Frida ile Linux Binary Instrumentation

—

Ahmet Bilal Can

android, malware, frida, reverse, ctf ..

0xabc0

İçindekiler :

- flareon
- challenge 6/12
- frida nedir, ne yapar
- sorumuzun çözümü (pray for demo gods)

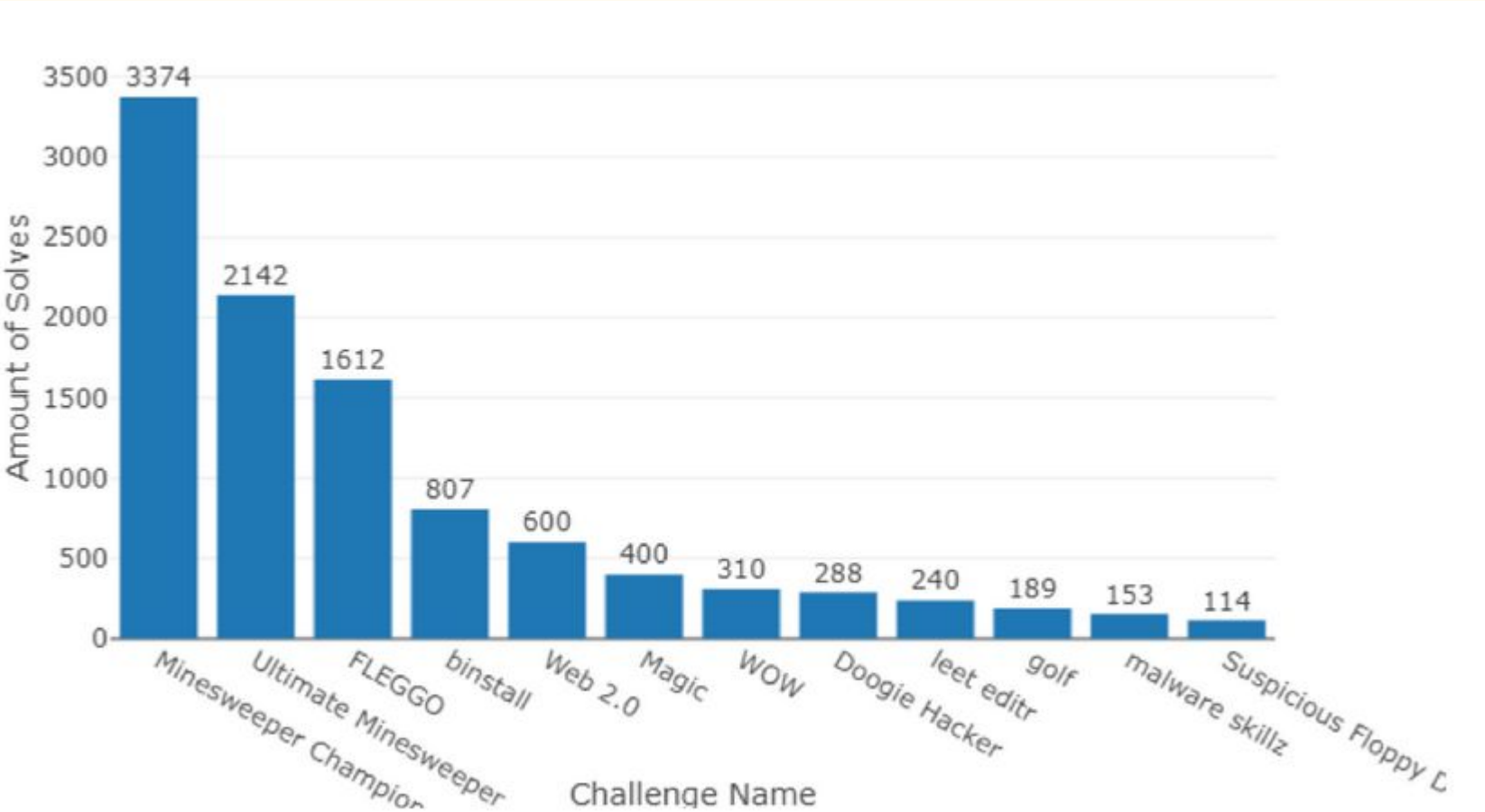
Flareon ?

