WRITEUP CTF COMPFEST 14

sak isone

blanktix
anya
Jisooo

MISC

[Sanity Check]

FLAG : COMPFEST14{_good_luck_and_have_fun__uWu_}

[Forum Feedback CTF COMPFEST 14]

Deskripsi :
Mohon mengisi form feedback berikut :

Solusi :
isi form dan didapatkan flag nya

FLAG : COMPFEST14{Terima kasih sudah mengisi feedback ini! Semoga mendapatkan hasil yang terbaik!!!}

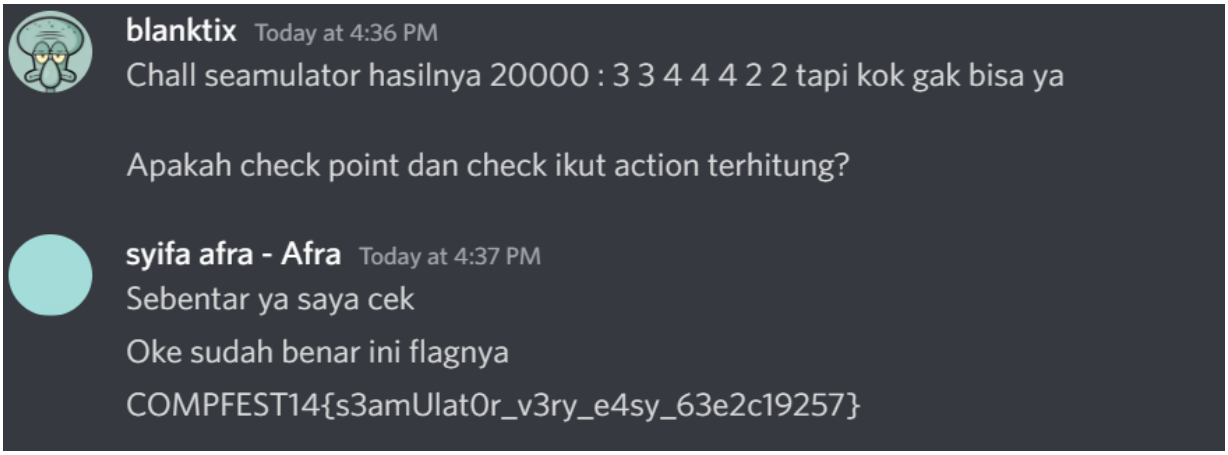
[Seamulator]

Deskripsi:
My brother has a new hobby, making a game. Yesterday, he made a cool game named Seamulator. I tried to play it, and after I did 7 actions, my fish price was $20,000. But I forgot which actions did I take.

Solusi :

Diberikan service netcat berisi sebuah program game sederhana. Di chall ini kita diharuskan untuk melakukan 7 kali aksi (*swim*, *eat another fish*, dan *jump*) agar kita mendapatkan poin akhir sejumlah $20000 dengan poin awal $1. Aksi *swim* meningkatkan poin 10x dari poin sebelumnya, *eat another fish* menjumlahkan poin sebelumnya dengan 12, dan *jump* menggandakan poin menjadi 2x dari poin sebelumnya.

Solusi dari chall ini adalah membuat 7 kombinasi aksi dari *swim*, *eat another fish*, dan *jump*. Karena hanya ada 3 aksi untuk membuat kombinasi maka saya bisa lakukan secara manual yaitu dengan memilih urutan menu: [3,3,4,4,4,2,2] untuk mencapai poin target $2000. Hanya saja langkah tersebut tidak bisa memberikan saya flag sehingga saya menanyakan ke probset dan ternyata memang langkah tersebut valid.



FLAG : COMPFEST14{s3amUlat0r_v3ry_e4sy_63e2c19257}

FORENSIC

[Color Pallete]

Deskripsi :

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?

