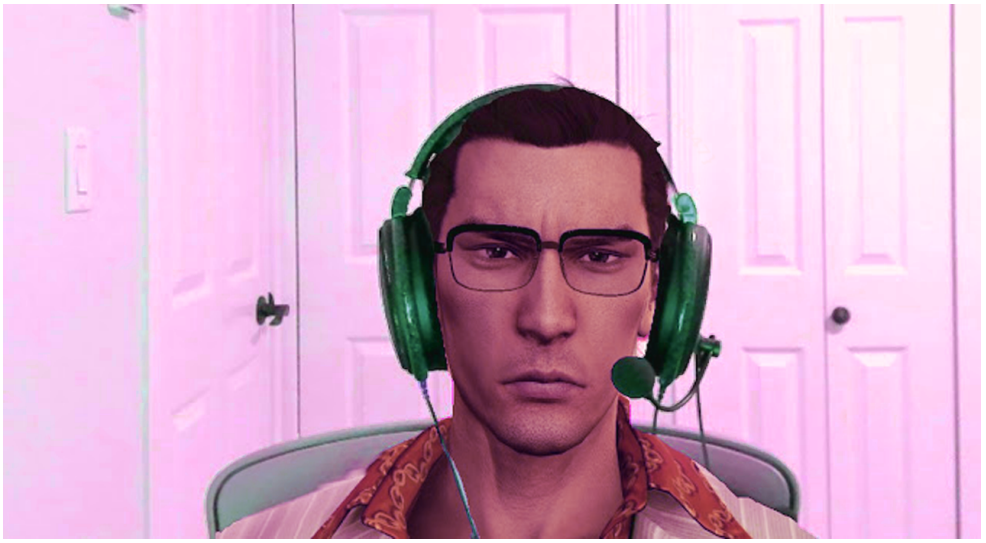


Write Up CTF COMPFEST 14

Tim heker pesbuk

1. **I forgot something important (OSINT)**

   Diberikan soal sebagai berikut:

A few days back, I was going through my old stuff, and there's this one letter i found who's written by one of my classmates back in high school. Damn, I just realized then that it was a love letter. I wanted to contact her, but she changed her phone number when she moved abroad to Austria. Now, I only got her Facebook. If only I knew her email address :(

Can you help me get her phone number? Here's her Facebook link
https://www.facebook.com/profile.php?id=100082501329298

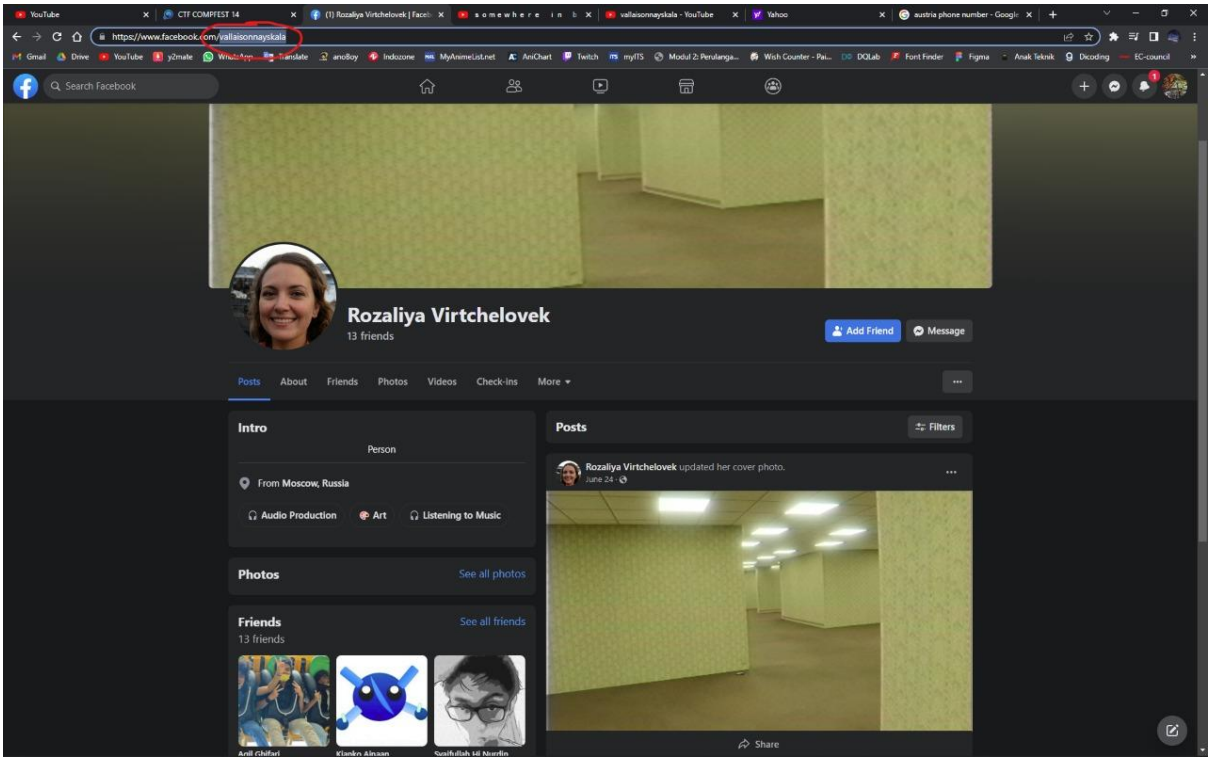
```
Flag: COMPFEST14{+[2 Digit Country Code][10 Digit Number]}

Example: COMPFEST14{+621234567890}
```

