

# **COMPFEST 14 - Capture The Flag**

## **Writeup Babak Penyisihan Tim HengkerNgangNgong**

### **Anggota:**

- **Alden Luthfi (Cheesewaffle)**
- **Muhammad Nabil Mu'afa (nabilmuafa)**
- **Muhammad Oka (okeeeeng)**

### **I forgot something important (OSINT)**

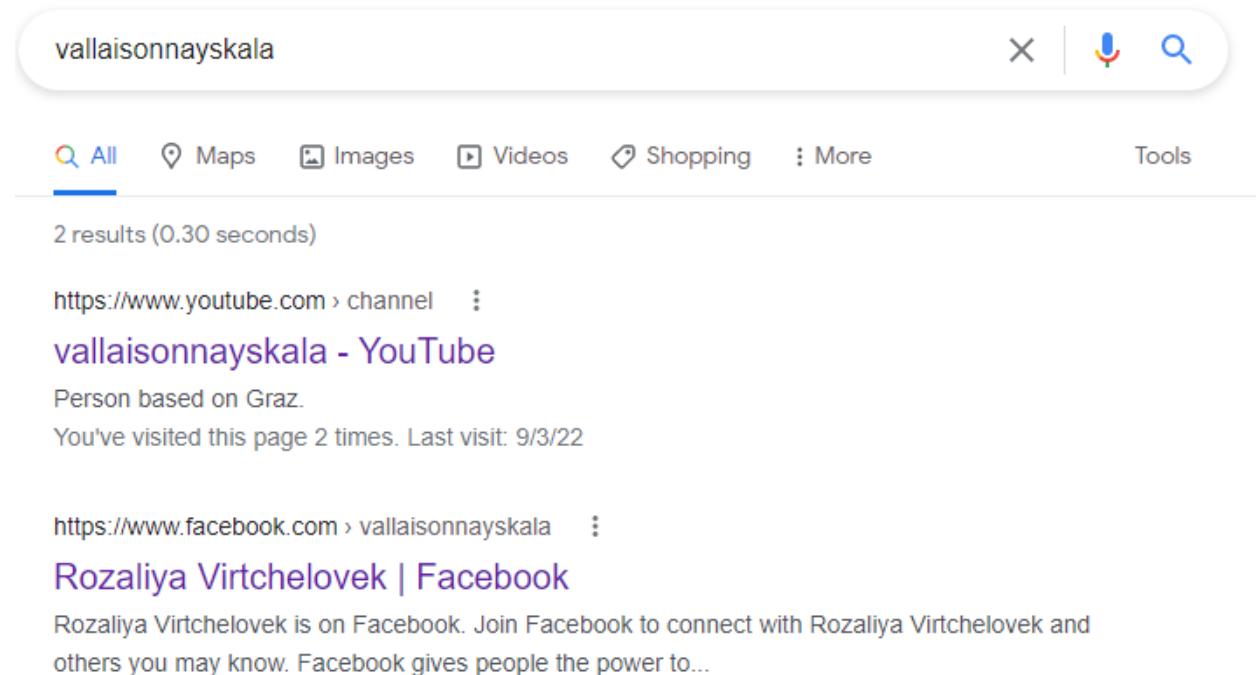
Deskripsi challenge memberikan kita [link](#) ke profil Facebook seseorang bernama Rozaliya Virtchelovek. Approach yang pertama kali terpikir oleh tim kami adalah untuk melihat friend list dari akun tersebut jika ada kejanggalan, tetapi tidak menemukan apa-apa. Setelah memeriksa bagian About dari akun tersebut, kami juga tidak menemukan apa-apa.

Kemudian melalui URL address bar, tim kami menemukan username dari akun Facebook tersebut:



facebook.com/vallaisonnayskala/?