http://flare-on.com

Windows odaklı 12 adet tersine mühendislik sorusu

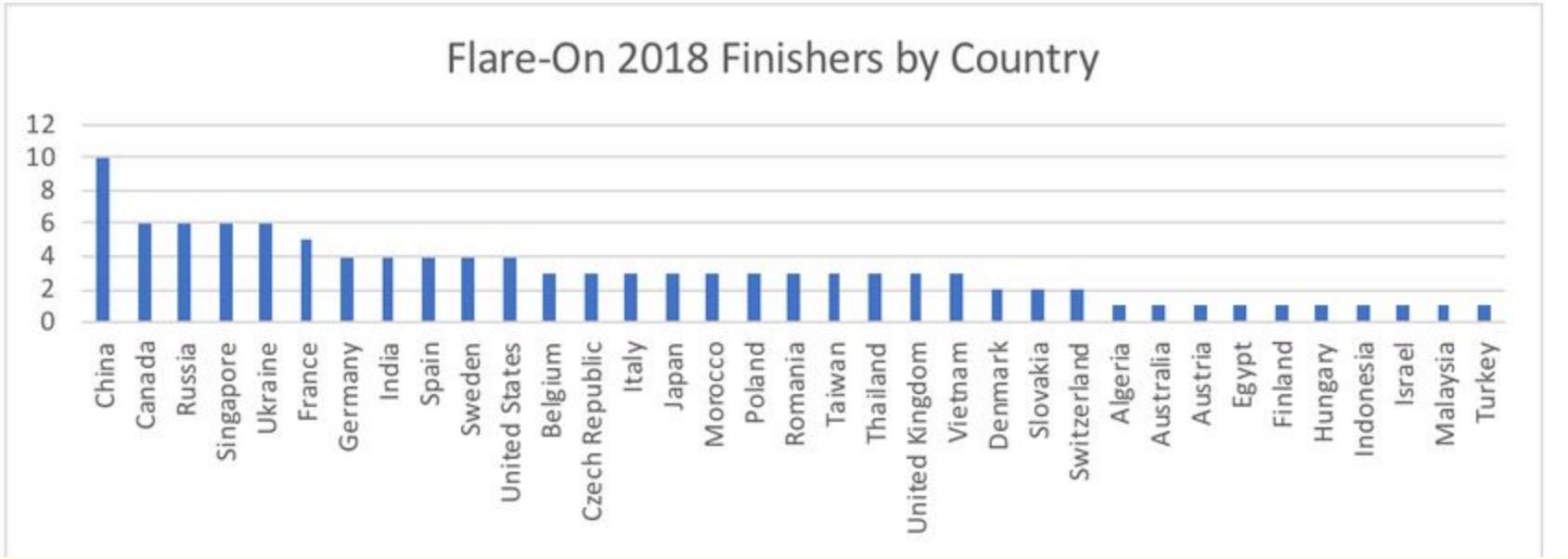
6 Hafta

FireEye

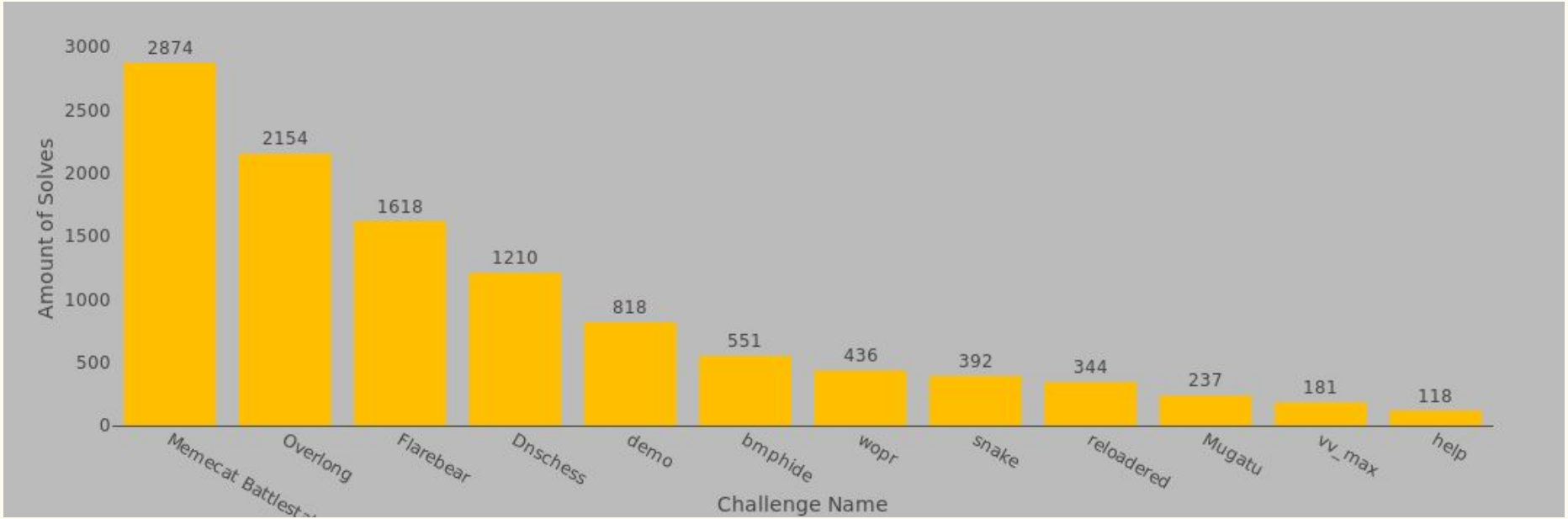

Amount of Solves
3500
3000
2500
2000
1500
1000
500
0
3374
2142
1612
807
600
400
310
288
240
189
153
114
Minesweeper Champion
Ultimate Minesweeper
FLEGGO
binstall
Web 2.0
Magic
WOW
Doogie Hacker
leet editr
golf
malware skillz
Suspicious Floppy D
Challenge Name