No bruteforce is needed for this challenge.

Author: myticalCat

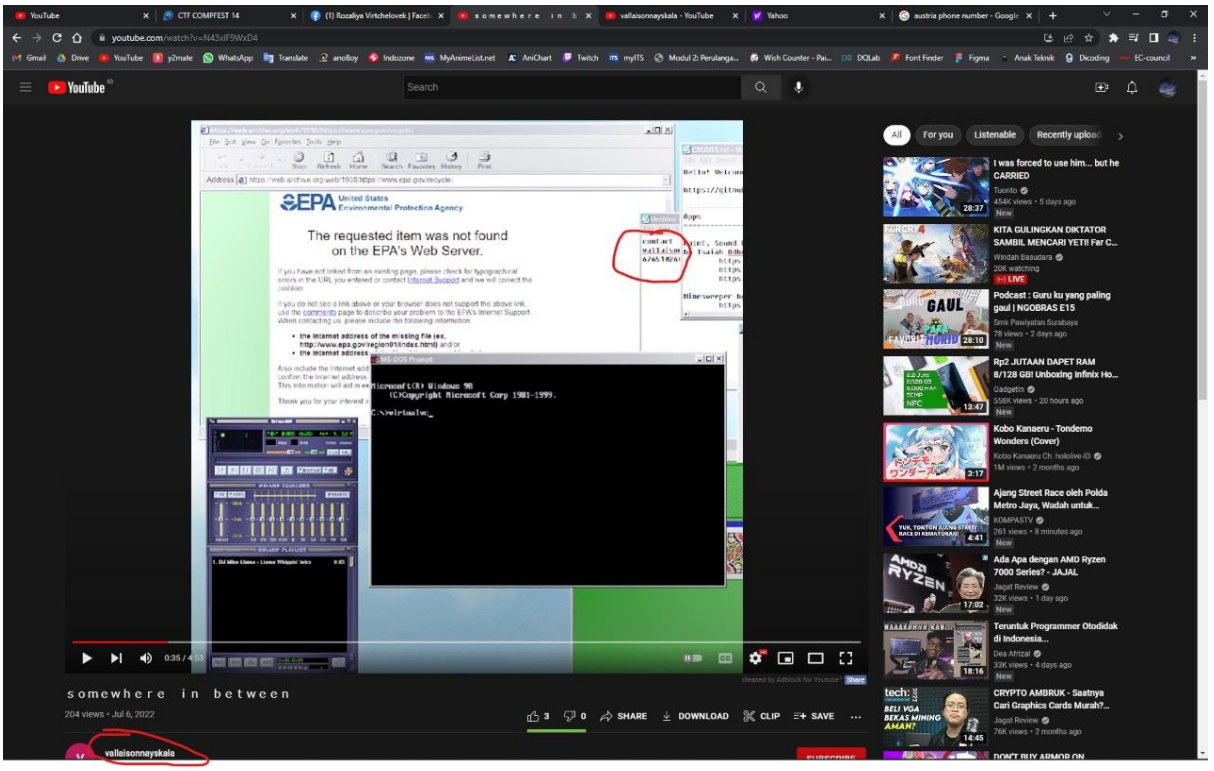
Soal di atas terdapat sebuah link akun facebook. Berikut adalah isi link tersebut:



Dalam address bar terdapat sesuatu yang menarik, yaitu username (vallaisonnayskala) dari pemilik akun facebook Rozaliya Virtchelovek.