Approach kami selanjutnya adalah untuk mencari username tersebut pada Google, jika seandainya terdapat jejak-jejak lain mengenai akun tersebut. Hanya ada dua hasil search, yaitu akun Facebook Rozaliya, dan juga sebuah akun YouTube dengan username vallaisonnayskala.



vallaisonnayskala

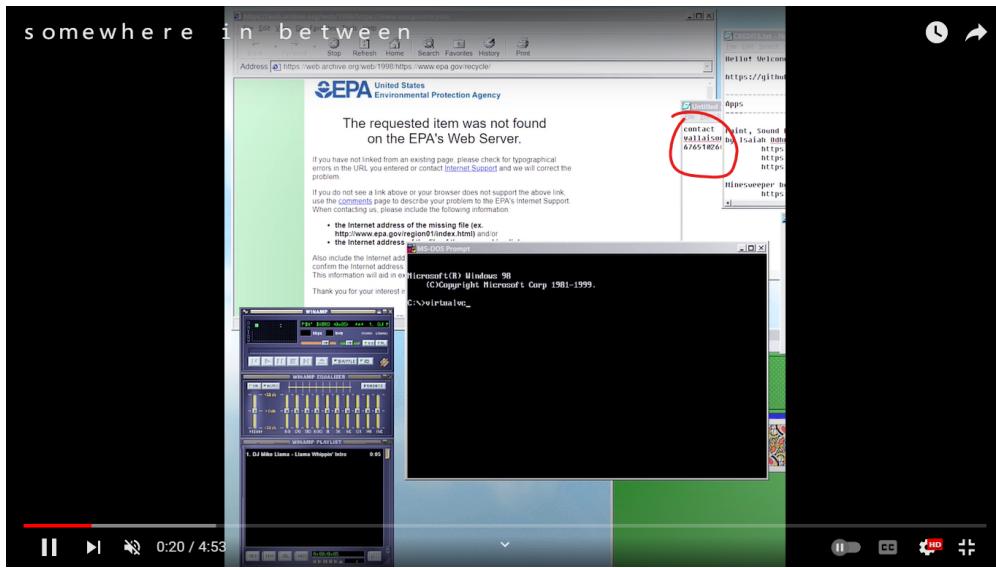
All Maps Images Videos Shopping More Tools

2 results (0.30 seconds)

<https://www.youtube.com/channel/UCVzXWzqfJLcOOGmQHg> ::  
**vallaisonnayskala - YouTube**  
Person based on Graz.  
You've visited this page 2 times. Last visit: 9/3/22

<https://www.facebook.com/vallaisonnayskala> ::  
**Rozaliya Virtchelovek | Facebook**  
Rozaliya Virtchelovek is on Facebook. Join Facebook to connect with Rozaliya Virtchelovek and others you may know. Facebook gives people the power to...

Akun YouTube tersebut hanya memiliki [satu video](#) bernama “somewhere in between”, dan pada video tersebut terdapat sebuah nomor telepon yang memiliki 8 digit, yaitu 67651026.

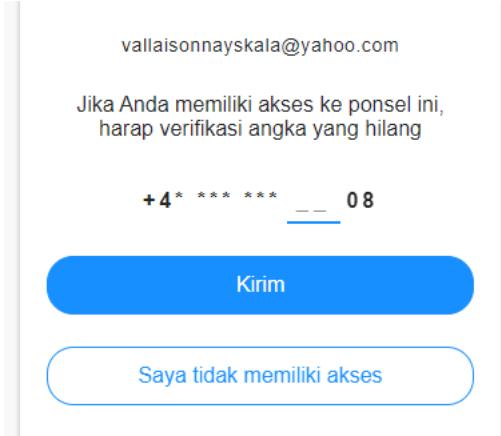


Karena nomor telepon yang diminta untuk flag adalah 10 digit, maka kami berasumsi itu adalah sebagian dari flag yang belum lengkap. Namun, tim kami sempat berkali-kali mencoba submit dengan memasukkan angka-angka random pada dua digit terakhir, berharap keberuntungan berpihak kepada kita.