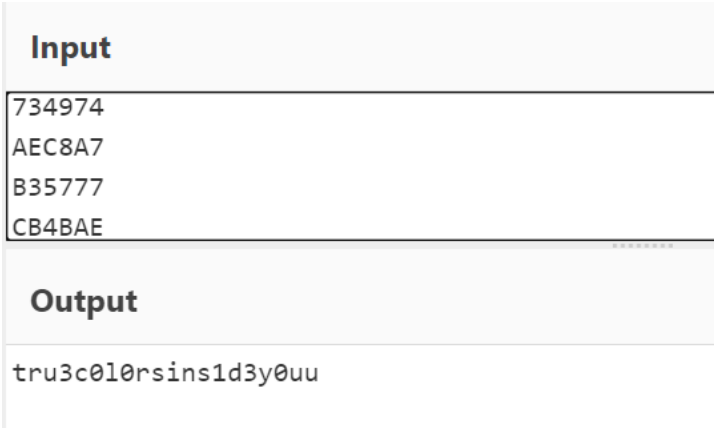
Petunjuk :

- Sorted by dominance visually
- If a color do not have specific wavelengths, then it is not a color, but still useful when it is needed. Remember the logo of Colorfest is pink, so it must be used in color palette.
- Hex to base64

Solusi :

Disajikan sebuah gambar PNG normal tidak ada kerusakan pada chunknya. Pada deskripsi diberitahukan jika ada 5 warna dominan yang ada pada gambar tersebut. Itu artinya kita harus mengekstrak *color pallete* dari gambar tersebut. Dengan menggunakan tools online https://color.adobe.com/create/image didapatkan 5 buah palet warna dengan nilai hex masing-masing.

Probset memberikan petunjuk bahwa kita harus mengurutkan warna tersebut dari warna yang paling dominan. Lalu setelah mendapatkan urutan warna yang sesuai, flag merupakan nilai base64 dari susunan hex setiap warna yang terurut.



FLAG : COMPFEST14{tru3c0l0rsins1d3y0uu}

OSINT

[I forgot something important]

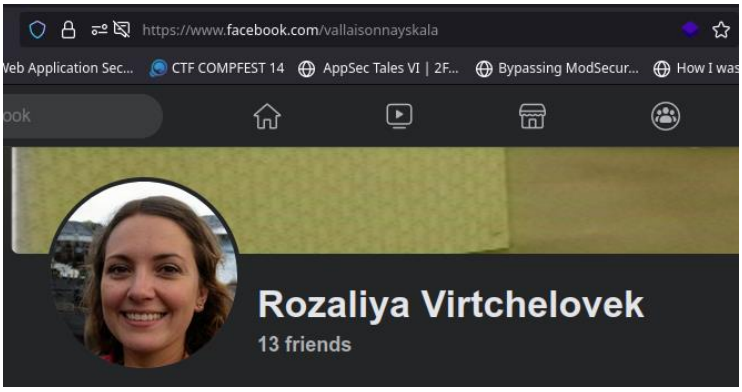
Deskripsi :

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 :(

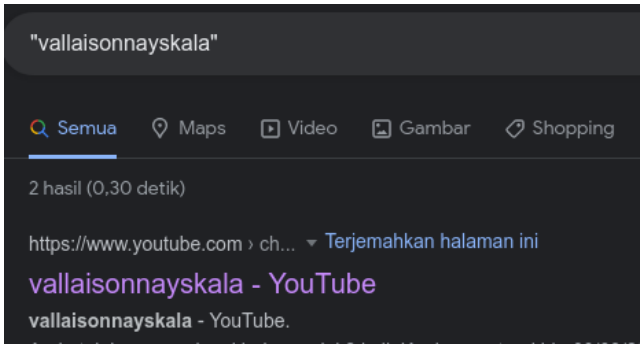
Can you help me get her phone number? Here's her Facebook link
https://www.facebook.com/profile.php?id=100082501329298
Flag: COMPFEST14{+[2 Digit Country Code][10 Digit Number]}
Example: COMPFEST14{+621234567890}
No bruteforce is needed for this challenge.

Solusi :

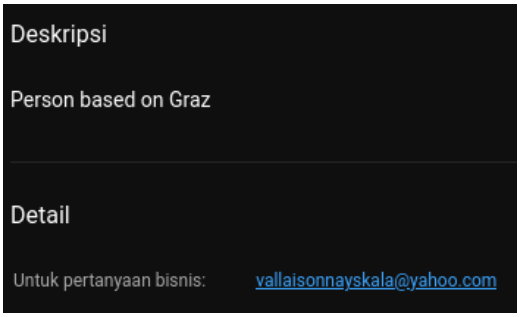
Diberikan link facebook dan kita diminta untuk mencari nomor telepon, ketika dibuka terlihat username facebook milik teman sekelasnya yaitu vallaisonnayskala.