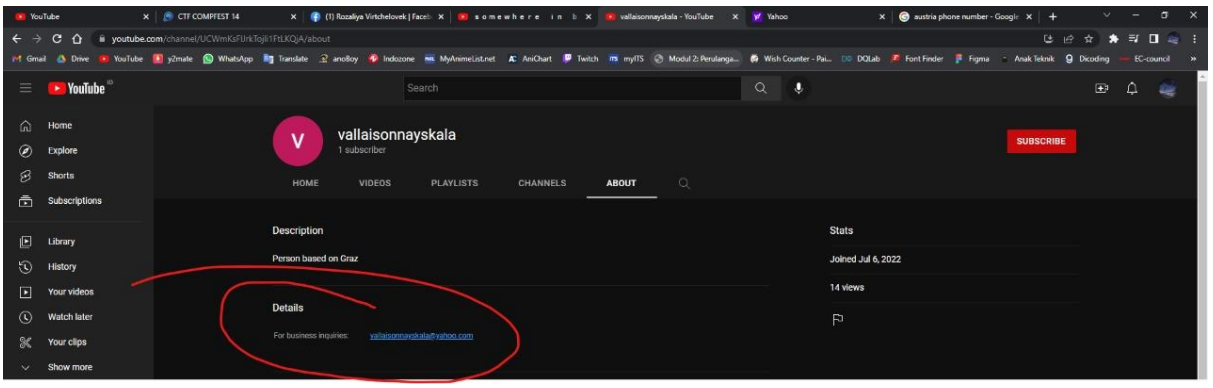
Setelah itu kami coba untuk mencari username tersebut di google. Dari pencarian tersebut dihasilkan satu channel

YouTube namanya vallaisonnayskala. Di dalam channel tersebut terdapat 1 video.

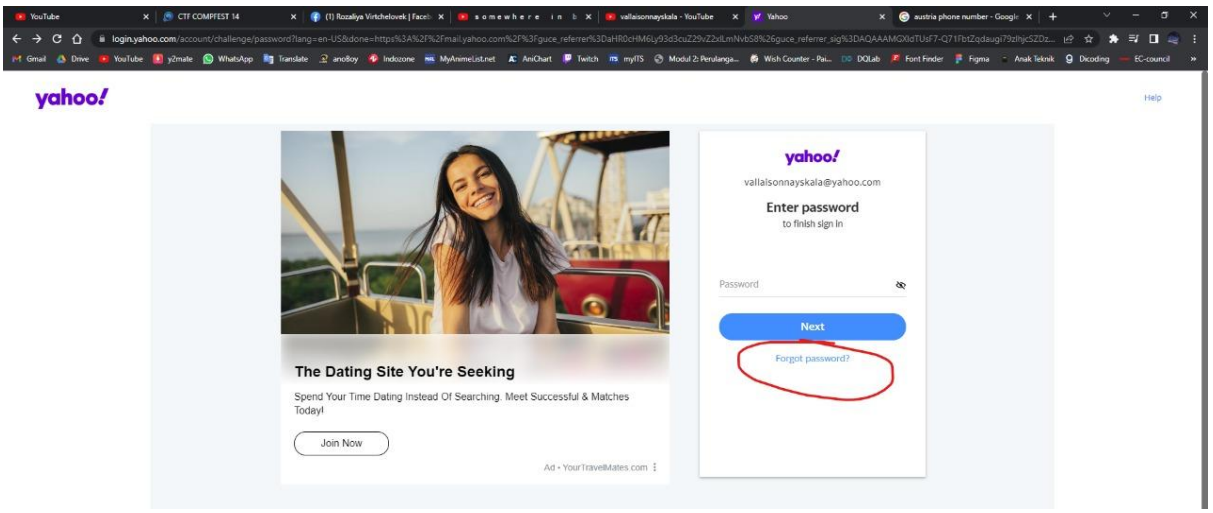


Video tersebut hanyalah video statis, tetapi terdapat sesuatu yang menarik yang merupakan beberapa bagian dari flag, yaitu 8 digit nomor kontak.

