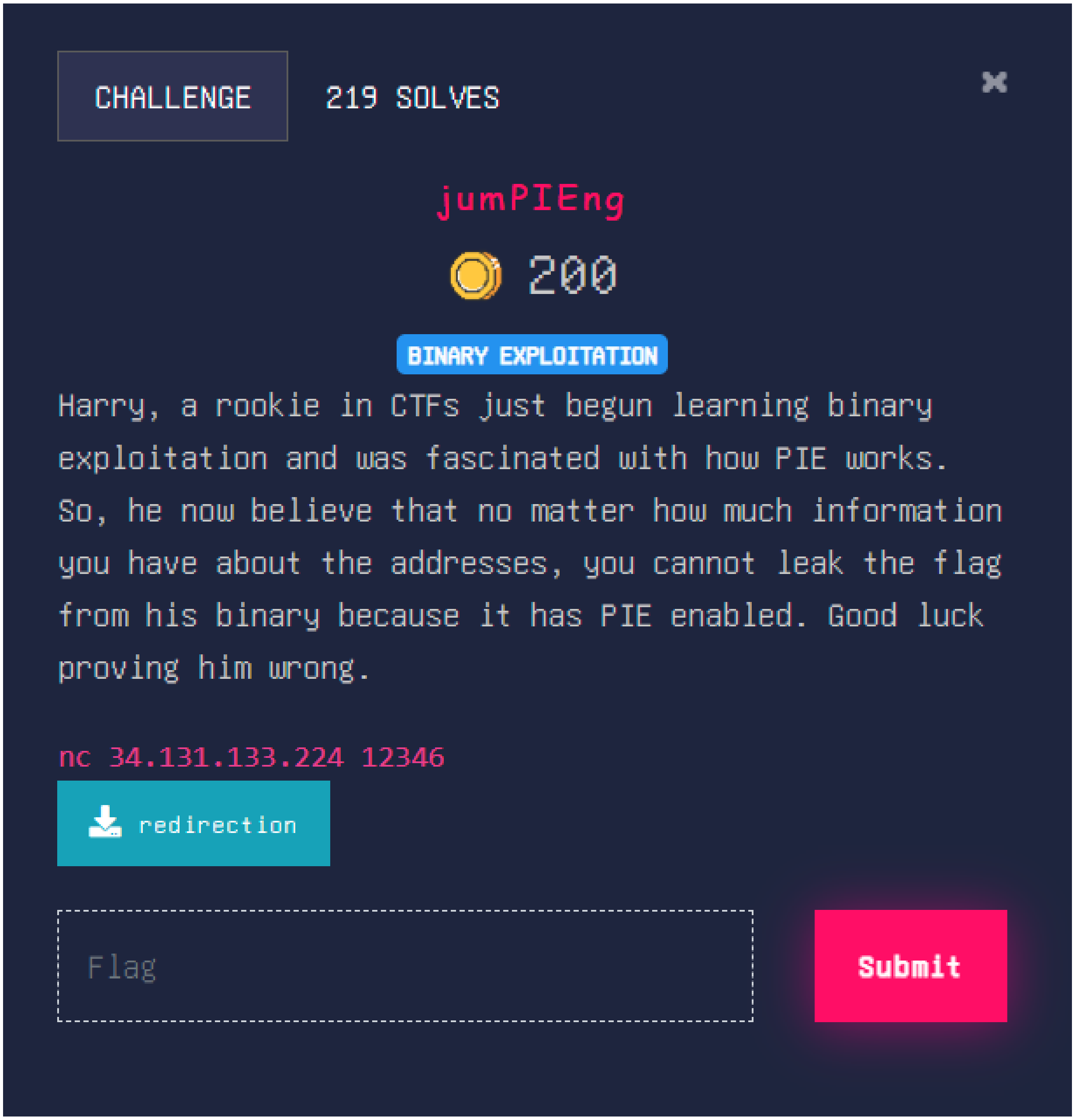
jumPIEng

Description



Harry, a rookie in CTFs just begun learning binary exploitation and was fascinated with how PIE works. So, he now believe that no matter how much information you have about the addresses, you cannot leak the flag from his binary because it has PIE enabled. Good luck proving him wrong.