Setelah kembali memperhatikan deskripsi challenge yang menyebutkan “If only I knew her email address” dan “No bruteforce is needed for this challenge”, kami berhenti mencoba angka-angka random dan berfokus untuk mencari email dari Rozaliya, dengan berasumsi dua digit terakhir memiliki kaitannya dengan email tersebut. Kami menemukan sebuah email Yahoo yang ter-link pada akun YouTube vallaisonnayskala pada bagian “About”-nya.

A screenshot of a YouTube channel page for "vallaisonnayskala". The channel has 1 subscriber. The page includes sections for "HOME", "VIDEOS", "PLAYLISTS", and "CHANNEL". Under "Description", it says "Person based on Graz". Under "Details", it lists "For business inquiries: vallaisonnayskala@yahoo.com".

Untuk mengetahui dua digit akhir dari nomor telepon Rozaliya, kami mencoba melakukan password recovery ke email tersebut, yang mana password recovery dari akun email tersebut dikirimkan ke nomor telepon yang berakhiran -08. Sehingga nomor telepon yang kita butuhkan sudah mencapai 10 digit, yaitu 6765102608.



Pada deskripsi soal, dinyatakan bahwa format flag juga harus menyertakan kode negara nomor telepon, dan berdasarkan deskripsi soal, kami mencoba menggunakan kode telepon Austria yaitu +43. Sehingga flag adalah:

**COMPFEST14{+436765102608}**

## c0rR3ct1On (Forensics)

Kita mendapatkan file .png yang tidak bisa dibuka. Kemungkinan terbesar adalah file yang corrupt. Mari kita buka file png itu ke dalam hex editor.

Setelah dibuka, terlihat beberapa keyword yang biasa ada di dalam file png namun terlihat bahwa file tersebut di-reverse.

Kita bisa membalikkan file png tersebut dengan python.

```
1  png = open("C:/Users/USER/Downloads/lemaoo.png", "rb")
2  png_reversed = open("C:/Users/USER/Downloads/lemaoo_reversed.png", "wb")
3
4  png_reversed.write(png.read()[:-1])
```

Setelah menggunakan script python tersebut dan membuka file output di hexeditor, terlihat file sudah mirip dengan file png dengan pengecualian file header yang belum sesuai.

Setelah file header sudah diperbaiki sesuai spesifikasi PNG yang ada di wikipedia, muncul gambar hitam putih.

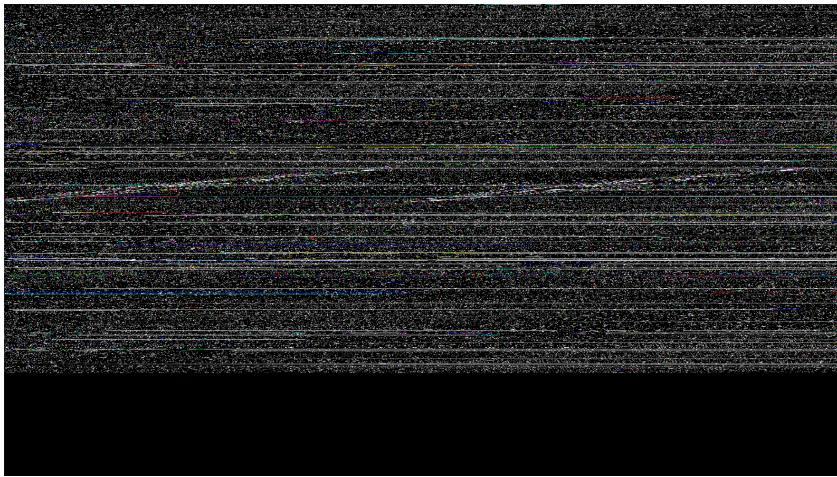
Melihat hint #1, bisa disimpulkan bahwa gambar hitam putih ini merepresentasikan binary.

