

Hacklabs.id Mini Weekly CTF 1.0



Problem :

Sanity Check (Misc.) – 5 pts

Souper (Cryptography) – 15 pts

Ez-Rev (Reverse Engineering) – 15 pts

Srand (Cryptography) – 15 pts

Way Back Home (OSINT) – 25 pts

Image Integrity (Forensic) – 35 pts

Sanity Check (Misc.)

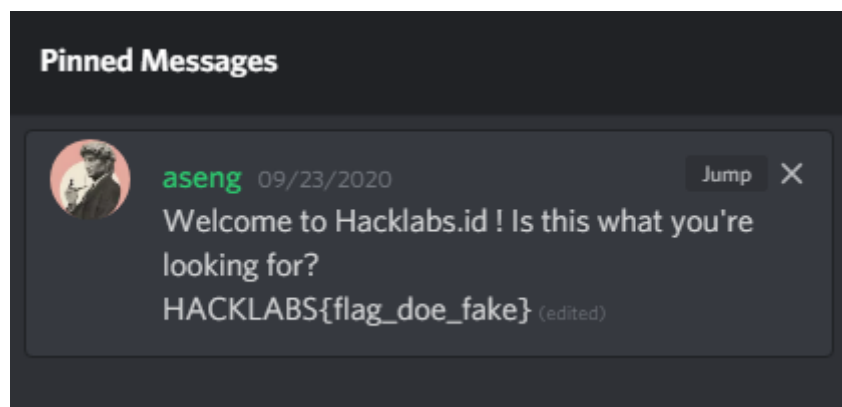


Dari caption yang ada pada post tersebut, kita disarankan untuk masuk ke dalam discord dari hacklabs.id menggunakan 1 dari 2 link di bawah.

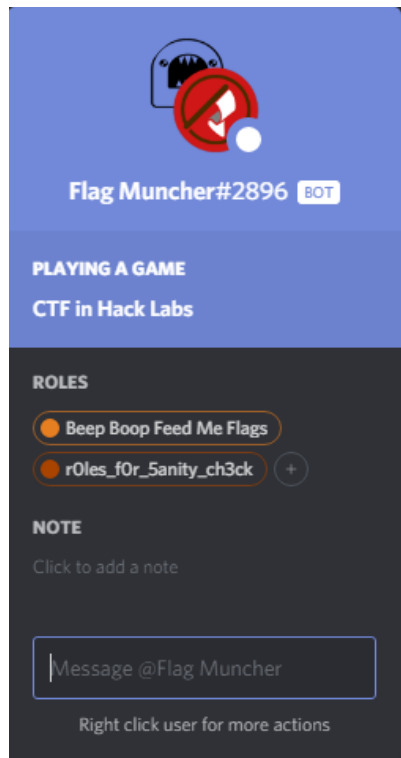
<https://discord.gg/wdSbgUA>

<https://discord.gg/Pz8GQSZ>

Setelah memasuki channel **discord** dari hacklabs.id, dan setelah mengecek tiap personil utama dari hacklabs.id kita tidak akan menemukan sesuatu yang menarik selain flag palsu pada pinned message.



dan yang tersisa adalah untuk mengecek bot yang ada.





Dari roles yang diassign pada bot tersebut, kita dapat mengetahui flag pada challenge ini

HACKLABS{r0les_f0r_5anity_ch3ck}

Souper (Cryptography)



Pada challenge ini, sama dengan challenge week sebelumnya di mana mengharuskan kita untuk mendownload file dari drive hacklabs, dari file yang di download terdapat 2 file, yaitu : **1 file txt** dan **1 file php** (meskipun isinya bukanlah php)

Name	Date modified	Type
 desc.txt	26/09/2020 17:39	Text Document
 souper.php	26/09/2020 17:35	PHP File

Kita akan mengecek **desc.txt** terlebih dahulu

desc.txt - Notepad

File Edit Format View Help

Desc:

Welp, this message seems weird. I found it from my Dad's Computer when he communicates to one of his acquaintances.

Can you help me decrypt them? I'm a newbie to HTML and PHP, so ... yeah :s.

Hints:

I hope there's a place, a place that can solve and decrypt this weird messages instantly ...
But Nyeh, I'll continue to learn coding and substitute my knowledges to this algorithm.