FIREEYE FLARE-ON CHALLENGE
REVERSE ENGINEER
2017
REVERSE ENGINEER
FLARE
FLARE
FLARE
FLARE
0x16


FLARE
FIREEYE FLARE ADVANCED REVERSE ENGINEERING TEAM CHALLENGE
SILENTIUM EST AUREUM
FIREEYE FLARE-ON CHALLENGE
REVERSE ENGINEER
2018
FLARE


Flare-On 2018 Finishers by Country
12
10
8
6
4
2
0
China
Canada
Russia
Singapore
Ukraine
France
Germany
India
Spain
Sweden
United States
Belgium
Czech Republic
Italy
Japan
Morocco
Poland
Romania
Taiwan
Thailand
United Kingdom
Vietnam
Denmark
Slovakia
Switzerland
Algeria
Australia
Austria
Egypt
Finland
Hungary
Indonesia
Israel
Malaysia
Turkey

Flareon 2019 ? Hala devam ediyor !



Challenge 6 : Magic

```
→  flareon5 file magic
magic: ELF 64-bit LSB executable, x86-64,
48effe87, stripped
```

```
→  flareon5 ./magic
Welcome to the ever changing magic mushroom!
666 trials lie ahead of you!
Challenge 1/666. Enter key:
```

Decompile: main - (magic)

```
85    do {
86      if (0x299 < c) {
87        printf("Congrats! Here is your price:\n%s\n",&flag);
88        uVar2 = 0;
89  LAB_00403c03:
90        if (local_20 != *(in_FS_OFFSET + 0x28)) {
91                        /* WARNING: Subroutine does not return */
92          __stack_chk_fail();
93        }
94        return uVar2;
95      }
96      printf("Challenge %d/%d. Enter key: ",c + 1,0x29a,c + 1);
97      r_fget = fgets(buf,0x80,stdin);
98      if (r_fget == 0x0) {
99        uVar2 = 0xffffffff;
100       goto LAB_00403c03;
101     }
102     len = strlen(buf);
103     importante(buf,len,local_128);
104     i = 0;
105     while( true ) {
106       len_ = strlen(buf);
107       if (len_ <= i) break;
108       *(&flag + i) = *(&flag + i) ^ *(buf + i);
109       i = i + 1;
110     }
111     FUN_004037bf(*puParm2);
112     c = c + 1;
113   } while( true );
114 }
115
```