Ketika dilakukan pencarian pada search engine google dengan keyword “vallaisonnayskala” mendapatkan hasil akun youtube

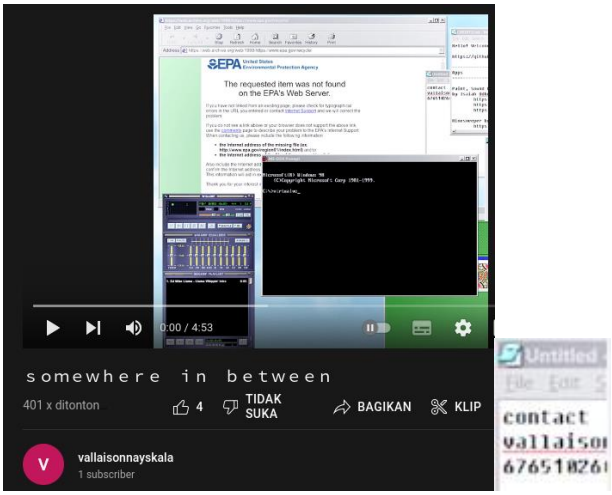


Ditemukan email pada bagian *about* akun youtubenya.

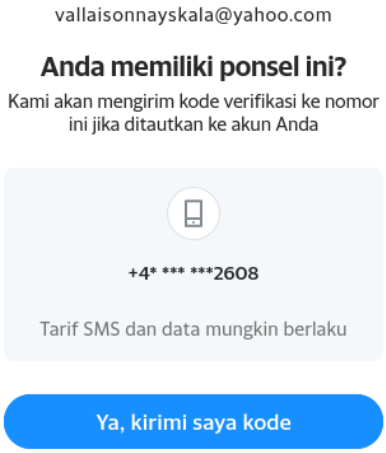


Mengutip kalimat pada deskripsi soal " *If only I knew her email address :(Can you help me get her phone number ? "* saya teringat fitur reset password dimana biasanya akan mengirimkan otp ke no hp pemilik email dimana disitu akan terlihat no hpnya walaupun sebagian. Ketika melakukan reset password email yahoo terdapat 2 digit angka yang harus kita isi dan beberapa angka yang tidak terlihat.

Sebelumnya pada akun youtube tersebut ada 1 video, cek video tersebut dan zoom pada notepad ternyata terdapat potongan no hp.



Kita bisa melengkapi nomor hpnya menjadi +43 6765102608 (+43 didapat dari kode negara temannya yang pindah yaitu austria). Validasi jika nomornya memang benar dan berhasil yahoo meminta otp ke nomor tersebut.



FLAG : COMPFEST14{+436765102608}

[W3Win]

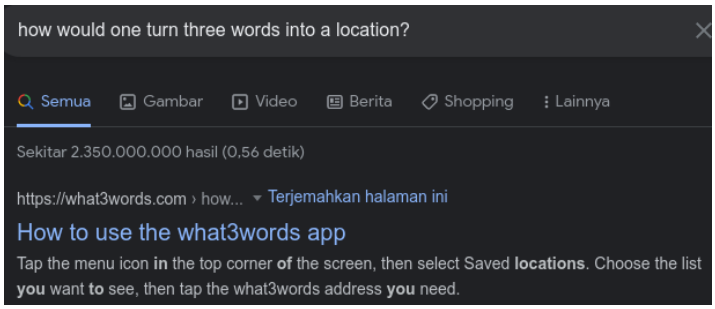
Deskripsi :

My middle-term exam has finished, and now I have 3 days of holiday. I wanted to refresh, so I decided to travel with my friends. I will tell you a secret, one of our plans is to rent a vehicle. Can you help us to check Instagram to find the open hours?