Lalu pada file **souper.php** dapat ditemukan cipher message seperti berikut :

```
souper.php
D: > WriteUp > Souper > soupe.php
1  <?php
2  MMBT LPADN CPO, BCY KB OJG MQMOMU NOHOG, MBF TUMRN CYMK RX JEN ICHOGG. CYMK OUKGN OC HKUGRGEF MO OJG MQMOMU, RPO MMBT AGUGZX SBCESN JKN JMBF HUWK. JG EUGMOGN M RZMNO CH HKU
NGBFKBI CYMK HZKXBT RHESMULF. EPO RUKGEXN OC MB COGU OJG NDCPZFGU CH MMBT OKGV CH CYMK ROKBT HUEJGF MMBT, EUMNOKBT KBQC M DKZZMU CH UCES. JG HAZZN FCVB OC OJG TUCPBF MBF MN OJG
FMPO EZGNAN JG ZCCSN PD MO MMBT KB OJG NSX VKOJ M NODJUG CH HKU MUCPBF JKA. MMBT DUEGEGFN OC UCHU MBF EUGMOGN HKUG CPO CH JKN ACPOD, HONON MBF HGGO. MMBT EUGMOGN M AMNWKOG IPMO
CH HKU EMPNKB CYMK OC ECGU JKANZH MN JG TUCBKN KB NOUTIZZO, DKZZMUN CH GJUGJ FKNKBOGILMUG MBF ACQG OCUMUF MMBT MN COJGU DKGEGN CH UCES UONG PD HUCA OJG TUCPBF OC MNUCUPBF
MMBT. VMOGU NZMC UKNGN OCUMUF MMBT MN JG EUGMOGN M UKBT CH HKUG MUCPBF JKANGZH. OJG GJUGJ RGIXBN OC EUGMOG M UKBT KBKNGF OJG HKU NODJUG MN OJG VMOGU ECBOKBPN OC UKNG PD MBF
HCUA MBCOJGU UKBT KBKNGF OJG GJUGJ NODJUG. EPO OC CYMK VJG VMOEJGN, ECQGUUKBT JKN JGME VKOJ JKN MUJAN. EPO RMES OC MMBT MN OJG EMAGUM YCCAN CPO OC NJCV JKA NPUJCPBFGE RX M UKBT CH
VMOGU, M UKBT CH GJUGJ, M NODJUG CH HKU MBF M UKBT CH HKUG.<br />
3  OJG NEGBG EJMIGN OC OJG ZKRGUKOCB CH RN NKBT NG MN RPAS UKNGN CPO CH OJG TUCPBF VKOJ GJUGJRGFBFKBT. JG OPURN MUCPBF MN HKUG BMOKCB OMBSN MDDGRU MBF HKUG CB JKA, RPO JG RZCESN
KO VKOJ GJUGJRGFBFKBT. JG ZCVGUN OJG RPUJGU NAKZKBT. JG NJCCON UCESN MO OJG JCGZN VJUG OJG NJCCO HKUG. JG NPMRMTSGBOZX PNGN GJUGJRGFBFKBT OC NJCCO OJGA KBQC OJG HKU MBF OJGX
ZMBF DKZGF CB OCD CH CBG MBCOJGU VKZGZ OJG NCZFKGUN ECAG CPO OJG OMBS TUCBKNBT KB DMKB. EPO OC KUJC MN JG RPUJN OJG HKUG BMOKCB HZMT CB RN NKBT NG UCHMZ DMZNEG OC UGQGNZ OJG
GJUGJ SKBIFCA KBKTBKMN.<br />
4  <br />
5  OJG NEGBG EJMIGN OC MMBT MBF CYMK. MMBT EJMIGN MO CYMK, UMAAKBT JKA, MBF RZCVN JKA CH JKN GZGAGBOMZ NODJUG. CYMK HZKGN MMX HUCA MMBT. MMBT PNGN GJUGJRGFBFKBT OC NJCCO AMEJKBG
IPB-ZKSG GJUGJ RPZZGN MO JKA. MMBT EJMIGN M HZGGBBT CYMK.<br />
6  <br />
7  OJG NEGBG EJMIGN OC OJG ECAGO-GJMBEGF MITK SM. M HOV NAMZZ HZMAGN EMB RG NSGB, MBF KB OJG AKFEZG CH OJGA KN M RMEZX KBLPUGF YPSC. JG UKJGN OC IGO PD, RPO JG KN OCC JPUO HUCA
OJG ZKJIOKBT NOUKSG MBF JG HAZZN FCVB. SMOULM UPNIGN OC OJX MBF JGZO JKA, RPO MYPMZ ZMPBEJGN M HKUG RZMNO KB HUCBO CH JGU RGHUGJ NGB EMB UGMEJ JKA. NGB ZMPTJN AMBKEMZZX MBF
NOCCON ZKJIOKBT VJKEJ SMOULM FCFIGN. YPSC MOOGADON OC IGO RMES PD, RPO KN OCC VQMS MBF EMB FC BCQJKB BT RPO VMOEJ MN MYPMZ NJCCON MBCOJGU ZKJIOKBT BCZO MO SMOULM, VJKEJ NGB
FCEIGN. SMOULM OPURN OC VMOEJ MN MYPMZ ZMBFN CB M UCCH BGMURX. NGB RGIXBN EJMUKBT MBCOJGU ZKJIOKBT MOOMES.<br />
8  <br />
9  KF UGHZZX UMOJGU CPU HMAKZX DJANKKMB ZCCS MHOGU ZKOZG YPPY KH XCP FCB'D AKBF. [MYPZM NJCCON ZKJIOKBT MBF HKUG MO JGU HUCA OJG UCCH CH M RPKZFKBT. SMOULM AMBIGN OC FCFIG OJGA
HZZ MBF JXGN RGJKB BT ECPZAB BGMURX. OC YPSC KB M OMPROKBT AMBBGU, I YPPY, XCP FCB'D ZCCS NC JCCFI.<br />