Untuk merubah gambar menjadi binary, bisa menggunakan tools dari dcode.fr dengan catatan parameter “Size/Width of the Image” dengan pilihan “Original Size”.

Setelah mendapat binary dan di convert menjadi teks, kita mendapatkan sebuah link <https://tinyurl.com/m00nlander>.

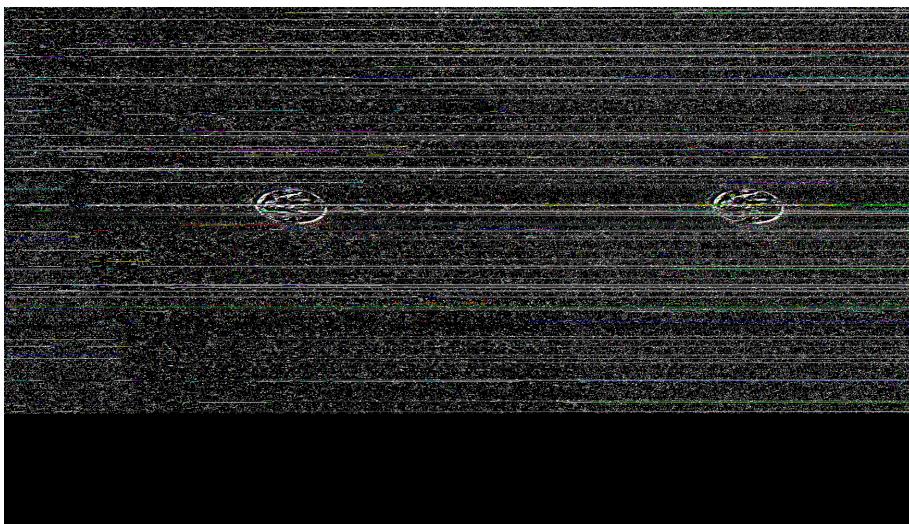
Link tersebut akan memberikan kita file jpg yang lagi lagi tidak bisa dibuka. Langkah selanjutnya adalah untuk membuka hex editor. Ternyata, di dalamnya terlihat seperti PNG walaupun extension file tersebut adalah JPG. Solusinya adalah memperbaiki file tersebut lalu merubah extension file menjadi .png. Permasalah yang ditemui di file ini adalah file header yang tidak sesuai, width dan height yang kosong, dan chunk IEND yang tidak sesuai.

Setelah diperbaiki, terlihat gambar yang mirip dengan file pertama namun dengan warna. Menurut deskripsi soal, file ini menggunakan rasio widescreen. Ukuran pertama yang terlintas adalah 1920x1080. Mari kita coba ubah ke width dan height tersebut menggunakan tool TweakPNG.



Terlihat bahwa ada beberapa titik yang menyerupai garis diagonal ke kanan. Biasanya, ini menunjukkan bahwa kita mempunyai width yang berlebih sehingga gambar yang dihasilkan menjadi stretched. Solusinya adalah mengurangi width hingga garis diagonal tersebut hilang/hampir tegak lurus.

Ketika mengganti width menjadi 1908, terlihat ada dua objek berbentuk bulat yang terlihat seperti bulan, sesuai dengan nama file tersebut (m00n). Berarti solusinya sudah dekat!



Karena gambar belum jelas dan objek tersebut ada dua, saya mencoba untuk membagi width dengan 2 menjadi 954.

Setelah menggunakan width 954, terlihat gambar bulan. Namun, flagnya ada dimana? Kemungkinan pertama adalah width atau height kurang besar yang menyebabkan flag tidak terlihat. Namun seperti yang kita tahu, merubah width akan merusak gambar. Mari kita coba mengubah heightnya.

Ketika mengganti height dengan 2000, terlihat tulisan flag dengan warna merah marun. Dan itulah flag kita!