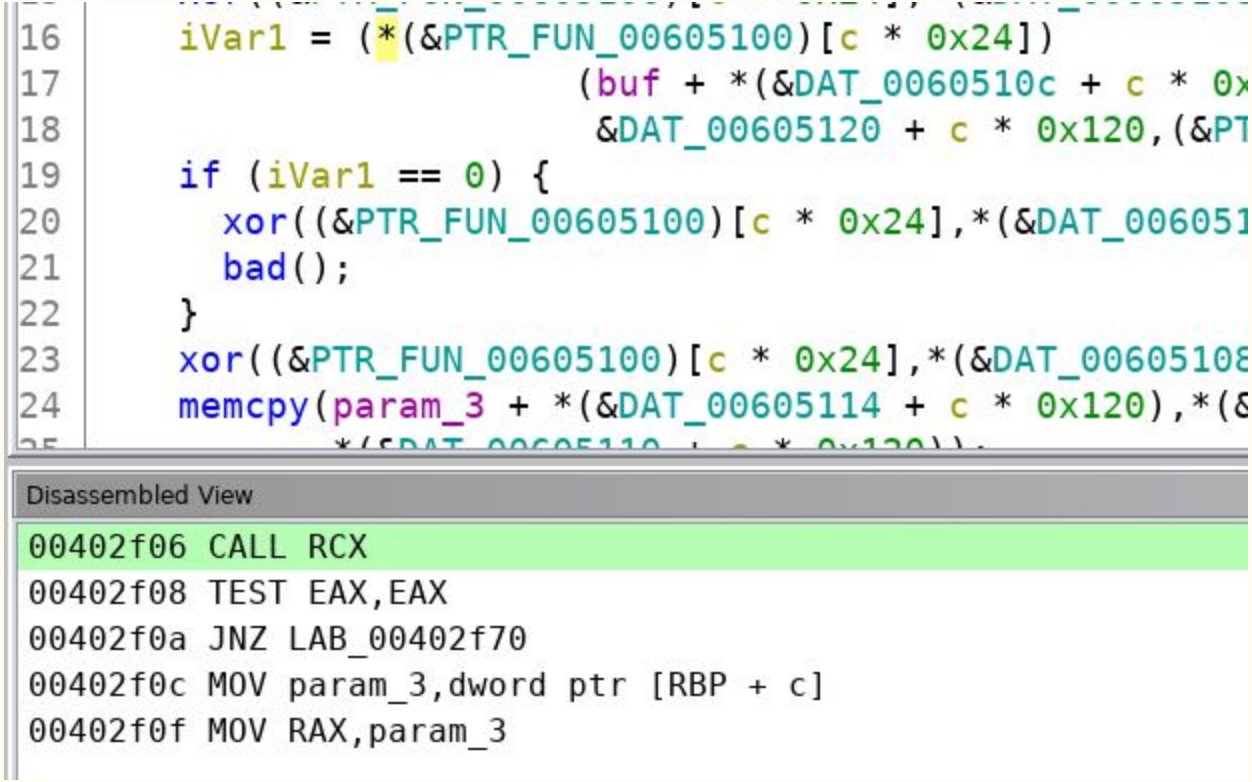
Decompile: importante - (magic)

```
1
2  /* DISPLAY WARNING: Type casts are NOT being printed */
3
4  void importante(long buf,ulong len,long param_3)
5
6  {
7    int iVar1;
8    uint c;
9
10   c = 0;
11   while (c < 0x21) {
12     if (len < *(&DAT_00605110 + c * 0x120) + *(&DAT_0060510c + c * 0x120)) {
13       bad();
14     }
15     xor((&PTR_FUN_00605100)[c * 0x24],*(&DAT_00605108 + c * 0x120),(&PTR_DAT_00605118)[c * 0x24]);
16     iVar1 = (*(&PTR_FUN_00605100)[c * 0x24])
17                       (buf + *(&DAT_0060510c + c * 0x120),*(&DAT_00605110 + c * 0x120),
18                        &DAT_00605120 + c * 0x120,(&PTR_FUN_00605100)[c * 0x24]);
19     if (iVar1 == 0) {
20       xor((&PTR_FUN_00605100)[c * 0x24],*(&DAT_00605108 + c * 0x120),(&PTR_DAT_00605118)[c * 0x24]);
21       bad();
22     }
23     xor((&PTR_FUN_00605100)[c * 0x24],*(&DAT_00605108 + c * 0x120),(&PTR_DAT_00605118)[c * 0x24]);
24     memcpy(param_3 + *(&DAT_00605114 + c * 0x120),*(&DAT_0060510c + c * 0x120) + buf,
25            *(&DAT_00605110 + c * 0x120));
26     c = c + 1;
27   }
28   return;
29 }
30
```

```
4  void bad(void)
5
6  {
7    puts("No soup for you!");
8                          /* WARNING: Subroutine does not return */
9    exit(1);
10 }
```

Decompile: xor - (magic)

```
1
2  /* DISPLAY WARNING: Type casts are NOT being printed */
3
4  void xor(char *src,ulong len,char *dst)
5
6  {
7    ulong c;
8
9    if (dst != 0x0) {
10     c = 0;
11     while (c < len) {
12       src[c] = dst[c] ^ src[c];
13       c = c + 1;
14     }
15   }
16   return;
17 }
18
```