10 NGB NJCCON MO SMOULM MIMKB. SMOULM AMBIGN OC FCFIG JGU MBF ACQGN RGJKB MBCOJGU ECPZAB. NGB NODON VMOGU BGMURX MBF RBBFN KO CBQC OJG UCCH, RPO MYPMZ JMN ACQGF. MYPMZ ECAGN HUCA
RGJKB BT JGU CB HKUG LGON MBF SMOULM KN HUEJGF OC HZGG. NGB PNGN OJG BGMURX VMOGU EMBBGGZ OC AMSG KEG OC NZKFG CB MN MYPMZ EJMIGN MHOGU JGU MBF HKUGN MBCOJGU RZMNO CH HKUG VJKEJ
OMDCKUYGN KO ECADZGOGZX. MYPMZ PBZGNIGN M ZMUG RPUNO CH HKUG, RPO SMOULM AMBIGN OC IGO MMX. SMOULM IGN CH JGU KEG DMOT, RPO OUKDN CB M IUMOG MBF NGN NCAG VMOGU RGTZCV. NGB
ZCCSN PD MBF TUMRN NCAG EJMKN JMBIKBT HUCA OJG VMZZ. EPO OC M VKFG-QKGV CH OJG MUJN MN MYPMZ MDOUCHEJGN OJG IUMOGN.<br />
11 <br />
12 NGB JGZGN JKA PD. MYPMZ DMON KB MBIGU, NEUGMAN KB AMFBGNN, MBF RUGMOJGN HKUG, VUKOJBT KB MB MOOGADO OC RUHGS HUGG. HKBMZZX NGB NODON MBF RGIXBN OC ELX PBECBOUCZZMRZX. SMOULM
MBF YPSC VMOEJ KB JCUUCU MBF DKOX.<br />
13 OJG NEGBG EJMIGN OC MQMOMU MMBT MBF DJCGBKN SKBT CYMK. MMBT NOKZZ EJMIGN CYMK MBF PNGN GJUGJRGFBFKBT OC ACQG OVC DKZZMUN KB HUCBO CH CYMK, VJC UGECZN MBF HZKGN MMX. MMBT NGBFN
M VMOG CH VMOGU MO CYMK, EMPNKB BT JKA OC EUMNO OC OJG TUCPBF. MN CYMK UGECQUN MBF ZCCSN PD, MMBT RPUNON OJUCPIJ OJG DKZZMU JG ZMBFGF BGMU. CYMK UGUGHON RHESMULF MBF NJCCON M
NOUGMA CH HKUG MO MMBT. KB NZCV ACOKCB. MMBT FUCDN OC OJG TUCPBF BMUUCVZX AIONKBT CYMK VJC DUCDGN JKANGZH MMX VKOJ HKUG HUCA JKN HGGO. MMBT UKNGN MBF RGIXBN HCZZCVKBT OJG
HZGGBBT CYMK MIMKB. CYMK ZMBFN CB M DKZZMU MBF ZMPBEJGN M VKFG HKUG RZMNO MO MMBT, VJC PNGN GJUGJRGFBFKBT OC ACQG OVC ZMUG DKZZMUN OC DUCGEO JKANGZH. MMBT RUGHSN MBF ZGN OJG
DKZZMUN HZZ MN CYMK HZKGN MMX MIMKB. MMBT PBZGNIGN APZOKDZG RZMNON CH HKUG OCUMUF CYMK, VJC AMBIGN OC FCFIG OJGA. CYMK ZMBFN CB OJG NKFG CH M DKZZMU MBF ZMPBEJGN OJUGG
NKAIXGN OJG HZMT KN NPNRKOPOKCBEOJGUKNCONCRMF RZMNON MO MB MDOUCHEJBT MMBT, VJC PNGN MKU MBF VMOGU OC FNDGUNG OJGA. MMBT HKUGN M NOUCBT RZMNO CH MKU MO CYMK, FKNKBOGILMOKBT
OJG DKZZMU JG NOKCF CB RPO JG AMBIGN OC IGO MMX. MMBT ECBOKBPN OC EJMNG JKA MN CYMK ZCCSN RMES, UGHZKYKBT MMBT KN EMOEJBT PD. MMBT ACQGN JKN MUA KB M EKUEPZMU ACOKCB EMPNKB BT
VMOGU OC VUMD KONGZH MUCPBF CYMK'N ZGI MBF PD OC JKN CPONUGOEJGF MUA, VJDKOKBT JKA MUCPBF, RGHUGJ NZMAAKBT JKA CB OCD CH M DKZZMU. MMBT HZKGN HCUUMUF MBF GJUGJRGFBFN CYMK'N
JMBFN MBF HGGO OC OJG TUCPBF, OUMDKBT JKA. JGZDZGN, CYMK VMOEJGN HGMUPZZX MN MMBT JCGUN CQGU JKA, JKN QCKEG GEJCKBT VKOJ OJG HPLX CH JKN DUGFEGGNNCLUN.<br />
14 <br />
15 CYMK ACQGN OC MOOMES MMBT VJC NGBNKN KO VKOJ OJG NGNAKE NGBNG JG ZGMBUG HUCA OCDJ. JG NOMADN FCVB MBF ZKHON M HCCO PD, FUMIKBT M DKZZMU CH GJUGJ HZCBI VKOJ JKA, FGHZGEOKBT
CYMK'N MOOMES MBF RKBFKBT JKA KBKNGF OJG UCES. JG EKUEZGN CYMK MBF DUEGEGFN OC RKBK JKN COJGU JMBF MN CYMK MOOGADON OC MOOMES MIMKB. JG DPZZN OJG UCESN FCVB KBQC OJG GJUGJ
NZKJIOZX, EMPNKB CYMK OC SBGGZ. CYMK MOOGADON CBG HKBMZ HKUG RUGHOJ MOOMES, RPO MMBT PNGN MKURGFBFKBT OC NODC MBF MDOUCHEJ JKA MBF DPON CBG JMBF CB CYMK'N HCUJGGMF, MBF CBG CB
JKN EJGNO, VJKEJ JG VMOEJGN KB JCUUCU.<br />
16 MMBT EZCHGN JKN GXGN MBF KO HZMIGN RMES OC MMBIN AGGOKBT VKOJ OJG ZKCB OPUOZG.
17 ?]
```