**COMPFEST14{hHhH\_th0u\_4re\_c0rR3ect\_634af16261}**



## Color Pallete (Forensics)

Di soal ini kita mendapatkan gambar png. Terlihat sebuah design untuk promosi sebuah acara.



Melihat hint #3 dan melihat tema soal ini adalah warna, saya berasumsi bahwa ada hubungannya dengan kode hexadeciml dari warna-warna yang ada di gambar ini.

Setelah mencari kode hex untuk semua warna yang ada di gambar ini, saya mendapatkan warna-warna berikut:

```
#b6bbb7  
#734974  
#aec8a7  
#b35777  
#cb4bae
```

Setelah mendapat hex untuk setiap warna, mari kita ubah hex tersebut ke base64 dengan urutan warna yang paling banyak terlihat di gambar adalah yang paling atas (sesuai hint #1).

Dan hasil dari konversi hex ke base64 adalah flag kita!

Hasil konversi : tru3c0l0rsins1d3y0uu

**COMPFEST14{tru3c0l0rsins1d3y0uu}**

### **Seamulator (Miscellaneous)**

Seperti pada deskripsi soal, kita harus mencapai tepat \$20000 dolar dengan tepat 7 langkah. Saat program ini dijalankan kita dapat mengecek status uang kita setiap langkah dengan input 1, darisana kita dapat mengetahui bahwa input 2 (Swim) akan mengalikan jumlah uang saat itu dengan 10, input 3 (Eat another fish) akan menambahkan jumlah uang saat itu dengan 12, dan input 4 (jump) akan mengalikan jumlah uang saat itu dengan 2.

Dengan demikian kita bisa mencapai \$20000 dari \$1 dengan tepat 7 langkah dengan input 4-4-4-3-2-2-2. Lalu kita bisa mengambil flag dengan input 5

**COMPFEST14{s3amUlat0r\_v3ry\_e4sy\_63e2c19257}**

### **WaifuDroid 3 (Miscellaneous)**

Di soal ini kita diharuskan untuk berinteraksi dengan bot discord bernama Nadenka. Untuk mencari vulnerability di soal ini, kita juga diberikan source code untuk bot tersebut.

Soal ini menggunakan konsep hoisting dalam JavaScript. Dimana function bisa digunakan sebelum dideklarasikan (hoisting). Dalam kata lain, sebuah function dapat digunakan sebelum diinisialisasi. Sifat dari javascript yang sering dilupakan inilah yang kita akan exploitasi. Pertama kita melakukan overview dari kode nya. Bisa dilihat bahwa kita mengontrol variabel content dengan input kita, kemudian kita juga bisa melihat ada check dimana input kita di-check apakah panjangnya dibawah 766 karakter dan sesuai dengan hasil return dari fungsi isValid. Fungsi isValid cek apakah string input kita sesuai dengan regex yang ditentukan. Kemudian setelah check itu berhasil, input kita akan di eval, eval akan run string kita menjadi sebuah fungsi, dan itu lah metode yang kita gunakan untuk mendapatkan flag nya. Hasil dari eval tersebut akan dicek lagi apakah sesuai dengan string “yes Flag”, jika iya maka kita akan mendapatkan flag nya.

Langkah yang kita lakukan adalah menggunakan website [regexpr.com](http://regexpr.com) untuk memastikan input kita sesuai dengan regex nya. Yang terpenting adalah fungsi yang kita buat menghasilkan string “yes Flag”, jadi payload yang dapat kita gunakan dengan konsep hoisting adalah “win();function win(){return ‘yes Flag’}”, dimana hasil dari eval input tersebut menghasilkan string “yes Flag”. Kemudian, kita dapat DM bot Nadenka dengan payload tersebut untuk mendapatkan flagnya.

**COMPFEST14{w0w\_jS\_iS\_s0\_we1rD\_HuH\_s3r10u5IY\_w0t\_wos\_dat\_d0baa4f9d0}**