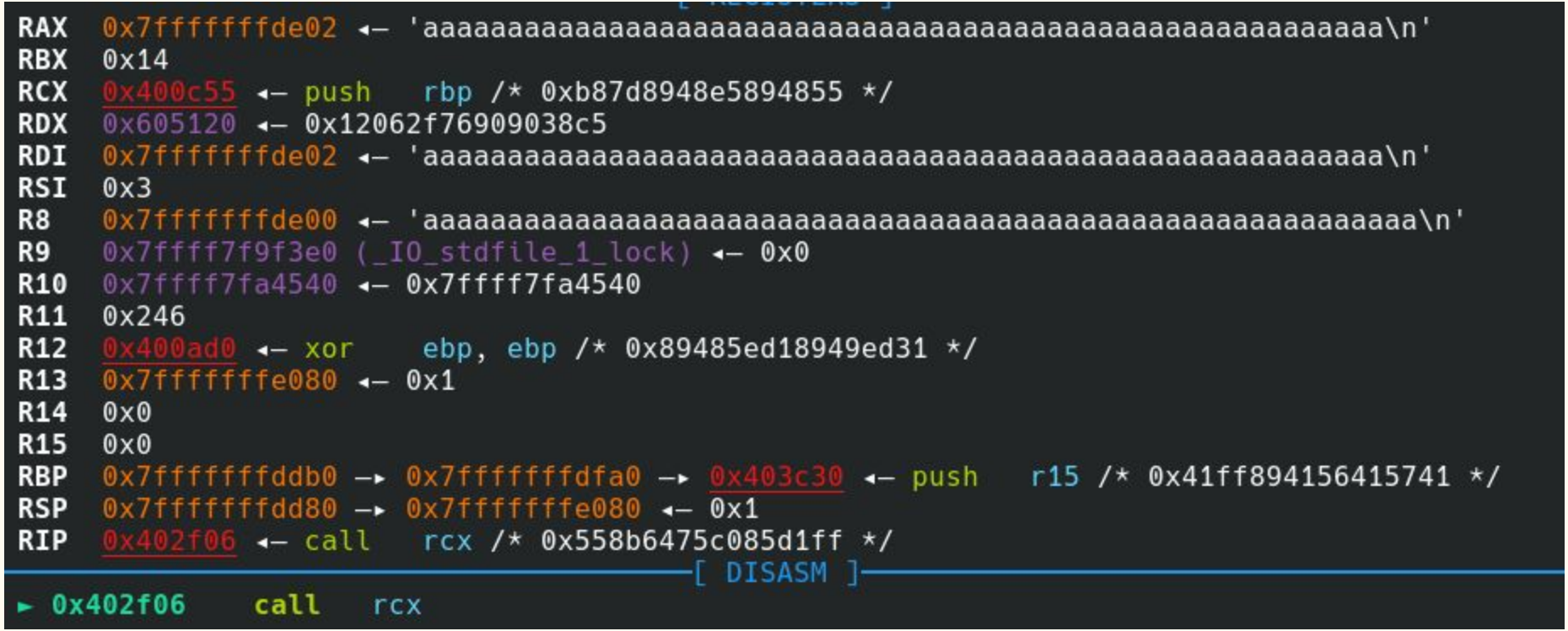

16 iVar1 = (*(&PTR_FUN_00605100)[c * 0x24])
17 (buf + *(&DAT_0060510c + c * 0x
18 &DAT_00605120 + c * 0x120,(&PT
19 if (iVar1 == 0) {
20 xor((&PTR_FUN_00605100)[c * 0x24],*(&DAT_006051
21 bad();
22 }
23 xor((&PTR_FUN_00605100)[c * 0x24],*(&DAT_00605108
24 memcpy(param_3 + *(&DAT_00605114 + c * 0x120),*(&
Disassembled View
00402f06 CALL RCX
00402f08 TEST EAX,EAX
00402f0a JNZ LAB_00402f70
00402f0c MOV param_3,dword ptr [RBP + c]
00402f0f MOV RAX,param_3

x64 calling convention ?

Fonksiyona giren parametreler sirasiyla hangi registerlara gidiyor ?

Decompile: importante - (magic)

```
1
2  /* DISPLAY WARNING: Type casts are NOT being printed */
3
4  void importante(long buf,ulong len,long param_3)
5
6  {
7    int iVar1;
8    uint c;
9
10   c = 0;
11   while (c < 0x21) {
12     if (len < *(&DAT_00605110 + c * 0x120) + *(&DAT_0060510c + c * 0x120)) {
13       bad();
14     }
15     xor((&PTR_FUN_00605100)[c * 0x24],*(&DAT_00605108 + c * 0x120),(&PTR_DAT_00605118)[c * 0x24]);
16     iVar1 = (*(&PTR_FUN_00605100)[c * 0x24])
17                       (buf + *(&DAT_0060510c + c * 0x120),*(&DAT_00605110 + c * 0x120),
18                        &DAT_00605120 + c * 0x120,(&PTR_FUN_00605100)[c * 0x24]);
19     if (iVar1 == 0) {
20       xor((&PTR_FUN_00605100)[c * 0x24],*(&DAT_00605108 + c * 0x120),(&PTR_DAT_00605118)[c * 0x24]);
21       bad();
22     }
23     xor((&PTR_FUN_00605100)[c * 0x24],*(&DAT_00605108 + c * 0x120),(&PTR_DAT_00605118)[c * 0x24]);
24     memcpy(param_3 + *(&DAT_00605114 + c * 0x120),*(&DAT_0060510c + c * 0x120) + buf,
25            *(&DAT_00605110 + c * 0x120));
26     c = c + 1;
27   }
28   return;
29 }
30
```


RAX 0x7fffffffde02 ◂— 'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa\n'
RBX 0x14
RCX 0x400c55 ◂— push rbp /* 0xb87d8948e5894855 */
RDX 0x605120 ◂— 0x12062f76909038c5
RDI 0x7fffffffde02 ◂— 'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa\n'
RSI 0x3
R8 0x7fffffffde00 ◂— 'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa\n'
R9 0x7ffff7f9f3e0 (_IO_stdfile_1_lock) ◂— 0x0
R10 0x7ffff7fa4540 ◂— 0x7ffff7fa4540
R11 0x246
R12 0x400ad0 ◂— xor ebp, ebp /* 0x89485ed18949ed31 */
R13 0x7fffffffe080 ◂— 0x1
R14 0x0
R15 0x0
RBP 0x7fffffffddb0 —▸ 0x7fffffffdfa0 —▸ 0x403c30 ◂— push r15 /* 0x41ff894156415741 */
RSP 0x7fffffffdd80 —▸ 0x7fffffffe080 ◂— 0x1
RIP 0x402f06 ◂— call rcx /* 0x558b6475c085d1ff */
[DISASM]
► 0x402f06 call rcx

```
pwndbg> x /20x 0x605100
0x605100:       0x00400c55      0x00000000      0x00000147      0x00000002
0x605110:       0x00000003      0x00000025      0x0061385a      0x00000000
0x605120:       0x909038c5      0x12062f76      0x287bce2d      0x0ec9b9e4
0x605130:       0x0035c7e2      0x00000000      0x00000000      0x00000000
0x605140:       0x00000000      0x00000000      0x00000000      0x00000000
```