Kembali melihat ke desc.txt kita dapat menduga bahwa cipher message tersebut merupakan **subtitusi character**, tapi subtitusi tersebut bukanlah caesar karena subtitusi tersebut tidak jelas.

Menggunakan online decoder dari <https://quipqiup.com/> yang dapat digunakan sebagai **Cryptogram Solver**, hasil yang di dapatkan adalah sebagai berikut :

0 -1.551 AANG JUMPS OUT, NOW IN THE AVATAR STATE, AND GRABS OZAI BY HIS GOATEE. OZAI TRIES TO FIREBEND AT THE AVATAR, BUT AANG MERELY KNOCKS HIS HAND AWAY. HE CREATES A BLAST OF AIR SENDING OZAI FLYING BACKWARD. CUT BRIEFLY TO AN OVER THE SHOULDER OF AANG VIEW OF OZAI BEING FORCED AWAY, CRASHING INTO A PILLAR OF ROCK. HE FALLS DOWN TO THE GROUND AND AS THE DUST CLEARS HE LOOKS UP AT AANG IN THE SKY WITH A SPHERE OF AIR AROUND HIM. AANG PROCEEDS TO ROAR AND CREATES FIRE OUT OF HIS MOUTH, FISTS AND FEET. AANG CREATES A MASSIVE GUST OF AIR CAUSING OZAI TO COVER HIMSELF AS HE GROANS IN STRUGGLE. PILLARS OF EARTH DISINTEGRATE AND MOVE TOWARD AANG AS OTHER PIECES OF ROCK RISE UP FROM THE GROUND TO SURROUND AANG. WATER ALSO RISES TOWARD AANG AS HE CREATES A RING OF FIRE AROUND HIMSELF. THE EARTH BEGINS TO CREATE A RING INSIDE THE AIR SPHERE AS THE WATER CONTINUES TO RISE UP AND FORM ANOTHER RING INSIDE THE EARTH SPHERE. CUT TO OZAI WHO WATCHES, COVERING HIS HEAD WITH HIS ARMS. CUT BACK TO AANG AS THE CAMERA ZOOMS OUT TO SHOW HIM SURROUNDED BY A RING OF WATER, A RING OF EARTH, A SPHERE OF AIR AND A RING OF FIRE. THE SCENE CHANGES TO THE LIBERATION OF BA SING SE AS BUMI RISES OUT OF THE GROUND WITH EARTHBENDING. HE TURNS AROUND AS FIRE NATION TANKS APPEAR AND FIRE ON HIM, BUT HE BLOCKS IT WITH EARTHBENDING. HE LOWERS THE BARRIER SMILING. HE SHOOTS ROCKS AT THE HOLES WHERE THEY SHOOT FIRE. HE SUBSEQUENTLY USES EARTHBENDING TO SHOOT THEM INTO THE AIR AND THEY LAND PILED ON TOP OF ONE ANOTHER WHILE THE SOLDIERS COME OUT THE TANK GROANING IN PAIN. CUT TO IROH AS HE BURNS THE FIRE NATION **FLAG** ON BA SING SE ROYAL PALACE TO REVEAL THE EARTH KINGDOM INSIGNIA. THE SCENE CHANGES TO AANG AND OZAI. AANG CHARGES AT OZAI, RAMMING HIM, AND BLOWS HIM OFF HIS ELEMENTAL SPHERE. OZAI FLIES AWAY FROM AANG. AANG USES EARTHBENDING TO SHOOT MACHINE GUN-LIKE EARTH BULLETS AT HIM. AANG CHASES A FLEEING OZAI. THE SCENE CHANGES TO THE COMET-ENHANCED AGNI KAI. A FEW SMALL FLAMES CAN BE SEEN, AND IN THE MIDDLE OF THEM IS A BADLY INJURED ZUKO. HE TRIES TO GET UP, BUT HE IS TOO HURT FROM THE LIGHTNING STRIKE AND HE FALLS DOWN. KATARA RUSHES TO TRY AND HELP HIM, BUT AZULA LAUNCHES A FIRE BLAST IN FRONT OF HER BEFORE SHE CAN REACH HIM. SHE LAUGHS MANICALLY AND SHOOTS LIGHTNING BOLT AT KATARA DODGES. ZUKO ATTEMPTS TO GET BACK UP, BUT IS TOO WEAK AND CAN DO NOTHING BUT WATCH AS AZULA SHOOTS ANOTHER LIGHTNING BOLT AT KATARA, WHICH SHE DODGES. KATARA TURNS TO WATCH AS AZULA LANDS ON A ROOF NEARBY. SHE BEGINS CHARGING ANOTHER LIGHTNING ATTACK. ID REALLY RATHER OUR FAMILY PHYSICIAN LOOK AFTER LITTLE ZUKU IF YOU DON'T MIND. [AZULA SHOOTS LIGHTNING AND FIRE AT HER FROM THE ROOF OF A BUILDING. KATARA MANAGES TO DODGE THEM ALL AND HIDES BEHIND A COLUMN NEARBY. TO ZUKO IN A TAUNTING MANNER.] ZUKU, YOU DON'T LOOK SO GOOD! SHE SHOOTS AT KATARA AGAIN. KATARA MANAGES TO DODGE HER AND MOVES BEHIND ANOTHER COLUMN. SHE SPOTS WATER NEARBY AND BENDS IT ONTO THE ROOF, BUT AZULA HAS MOVED. AZULA COMES FROM BEHIND HER ON FIRE JETS AND KATARA IS FORCED TO FLEE. SHE USES THE NEARBY WATER CHANNEL TO MAKE ICE TO SLIDE ON AS AZULA CHASES AFTER HER AND FIRES ANOTHER BLAST OF FIRE WHICH VAPORIZES IT COMPLETELY. AZULA UNLEASHES A LARGE BURST OF FIRE, BUT KATARA MANAGES TO GET AWAY. KATARA GETS OFF HER ICE PATH, BUT TRIPS ON A GRATE AND SEES SOME WATER BELOW. SHE LOOKS UP AND GRABS SOME CHAINS HANGING FROM THE WALL. CUT TO A WIDE-VIEW OF THE AREA AS AZULA APPROACHES THE GRATES. SHE HELPS HIM UP. AZULA PANTS IN ANGER, SCREAMS IN MADNESS, AND BREATHES FIRE, WRITHING IN AN ATTEMPT TO BREAK FREE. FINALLY SHE STOPS AND BEGINS TO CRY UNCONTROLLABLY. KATARA AND ZUKO WATCH IN HORROR AND PITY. THE SCENE CHANGES TO AVATAR AANG AND PHOENIX KING OZAI. AANG STILL CHASES OZAI AND USES EARTHBENDING TO MOVE TWO PILLARS IN FRONT OF OZAI, WHO RECOILS AND FLIES AWAY. AANG SENDS A WAVE OF WATER AT OZAI, CAUSING HIM TO CRASH TO THE GROUND. AS OZAI RECOVERS AND LOOKS UP, AANG BURSTS THROUGH THE PILLAR HE LANDED NEAR. OZAI RETREATS BACKWARD AND SHOOTS A STREAM OF FIRE AT AANG. IN SLOW MOTION, AANG DROPS TO THE GROUND NARROWLY MISSING OZAI WHO PROPELS HIMSELF AWAY WITH FIRE FROM HIS FEET. AANG RISES AND BEGINS FOLLOWING THE FLEEING OZAI AGAIN. OZAI LANDS ON A PILLAR AND LAUNCHES A WIDE FIRE BLAST AT AANG, WHO USES EARTHBENDING TO MOVE TWO LARGE PILLARS TO PROTECT HIMSELF. AANG BREAKS AND LETS THE PILLARS FALL AS OZAI FLIES AWAY AGAIN. AANG UNLEASHES MULTIPLE BLASTS OF FIRE TOWARD OZAI, WHO MANAGES TO DODGE THEM. OZAI LANDS ON THE SIDE OF A PILLAR AND LAUNCHES THREE SIMILAR THE **FLAG** IS SUBSTITUTIONCIPHERISNOTSOBAD BLASTS AT AN APPROACHING AANG, WHO USES AIR AND WATER TO DISPERSE THEM. AANG FIRES A STRONG BLAST OF AIR AT OZAI, DISINTEGRATING THE PILLAR HE STOOD ON BUT HE MANAGES TO GET AWAY. AANG CONTINUES TO CHASE HIM AS OZAI LOOKS BACK, REALIZING AANG IS CATCHING UP. AANG MOVES HIS ARM IN A CIRCULAR MOTION CAUSING WATER TO WRAP ITSELF AROUND OZAI'S LEG AND UP TO HIS OUTSTRETCHED ARM, WHIPPING HIM AROUND, BEFORE SLAMMING HIM ON TOP OF A PILLAR. AANG FLIES FORWARD AND EARTHBENDS OZAI'S HANDS AND FEET TO THE GROUND, TRAPPING HIM. HELPLESS, OZAI WATCHES FEARFULLY AS AANG HOVERS OVER HIM, HIS VOICE ECHOING WITH THE FURY OF HIS PREDECESSORS. OZAI MOVES TO ATTACK AANG WHO SENSES IT WITH THE SEISMIC SENSE HE LEARNED FROM TOPH. HE STAMPS DOWN AND LIFTS A FOOT UP, DRAGGING A PILLAR OF EARTH ALONG WITH HIM, DEFLECTING OZAI'S ATTACK AND BINDING HIM INSIDE THE ROCK. HE CIRCLES OZAI AND PROCEEDS TO BIND HIS OTHER HAND AS OZAI ATTEMPTS TO ATTACK AGAIN. HE PULLS THE ROCKS DOWN INTO THE EARTH SLIGHTLY, CAUSING OZAI TO KNEEL. OZAI ATTEMPTS ONE FINAL FIRE BREATH ATTACK, BUT AANG USES AIRBENDING TO STOP AND APPROACH HIM AND PUTS ONE HAND ON OZAI'S FOREHEAD, AND ONE ON HIS CHEST, WHILE HE WATCHES IN HORROR. AANG CLOSSES HIS EYES AND IT FLASHES BACK TO AANGS MEETING WITH THE LION TURTLE.