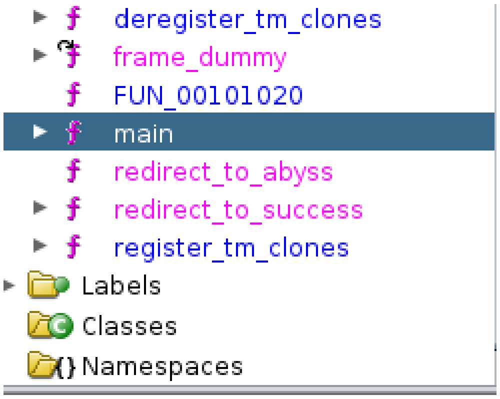
nc 34.131.133.224 12346

Category

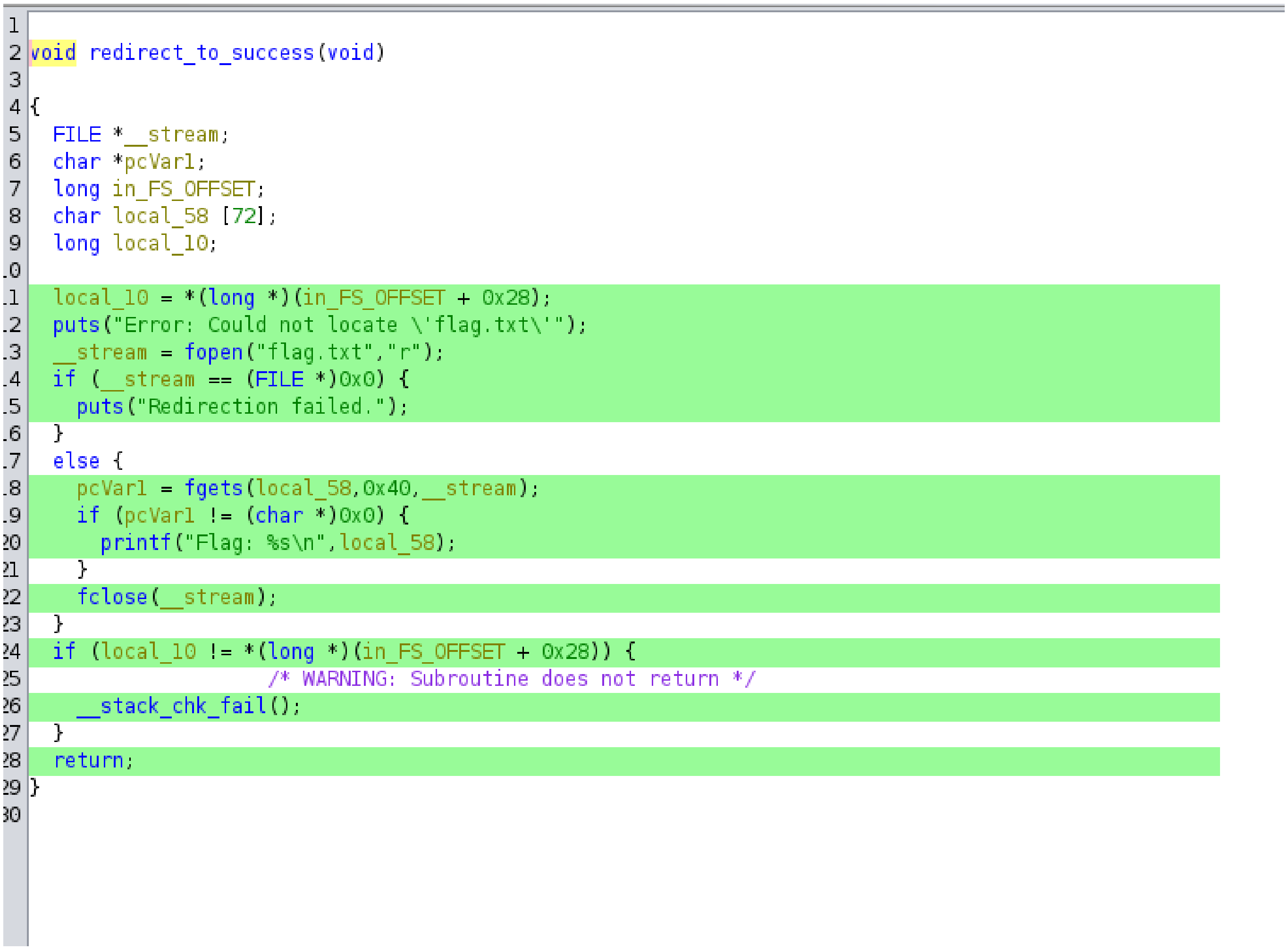
#binary

Solution

`strings` gives nothing useful so I use `Ghidra` instead

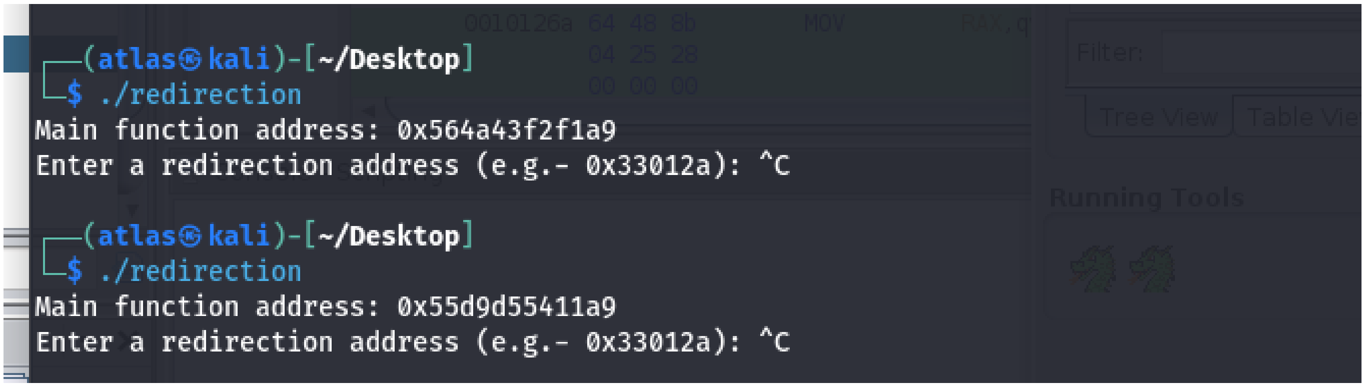


the redirect_to_success is the function that calls the flag



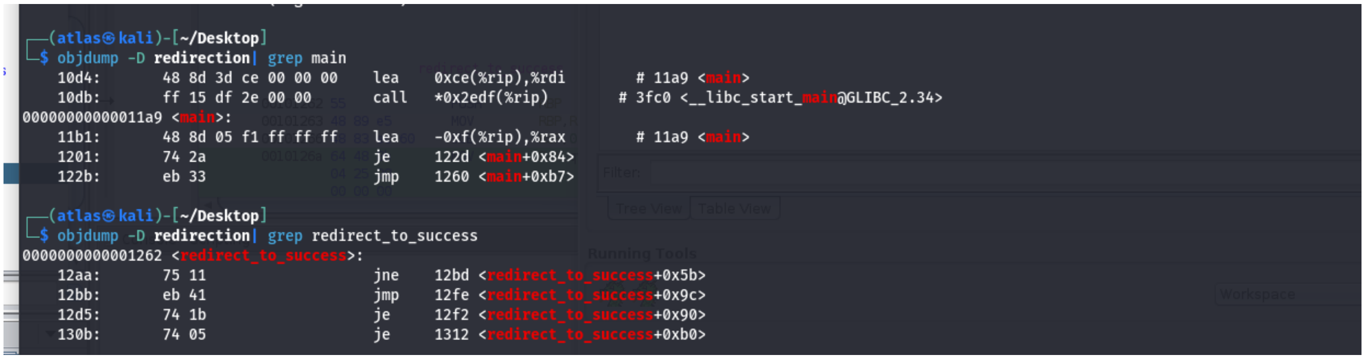
```

void redirect_to_success(void)

{
  FILE *__stream;
  char *pcVar1;
  long in_FS_OFFSET;
  char local_58 [72];
  long local_10;

  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  puts("Error: Could not locate \'flag.txt\'");