Base+0x8 //xor key

Base+0xc //index

Base+0x10 //len

Base // function

Base+0x18 //xor_target

Base + 0x20 // function target

PARSE!!

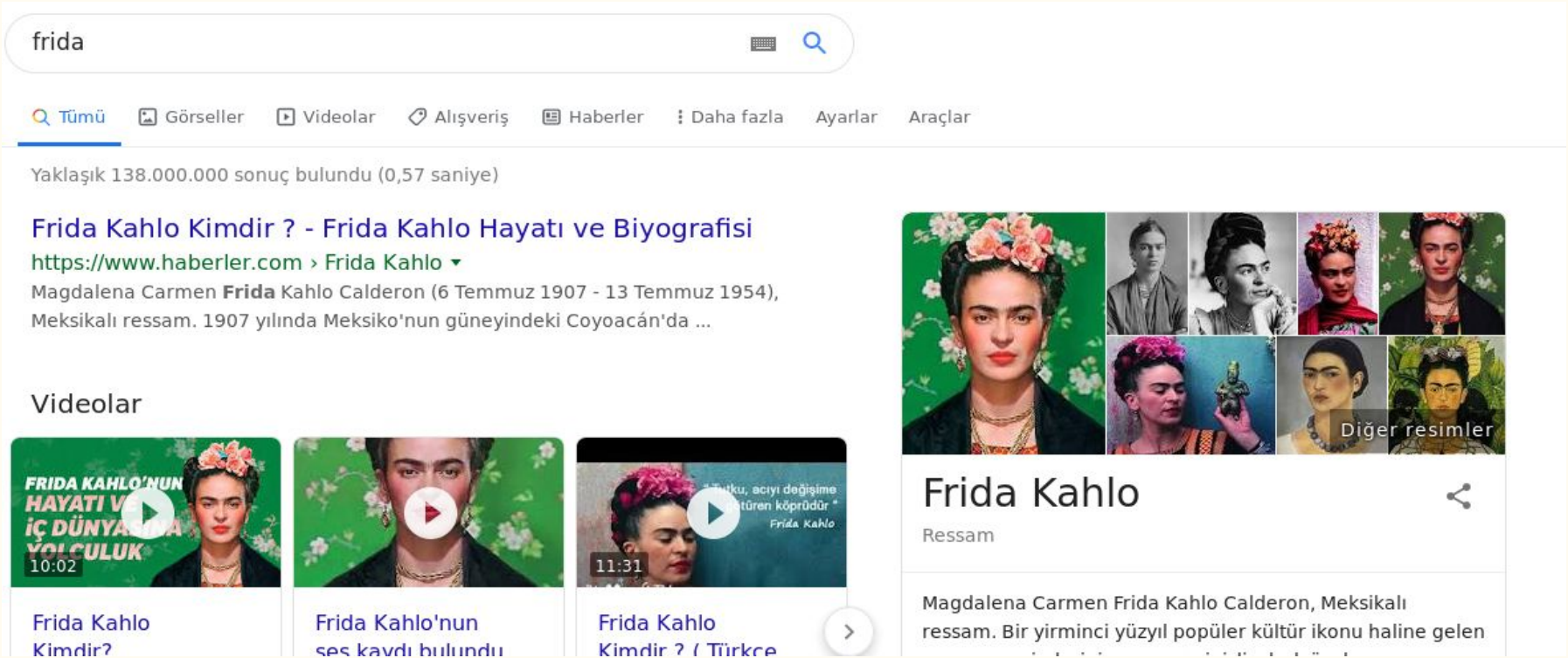
Python + Ghidra = 

- Window -> Script Manager
- Create New Script
- Edit with basic editor

RTFM : https://ghidra.re/ghidra_docs/api/

Deneme Yanilma/ Tab Complete : Window -> Python

Frida ?


frida
Tümü
Görseller
Videolar
Alışveriş
Haberler
Daha fazla
Ayarlar
Araçlar
Yaklaşık 138.000.000 sonuç bulundu (0,57 saniye)
Frida Kahlo Kimdir ? - Frida Kahlo Hayatı ve Biyografisi
https://www.haberler.com › Frida Kahlo
Magdalena Carmen Frida Kahlo Calderon (6 Temmuz 1907 - 13 Temmuz 1954), Meksikalı ressam. 1907 yılında Meksiko'nun güneyindeki Coyoacán'da ...
Videolar
FRIDA KAHLO'NUN
10:02
11:31
Frida Kahlo
Kimdir?
Frida Kahlo'nun
Frida Kahlo
Kimdir ? (Türkçe
Diğer resimler
Frida Kahlo
Ressam
Magdalena Carmen Frida Kahlo Calderon, Meksikalı ressam. Bir yirminci yüzyıl popüler kültür ikonu haline gelen

Frida ?