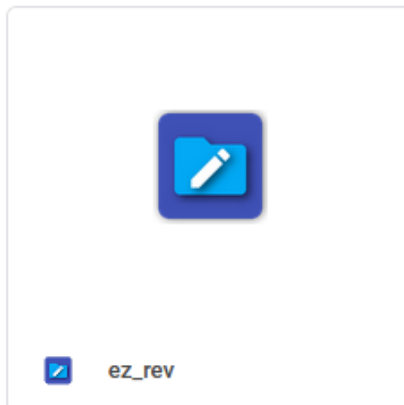
Dari hasil decode tersebut ketika kita mencari kata **flag**, dapat menemukan 2 kata di mana salah satunya berisikan flagnya.

HACKLABS{ SUBSTITUTIONCIPHERISNOTSOBAD }

Ez-Rev (Reverse Engineering)



Sama halnya dengan challenge yang sebelum-sebelumnya, di mana kita mendownload file dari drive hacklabs.id



Okay..Okay wait,
My friend just sent me this file and my Desktop keeps saying that
IT IS A VIRUS.

I wonder what kind of file is that?
It doesn't seem to be that dangerous, right??

First thing First, I want to know the type of this file and
what can I do with it.

Can you help me?

```
root@opacite:~# file ez_rev
ez_rev: ELF 64-bit LSB shared object, x86_64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=7b94218dd7dbe13fd8d84d97b3d31c4f196876ad, for GNU/Linux 3.2.0, not stripped
root@opacite:~#
```

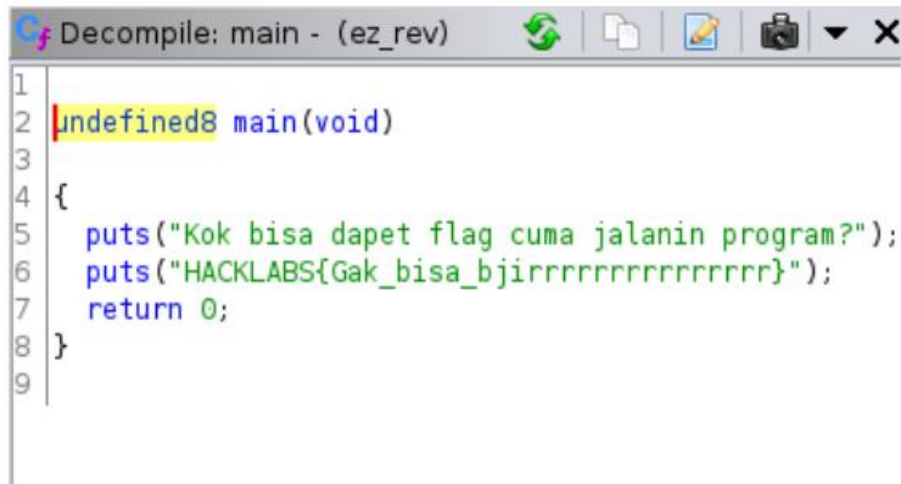
```
root@opacite:~# chmod +x ez_rev  
root@opacite:~# ./ez_rev  
Kok bisa dapet flag cuma jalanin program?  
HACKLABS{Gak_bisa_bjirrrrrrrrrrrrrrrrrr}  
root@opacite:~#
```