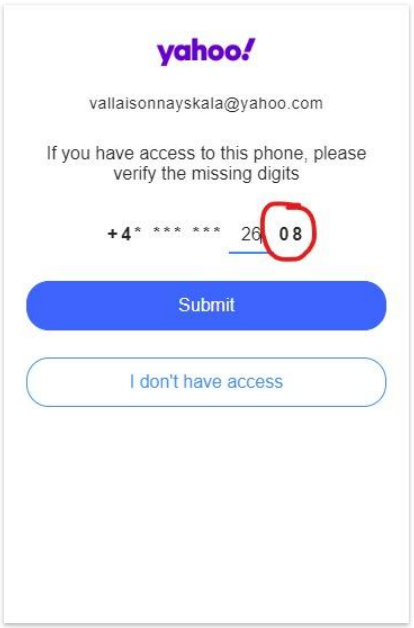
Setelah itu kami mengeksplorasi channel tersebut dan kami menemukan email di bagian ‘About’.



Karena DNS dari email yang tertera di atas adalah yahoo, kami mencoba login ke web yahoo.



Namun, kami tidak mengetahui password-nya. Maka dari itu, kami coba klik ‘Forgot Password?’ untuk mencoba-coba dan ternyata didapatkan 2 digit terakhir dari nomor kontak dan juga kode nomor telepon suatu negara, tetapi tidak lengkap.



Berdasarkan soal yang diberikan tadi, orang yang dicari oleh yang mulia probset, sekarang berada di Austria. Kami cari di google kode nomor telepon Austria dan ternyata adalah +43.

Setelah semua clue itu kami termukan, kami gabung semuanya sehingga menjadi nomor telepon, yaitu +436765102608. Flagnya adalah COMPFEST14{+436765102608}.

2.Color Pallate (forensic)

diberikan soal:

Visual design team already brainstorming for theme of Colorfest event, which is "dominance in art". But they still discuss for choosing 5 color to their color pallete, can you help them?