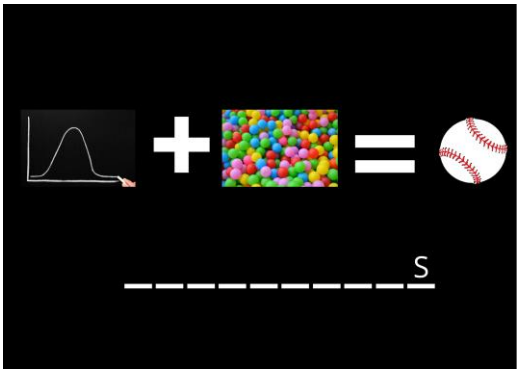
Flag : COMPFEST14{Y_XX:XX-XX:XX}
Instagram account = Y
Open hours = XX:XX-XX:XX

Solusi :

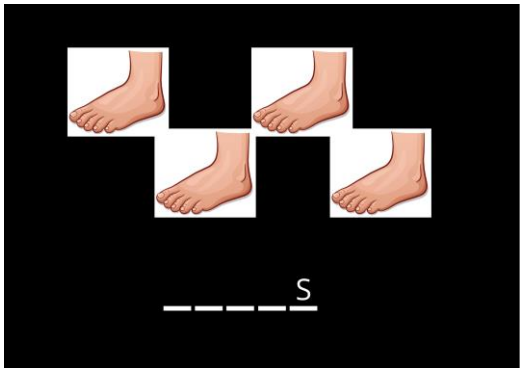
Mereka berencana untuk menyewa kendaraan dan kita diminta untuk cek instagram untuk menemukan jam buka dan tutup. Diberikan 3 gambar dimana kita harus menebak gambar tersebut, kemudian terdapat hint yaitu "*how would one turn three words into a location?*" saya teringat what3words.com dimana dengan 3 kata kita bisa mendapatkan lokasi dan disini diberikan 3 gambar jadi kemungkinan tiap gambar akan menjadi 1 kata. Sebenarnya juga bisa langsung copas hint ke google untuk mencari websitenya.



Mari kita coba, gambar pertama cukup menyulitkan, awalnya kami mengira baseball namun kekurangan 1 huruf. Kemudian teman setim saya berkata "itu paling kiri curve bells kan", ketika saya cari di search engine google nampaknya memang benar dan ternyata katanya pas namun masih belum tentu benar.



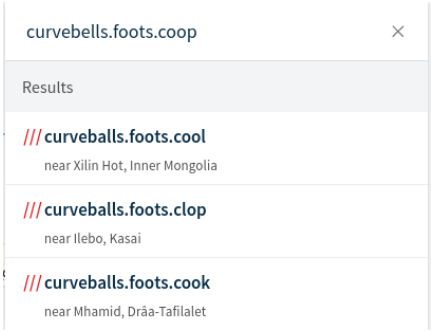
Beralih ke foto kedua terlihat gambar kaki dan ada banyak jadi ini jelas **foots**.



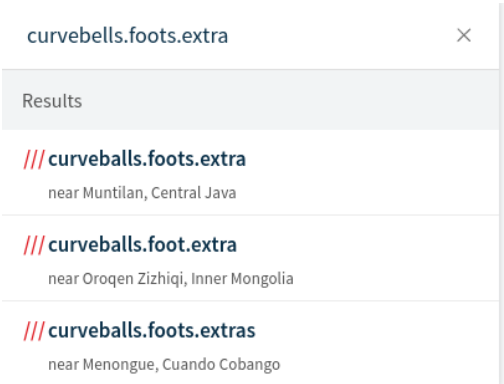
Kemudian gambar terakhir, kami melakukan reverse image search untuk mencari informasi gambar apa ini.

Didapat hasil logo coop extra, jadi antara coop atau extra.

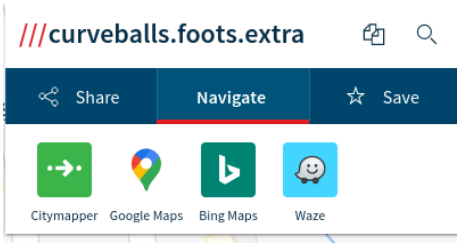
Kemudian kami mendatangi website what3words.com memberikan 3 kata yaitu curvebells.foots.coop dan tidak mendapat hasil.



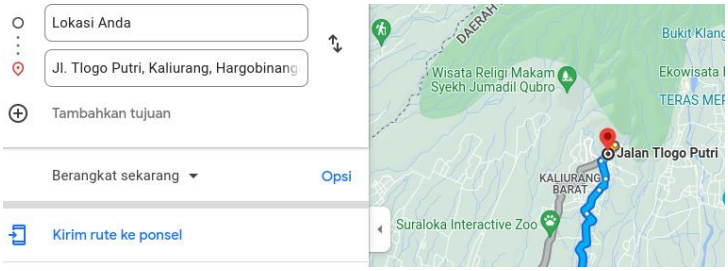
Kami mencoba menggunakan extra, menjadi curvebells.foots.extra dan didapat hasil lokasi berada di dekat muntilan jawa tengah, disini kami menyadari bahwa kata pada gambar pertama yang benar adalah curveballs bukan curvebells namun karena website memberikan rekomendasi jadi kami tetap mendapatkan lokasinya.