Unintended way :

```
00000000000004040 48 41 43 4B 4C 41 42 53 7B 54 68 65 5F 72 65 61 HACKLABS{The_rea
00000000000004050 6C 5F 66 6C 61 67 5F 45 7A 5F 53 74 72 69 6E 67 l_flag_Ez_String
00000000000004060 73 7D 00 ?? ?? ?? ?? ?? ?? ?? s}.??????.....
00000000000004070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

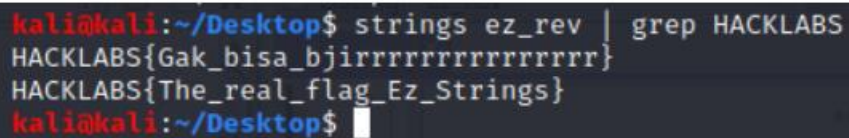
```

Dari Official Writeup yang ada, cara yang benar adalah sebagai berikut :



```
Decompile: main - (ez_rev)
1
2 undefined8 main(void)
3
4 {
5     puts("Kok bisa dapet flag cuma jalanin program?");
6     puts("HACKLABS{Gak_bisa_bjirrrrrrrrrrrrrrrrrrr}");
7     return 0;
8 }
9
```

Asumsi saya, **flag** sebenarnya berupa **strings independent** yang terdapat dalam *binary* file ini. Seharusnya, partisipan dapat melihatnya langsung dengan command **strings** <nama file> | **grep** HACKLABS



```
kali@kali:~/Desktop$ strings ez_rev | grep HACKLABS
HACKLABS{Gak_bisa_bjirrrrrrrrrrrrrrrrrrr}
HACKLABS{The_real_flag_Ez_Strings}
kali@kali:~/Desktop$
```

Sehingga dapat dipastikan flag dari challenge ini adalah

HACKLABS{The_real_flag_Ez_Strings}

Srand (Cryptography)



Challenge ini dimulai dengan diberikannya **3 file, 2 file txt & 1 file py**. Sebelum melanjutkan melihat challengenya, kita akan melihat terlebih dahulu deskripsi dari challenge ini.

Desc:

I've just studied C language and now I must
study a Snake language `--` ?

And what the heck is a seed ..?

Dari dekripsi tersebut, dapat dipastikan kita akan menggunakan bahasa **python** untuk menyelesaikan challenge ini, sehingga pengetahuan basic python dibutuhkan terlebih hint mengenai **Seed**. Dan kita dapat melihat txt berikutnya bernama encrypted.txt yang isinya adalah berikut :

```
G  fx pwW\ ! {Fdr z dLMr5V
```

Dan file terakhir yang merupakan file python, berisi kan seperti ini :

```
Srand.py X
C: > Users > Alexander Michael > Downloads > Srand.py > ...
1  import random
2
3  key = "SuP3rs3cR3tK3y"
4
5  random.seed(key)
6  flag = "REDACTED"
7
8  encrypted = ""
9  for c in flag:
10     encrypted += chr(ord(c) ^ random.randint(1,100))
11
12  with open('encrypted.txt', 'w') as f:
13     f.write(encrypted)
14
```

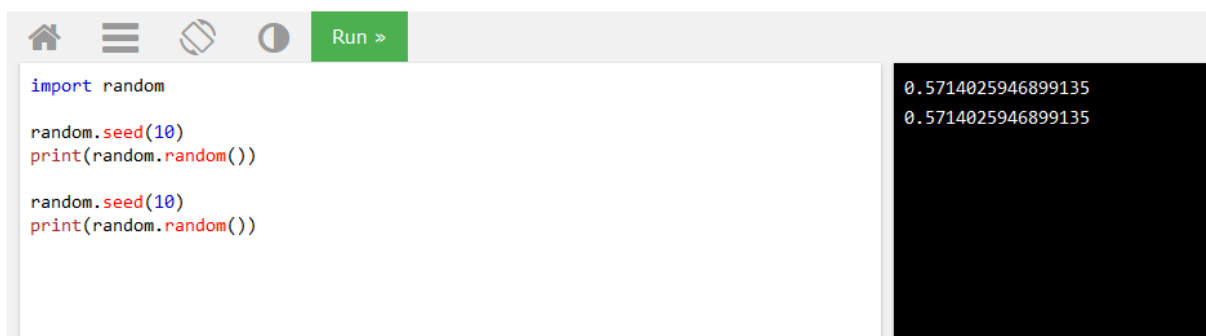
Dari bahasa python tersebut dapat dilihat bahwa saat melakukan enkripsi flag, digunakan function **XOR** yang artinya pengetahuan dasar XOR juga dibutuhkan :

$$A \wedge B = C$$

$$A \wedge C = B$$

$$B \wedge C = A$$

Selain **XOR**, kita dapat melihat variable key "SuP3rs3cR3tK3y" lalu terdapat **random.seed()** yang berfungsi untuk melakukan random number generator berdasarkan seed yang digunakan



```
import random

random.seed(10)
print(random.random())

random.seed(10)
print(random.random())
```

```
0.5714025946899135
0.5714025946899135
```

Contoh di atas diambil dari w3schools, dapat diambil kesimpulan bahwa integer tersebut memang akan random namun sifatnya menjadi **static** jika menggunakan **seed** yang sama.