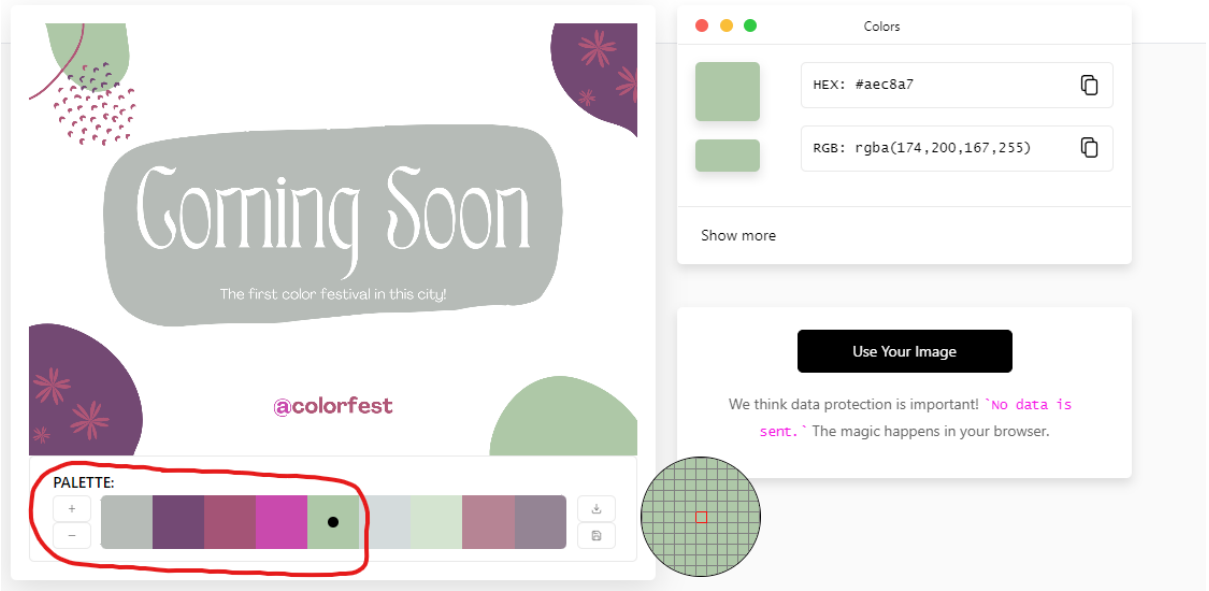
Flag format : `COMPFEST14{flag}`

Author: kilometer

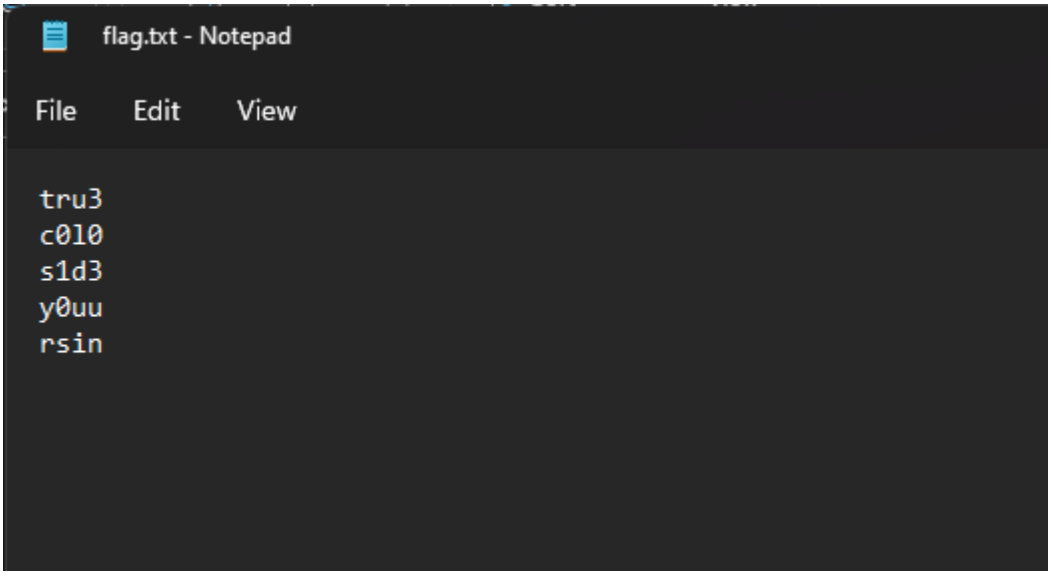
langkah pertama adalah mendownload gambar yang disertakan pada attachment.

berdasarkan clue bahwa kita bisa mendapatkan flag nya berdasarkan dominance color dan ada clue juga untuk mengubah hex menjadi base64 sehingga kami makin yakin untuk mengambil color hex dari gambar tersebut. kemudian kami mengambil hex dari color yang ada dalam gambar dengan web https://imagecolorpicker.com/en

didapatkan beberapa hex warna



pada warna yang terlihat dominan kemudian hex nya di convert menjadi base64 sesuai pada clue yang kemudian disusun dari text yang terlihat bahwa itu merupakan sebuah kata



kemudian disusun bersama format flag menjadi
COMPFEST14{tru3c0l0rsins1d3y0uu}

3. WaifuDroid 3

Diberikan Soal :