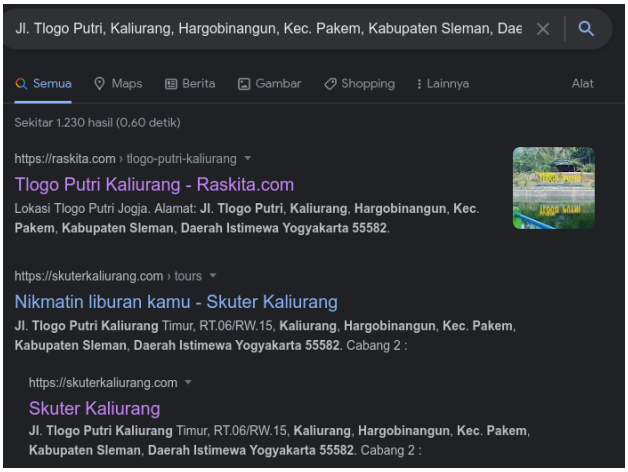
Disini pilih navigate lalu google maps untuk mendapatkan lokasi tepatnya.



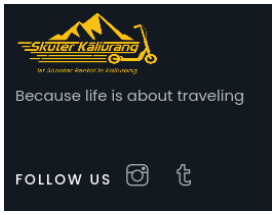
Lokasinya berada di Jl. Tlogo Putri, Kaliurang, Hargobinangun, Kec. Pakem, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55582



Kami kemudian mencari informasi terkait rencana mereka yang akan menyewa kendaraan dengan mencari di search engine google dengan keyword *Jl. Tlogo Putri, Kaliurang, Hargobinangun, Kec. Pakem, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55582*. Hasilnya terdapat skuter kaliurang dimana lokasinya sama serta menurut hint kendaraannya ini beroda 2 sedangkan skuter juga beroda 2 jadi cocok.



Pada bagian follow us ada icon yang akan redirect ke akun instagramnya.



Pada bio terdapat informasi open hours dan nama instagramnya skuterkaliurang.

FLAG : COMPFEST14{skuterkaliurang_08:00-20:00}

[Rookie Mistake]

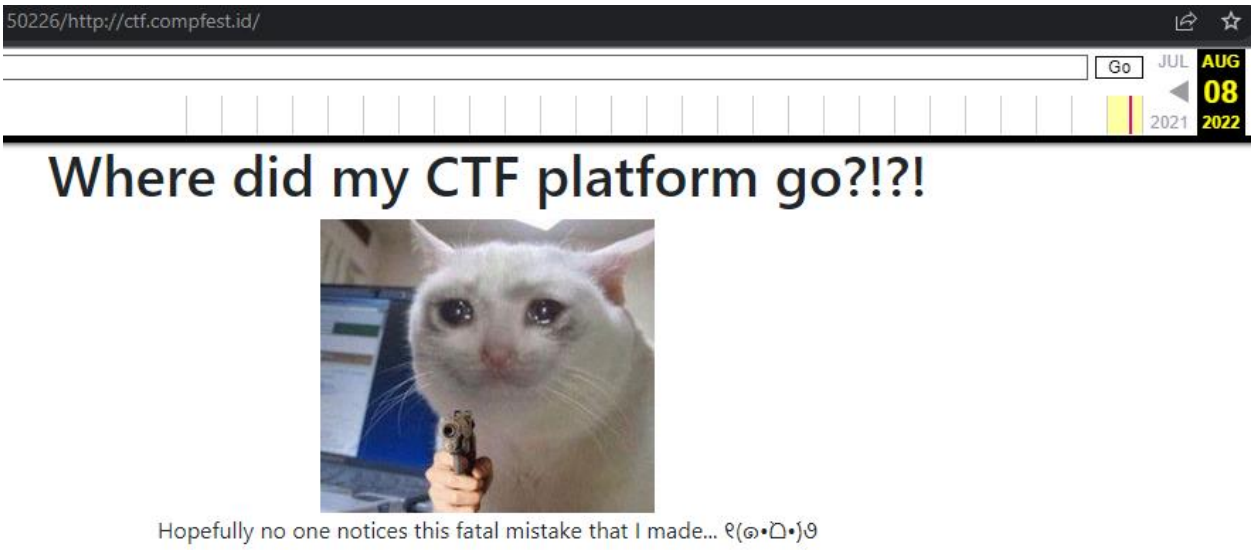
Deskripsi :

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?