Dinamik instrumentation:

Hook functions, memory write, read ..

Frida ?

Export olmayan fonksiyon tanımlama :

var xor = new NativeFunction(ptr(0x402CDF), 'void', ['pointer'']);

Memory okuma :

Memory.readS32

Partial Script

Keyleri buluyoruz

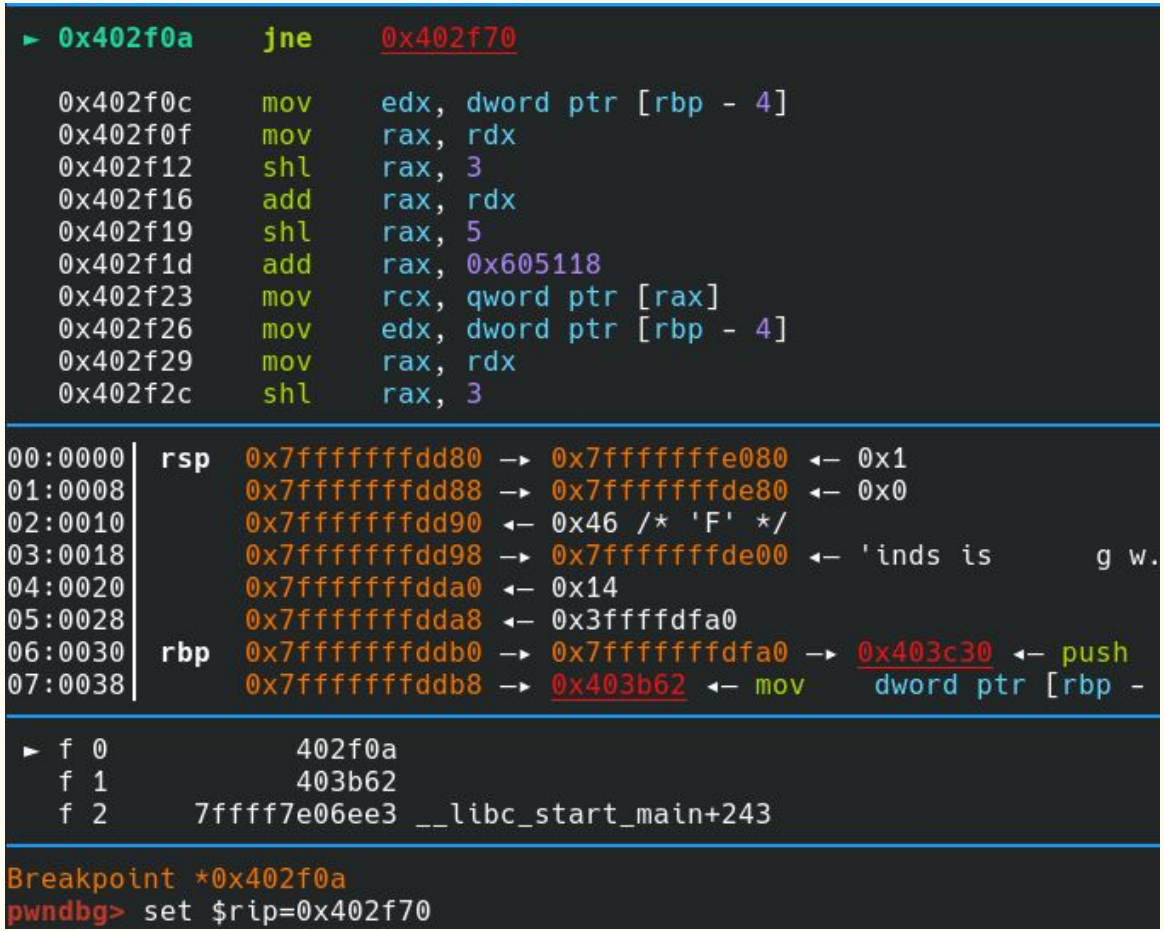
Frida magic -l first.js

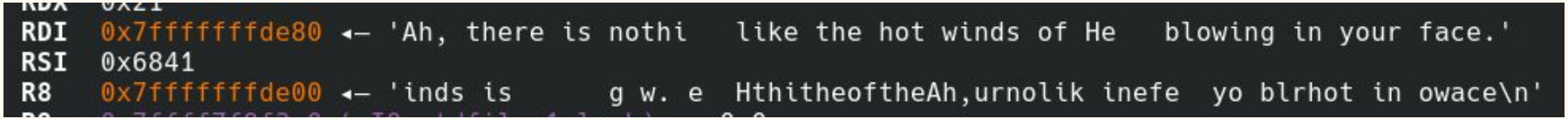
```
inds ----- --g--. e ----------the-----nolik ine-e ------rhot in --ace
inds ----- --g--. e  H--------the-----nolik ine-e ------rhot in --ace
inds ----- --g--. e  H--------the-----nolik ine-e  yo---rhot in --ace
inds ----- --g--. e  H--------the---urnolik ine-e  yo---rhot in --ace
inds ----- --g--. e  H------ofthe---urnolik ine-e  yo---rhot in --ace
inds ----- --g--. e  H------ofthe---urnolik inefe  yo---rhot in --ace
inds is--- --g--. e  H------ofthe---urnolik inefe  yo---rhot in --ace
inds is--- --g--. e  H------ofthe---urnolik inefe  yo blrhot in --ace
inds is--- --g--. e  H------ofthe---urnolik inefe  yo blrhot in owace
inds is--- --g--. e  Hthi---ofthe---urnolik inefe  yo blrhot in owace
inds is--- --g w. e  Hthi---ofthe---urnolik inefe  yo blrhot in owace
inds is--- --g w. e  HthitheoftheAh,urnolik inefe  yo blrhot in owace
inds is--- --g w. e  HthitheoftheAh,urnolik inefe  yo blrhot in owace
```

GDB bypass

b *0x402f0a

If not : set $rip ..


► 0x402f0a jne 0x402f70
0x402f0c mov edx, dword ptr [rbp - 4]
0x402f0f mov rax, rdx
0x402f12 shl rax, 3
0x402f16 add rax, rdx
0x402f19 shl rax, 5
0x402f1d add rax, 0x605118
0x402f23 mov rcx, qword ptr [rax]
0x402f26 mov edx, dword ptr [rbp - 4]
0x402f29 mov rax, rdx
0x402f2c shl rax, 3
00:0000 rsp 0x7fffffffdd80 —▸ 0x7fffffffe080 ◂— 0x1
01:0008 0x7fffffffdd88 —▸ 0x7fffffffde80 ◂— 0x0
02:0010 0x7fffffffdd90 ◂— 0x46 /* 'F' */