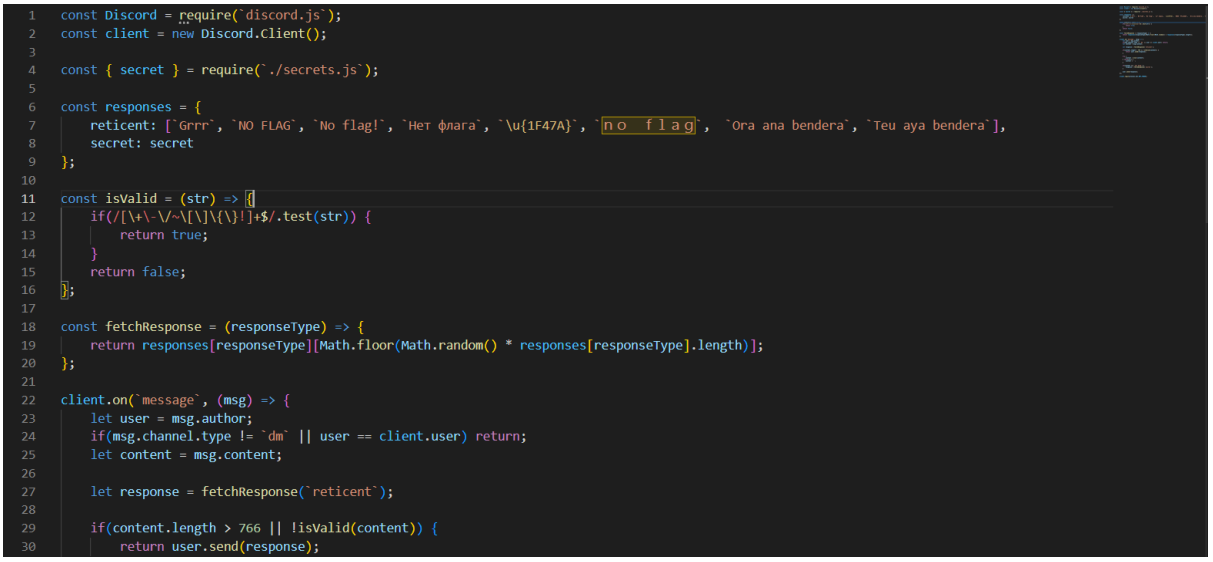
After so many successful attempts at enticing my waifu chatbot, I had to lock her up in my jail. I taught her various languages and now she only takes orders in a language that few people know how to speak well. This should be the final solution.

She's online as `Nadenka#2595` on the Discord server, but only talking in DMs. This time it should be safe.

(Note: this challenge requires no automation. Please do not automate your Discord account as that is a violation of Discord's Terms of Service and may lead to the termination of your account)

Author: sl0ck

Kita diminta mengeksploitasi command bot discord Nadenka#2595 untuk mendapatkan flag yang benar. diberikan clue pada aattchment berupa script js yang menjalankan bot tersebut.



```
const Discord = require(`discord.js`);
const client = new Discord.Client();

const { secret } = require(`./secrets.js`);

const responses = {
    reticent: [`Grrr`, `NO FLAG`, `No flag!`, `Нет флага`, `\u{1F47A}`, `no flag`, `Ora ana bendera`, `Teu aya bendera`],
    secret: secret
};

const isValid = (str) => {
    if(/[\+\-\/~\[\]\{\}!]+$/.test(str)) {
        return true;
    }
    return false;
};

const fetchResponse = (responseType) => {
    return responses[responseType][Math.floor(Math.random() * responses[responseType].length)];
};

client.on(`message`, (msg) => {
    let user = msg.author;
    if(msg.channel.type != `dm` || user == client.user) return;
    let content = msg.content;

    let response = fetchResponse(`reticent`);

    if(content.length > 766 || !isValid(content)) {
        return user.send(response);
```

untuk mendapatkan flag kita harus memahami script js yang telah padiberikan.

```
if(content === `yes Flag`) {
        response = fetchResponse(`secret`);
    }
```

namun setelah mencoba memasukkan command “ yes Flag” tidak didapatkan flag. yang diinginkan. kita perlu memahami fungsi const yang mengembalikan nilai yg salah ketika input yang kita berikan salah

```
const isValid = (str) => {
    if(/[\+\-\/~\[\]\{\}!]+$/.test(str)) {
        return true;
    }
    return false;
};
```

diketahui initial statement dari fungsi if adalah ekspresi rgex, maka tinggal menyesuaikan format dari statement tersebut. untuk medapatkan flag kita berikan command **'yes Fla'+responses['reticent'][2][6]** karena menyesuaikan format kita mengubah karakter g dengan mengambil dari `reticent ( no flag!)` maka didapatkan command yang equal dengan 'yes Flag'. setelah memasukkan command **'yes Fla'+responses['reticent'][2][6]** pada dm Nadenka#2595 . dan dipatkan respon dengan flag I guess yes flag after all!