Dengan merubah codingan yang diberikan, menjadi seperti berikut

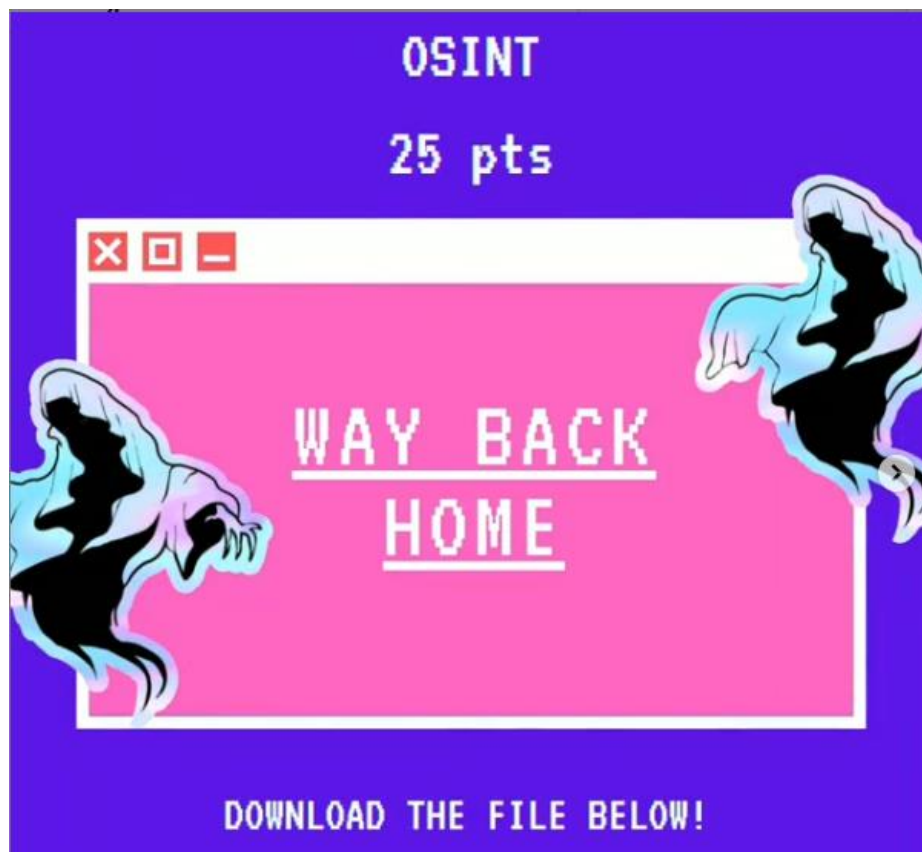
```
Srand.py X
C:\Users\Alexander Michael\Downloads> Srand.py > ...
1  import random
2
3  key = "SuP3rs3cR3tK3y"
4  random.seed(key)
5
6  # random.seed(key)
7  # flag = "REDACTED"
8
9  # encrypted = ""
10 # for c in flag:
11 #     encrypted += chr(ord(c) ^ random.randint(1,100))
12
13 # with open('encrypted.txt', 'w') as f:
14 #     f.write(encrypted)
15
16 with open('encrypted.txt', 'r') as f:
17     enc_flag = f.read()
18
19 decrypt = ""
20
21
22 for c in enc_flag:
23     decrypt += chr(ord(c) ^ random.randint(1,100))
24
25 print(decrypt)
26
```

Kita dapat mendapatkan hasil seperti berikut :

```
C:\Users\Alexander Michael\Downloads>python Srand.py
HACKLABS{St4t1c_k3Y_1s_B4d}
C:\Users\Alexander Michael\Downloads>
```

HACKLABS{St4t1c_k3Y_1s_B4d}

Way Back Home (OSINT)



Seperti challenge di HackLabs pada umumnya, di mana pertama kita akan diarahkan ke drive dari HackLabs.id dan kalin ini di dalam drive tersebut hanya ada 1 file txt, yang berisikan hintnya serta deskripsi soal

Way Back Home (Easy - Med)

Kepolisian Perancis mencurigai seorang pengguna Twitter bernama Opacite101 merupakan seorang mata-mata dari masa lampau, dapatkah kalian membantu kepolisian Perancis membuktikan hal tersebut?

Hint 1 : Look at every detail

Hint 2 : be careful for fake flag

Dari soal tersebut kita mempunyai clue untuk masuk ke twitter bernama Opacite101, setelah melakukan pengecekan berkali-kali saya mendapatkan beberapa hal menarik.