03:0018 0x7fffffffdd98 —▸ 0x7fffffffde00 ◂— 'inds is g w.
04:0020 0x7fffffffdda0 ◂— 0x14
05:0028 0x7fffffffdda8 ◂— 0x3ffffdfa0
06:0030 rbp 0x7fffffffddb0 —▸ 0x7fffffffdfa0 —▸ 0x403c30 ◂— push
07:0038 0x7fffffffddb8 —▸ 0x403b62 ◂— mov dword ptr [rbp -
► f 0 402f0a
f 1 403b62
f 2 7ffff7e06ee3 __libc_start_main+243
Breakpoint *0x402f0a
pwndbg> set $rip=0x402f70


RDI 0x7fffffffde80 ◂— 'Ah, there is nothi like the hot winds of He blowing in your face.'
RSI 0x6841
R8 0x7fffffffde00 ◂— 'inds is g w. e HthitheoftheAh,urnolik inefe yo blrhot in owace\n'

YEY!

Wrapper

Magici başlatıp frida scriptinden aldığı inputu processe vericek bir wrapper yazmamız gerek.

```
#/usr/bin/python

import frida
```

MASTER PLAN

Frida scripti belirli aralıklarla çalışıcak ve değişen keyi basıcak.

Wrapper scripti basılan keyi alıp processe yollayacak.

```
from pwn import *
```

```
(657, 'ing yoinlle thihot Hofe ds thenof  blisng  in ow.uracelik wr Ah,ethe ')
(658, 'theure  winofthithell blownorAh,ds g . yo inacehot  Hng like  in fise')
(659, 'e. theisg  wthehot  HAh,rnoin yoe aceow ble thi fllinofds ng likur in')
(660, 'thee  thiise   wurowe  yog llinds the.Ah,f Hlik bl ininnohotng raceof')
(661, ' aceowurllAh,likin He  blthi in yoishotds .noe in  therof wg ng efthe')
(662, ' yo inge the ng  ace blnothe Hise ds  .fowinlikhot llAh,urrofinethi w')
(663, 'theaceur HAh, ine eof  no  blingis.like f thirin yo whotds ng owllthe')
(664, 'in wisgtheds  thiowhot inllaceng e e noofAh,inur He flik .the r bl yo')
(665, 'owlllikhote  ace in of.ee  in H in blds nog your wtheisrthethifAh,ng ')
[*] Switching to interactive mode
 Here is your price:
mag!iC_mUshr00ms_maY_h4ve_g!ven_uS_Santa_ClaUs@flare-on.com
```

Soru varmı