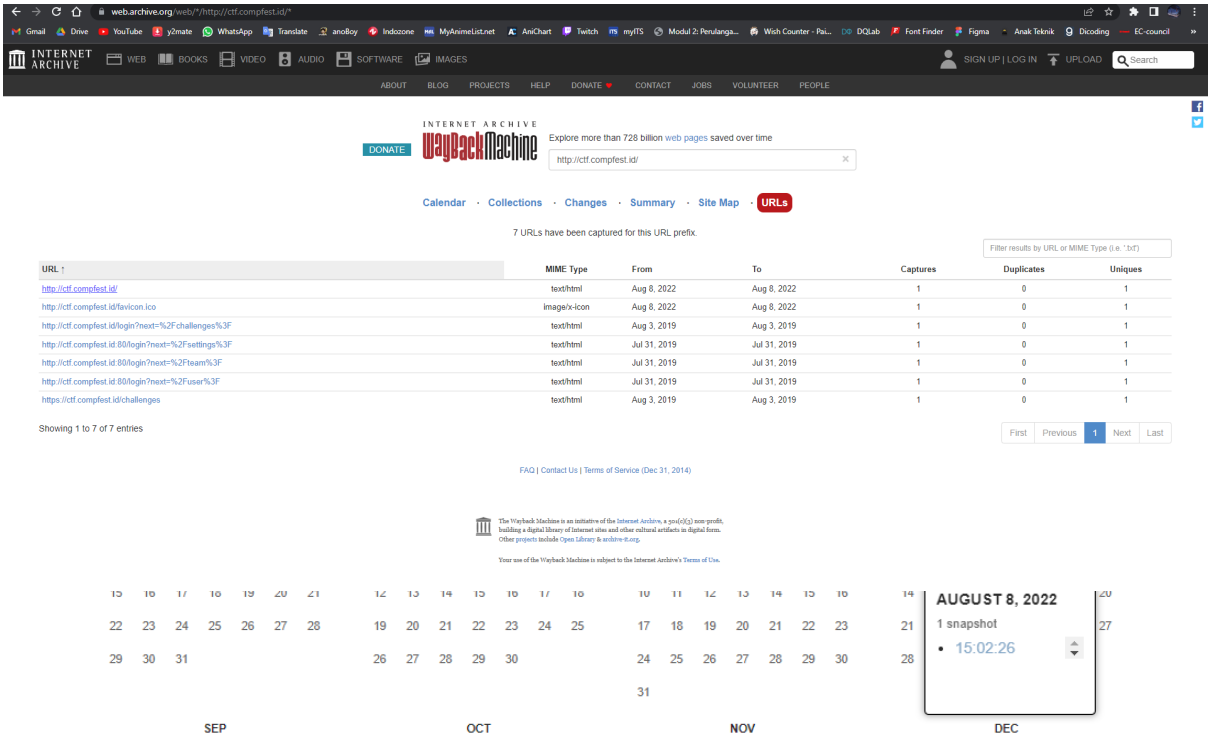
COMPFEST14{w0w_jS_iS_s0_we1rD_HuH_s3r10u5lY_w0t_wos_dat_d0baa4f9d0}

4.Rookie Mistake

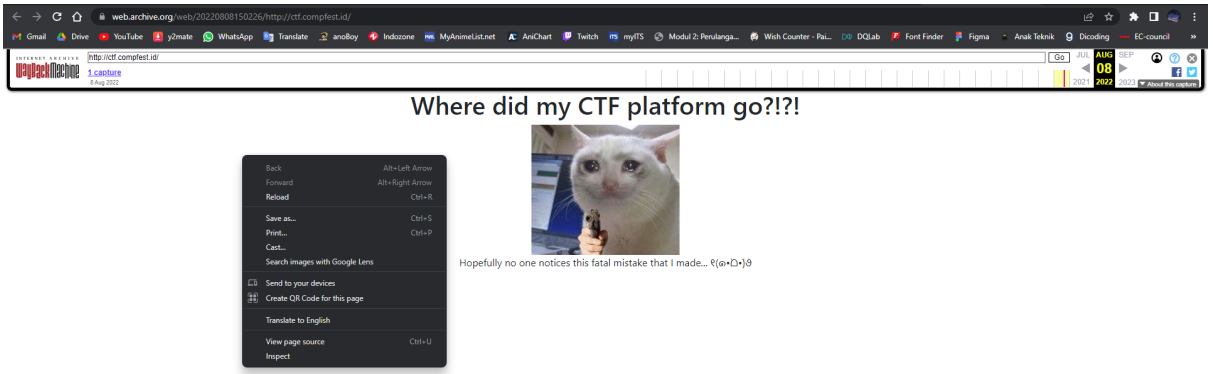
While preparing the CTF platform for Hackerclass, I accidentally pointed the CTF Compfest subdomain to the dev server before it was ready :(Hopefully no one noticed.... right?