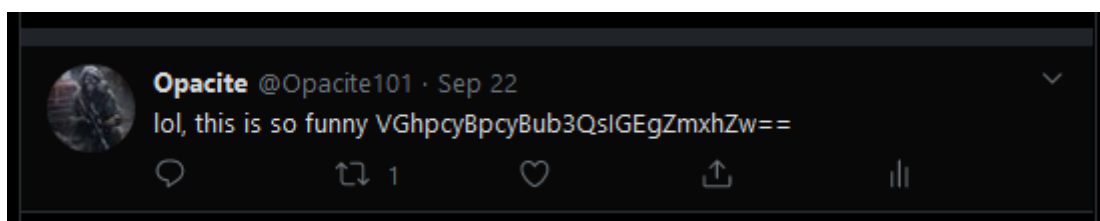
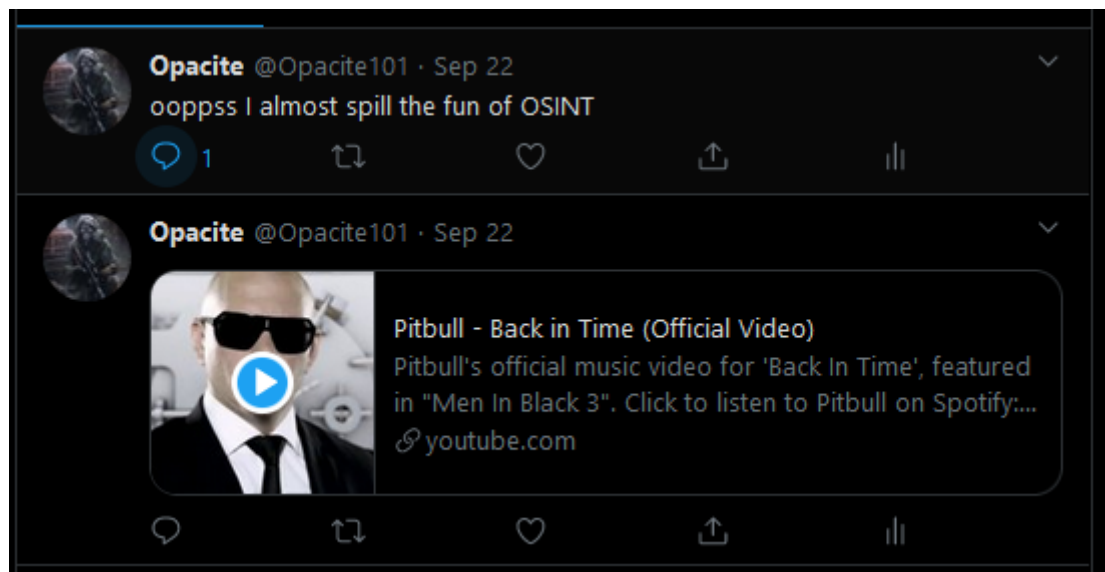
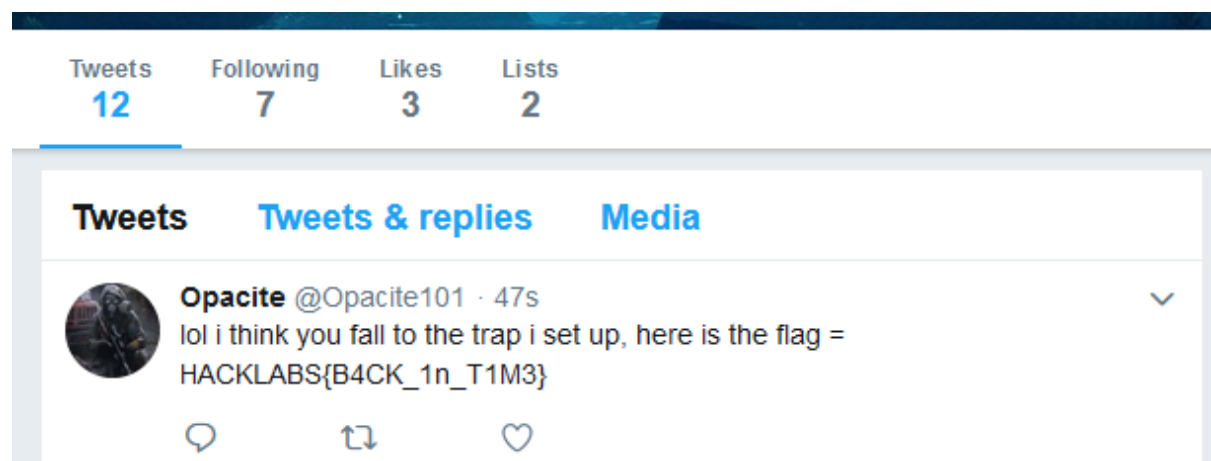


Foto tweet di atas bisa dipastikan merupakan flag palsu karna ketika saya mendecrypt base64 tersebut hasilnya adalah "This is not, a flag".



Kedua tweet di atas menurut saya cukup mencurigakan di mana lagu yang ada memiliki kata yang sama yaitu “Back” yang artinya kembali, dan tweet paling atas mengatakan bahwa akun tersebut hampir membocorkan sesuatu, dari kedua tweet ini saya menarik kesimpulan bahwa ada sesuatu yang ditweet namun kemudian dihapus, dan itu terjadi di sebelum tweet diatas diposting, oleh karna itu saya mencoba menggunakan Way Back Machine (<https://web.archive.org/>)

Kemudian setelah memasukkan URL dari twitter account Opacite101, saya menemukan sesuatu yang menarik yaitu tweet yang dihapus oleh akun tersebut dan tweet tersebut mengandung flag yang dibutuhkan



HACKLABS{B4CK_1n_T1M3}

Image Integrity (Forensics)



Pada challenge kali ini, kita diharuskan mendownload file zip yang berisikan suatu gambar dan sebuah file dekripsi challengenya, mari kita fokus ke deskripsi challenge nya terlebih dahulu

```
desc.txt - Notepad
File Edit Format View Help
desc
-----
After dealing with Monalisa Fraud,
Sherlock and I went to the premiere of Now You See Me
movie 2 years ago and we found this strange image which was
left by a woman in red.

There was this piece of paper wrapped besides it,
"The closer you look, the less you'll see
Can you use the hook, to reveal the hidden sea.."

-----
Hint #1 : I believe there's something hidden in there.
          But we haven't got a clue. What's the wrapped-paper mean
          to you?

Hint #2 : If you are using a tools called "stegsolve",
          you'll see something suspicious, a discoloured
          parts. I believe that'll lead to a conclusion too right?
          It's not that easy.

Hint #3 : You can't open the file if the file is corrupted.
          Really?
```

Berdasarkan dari clue yang diberikan, kata "hook" mengacu kepada mengait yang artinya ada sesuatu yang dikait dan ditarik, dan ketika kita membuka file gambar yang ada pada file zip tadi, kita dapat melihat isi gambar tersebut adalah sebagai berikut

NOW YOU SEE ME

Dan mengikuti saran dari desc.txt di mana menggunakan stegsolve, saya pun menggunakan stegsolve dan mendapatkan suatu hal



Terdapat warna yang berbeda pada kedua huruf E, dan ini membuat saya pusing hingga akhirnya saya berdiskusi dengan orang yang membuat challenge, dan dia mengatakan bahwa terdapat height dan width yang bisa diubah menggunakan hex editor.

4.1.1. IHDR Image header

The IHDR chunk must appear FIRST. It contains:

Width:	4 bytes
Height:	4 bytes
Bit depth:	1 byte
Color type:	1 byte
Compression method:	1 byte
Filter method:	1 byte
Interlace method:	1 byte

Dari foto di atas, kita mengetahui bahwa IHDR mempunyai width dan height, dan itulah yang akan kita rubah menggunakan hex editor, saya mendapatkan hasil seperti berikut



Setelah merubah bytes height dari foto yang diberikan sebanyak +16 sehingga dari 120 menjadi 136, hasilnya adalah memunculkan flag yang ada

HACKLABS{yea_you_cant_see_me_b4_>: } !}