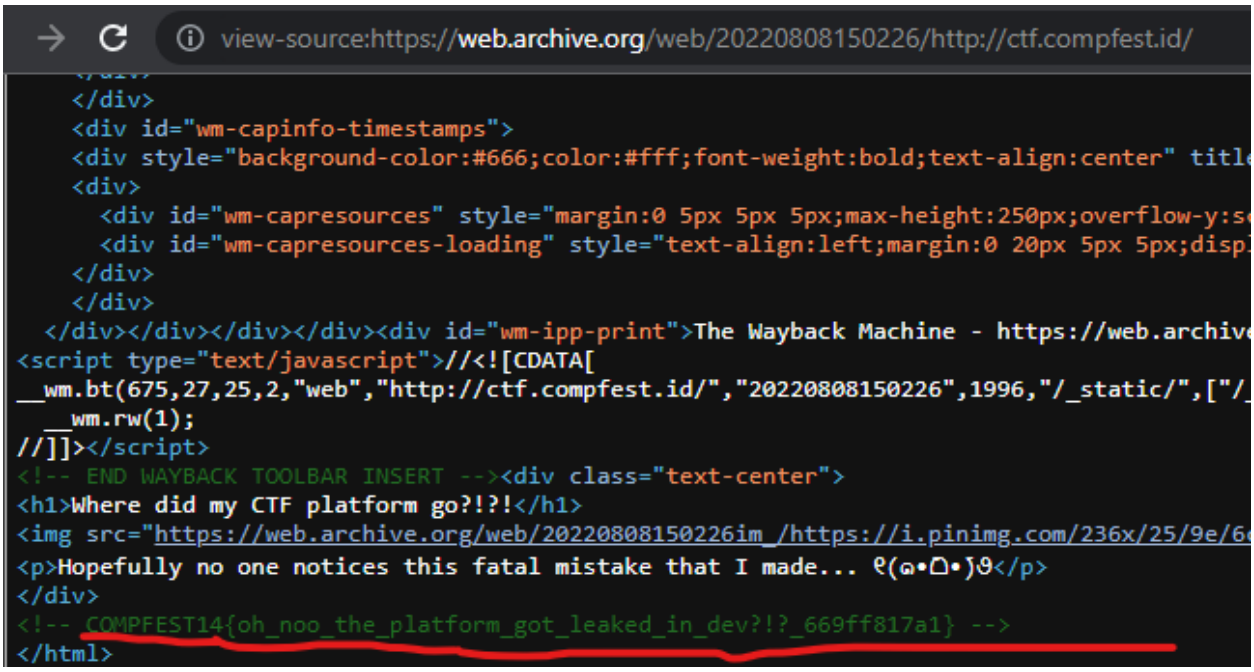
Solusi :

Dapat kita lihat pada deskripsi soal dimana probset ‘pointed ctf compest subdomain to the dev server before it was ready’, kita mengetahui bahwa ctf.compfest.id itu sendiri adalah subdomain compfest yang digunakan untuk kompetisi ctf itu sendiri. Dan disitu juga tertera ‘dev server’ dimana kemungkinan besar pernah digunakan pada saat develop sebelum ctf.compfest ini ready. Maka itu terpikirkan oleh kami untuk menggunakan wayback machine (**https://archive.org/web/**).

Disitu dapat terlihat bahwa ctf.compfest.id terdapat 1 riwayat yang tersimpan di wayback machine pada tanggal 8 Agustus 2022, langsung saja lakukan pengecekan pada tanggal itu



Saat dibuka, tidak ada sesuatu yang mengarah ke flag, namun disini kami melihat pada page source halaman tersebut dan menemukan flag nya di sana



FLAG : COMPFEST14{oh_noo_the_platform_got_leaked_in_dev?!?_669ff817a1}