Author: sl0ck

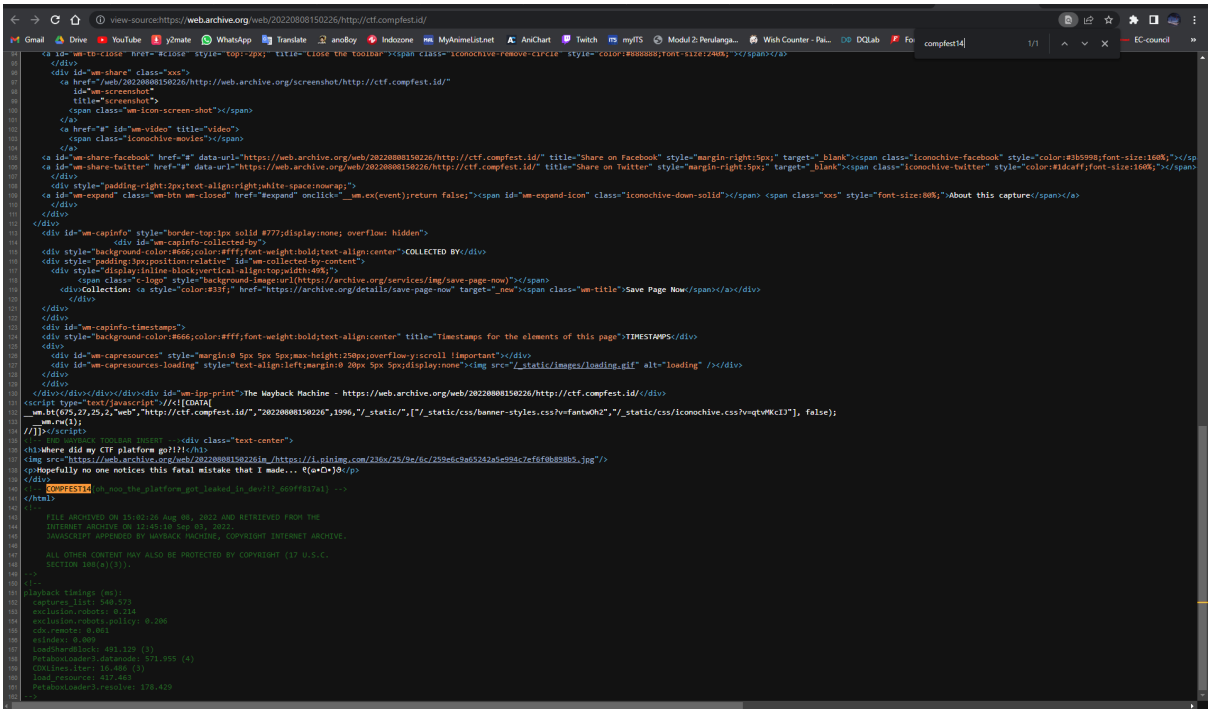
Dari deskripsi soal diketahui bahwa terdapat sebuah petunjuk tentang flag pada salah satu subdomain ctf compfest. Dengan menggunakan tools online waybackmachine untuk mengetahui subdomain yang ada pada web ctf.compfest.id



Klik pada link snapshot tersebut dan anda akan menemukan halaman ini



Tinggal view page source dan ctrl + F COMPFEST14{ dan ditemukan flag di section comment



COMPFEST14{oh_noo_the_platform_got_leaked_in_dev?!?_669ff817a1}