  __stream = fopen("flag.txt","r");
  if (__stream == (FILE *)0x0) {
    puts("Redirection failed.");
  }
  else {
    pcVar1 = fgets(local_58,0x40,__stream);
    if (pcVar1 != (char *)0x0) {
      printf("Flag: %s\n",local_58);
    }
    fclose(__stream);
  }
  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return;
}

```

so this problem seems to want to give it the address to the redirect_to_success method.



```
┌──(atlas㉿kali)-[~/Desktop]
└─$ ./redirection
Main function address: 0x564a43f2f1a9
Enter a redirection address (e.g.- 0x33012a): ^C

┌──(atlas㉿kali)-[~/Desktop]
└─$ ./redirection
Main function address: 0x55d9d55411a9
Enter a redirection address (e.g.- 0x33012a): ^C
```

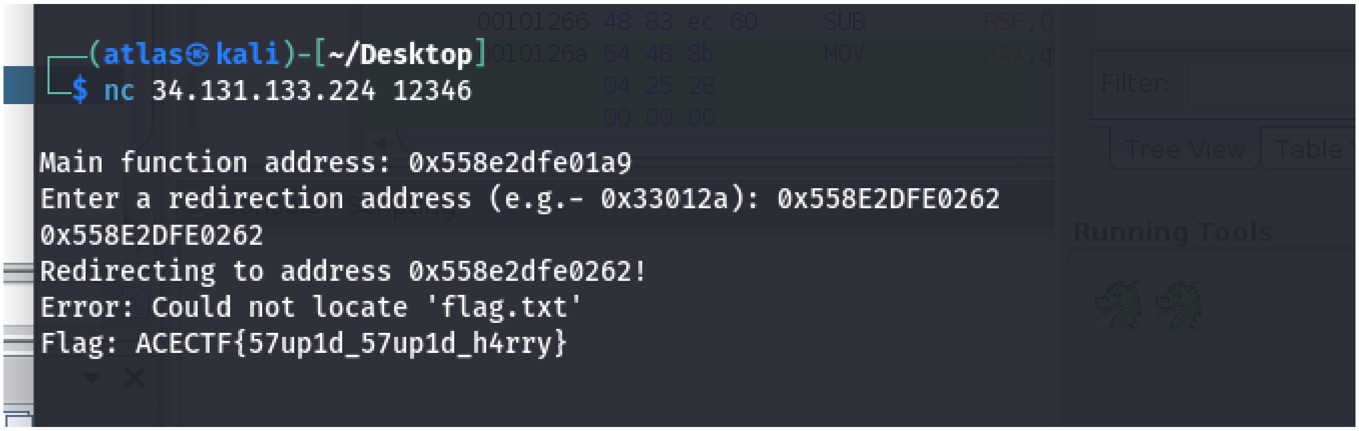
main address is dynamic but one thing static is the difference between two address



```
┌──(atlas㉿kali)-[~/Desktop]
└─$ objdump -D redirection| grep main
    10d4:       48 8d 3d ce 00 00 00    lea    0xce(%rip),%rdi        # 11a9 <main>
    10db:       ff 15 df 2e 00 00       call   *0x2edf(%rip)        # 3fc0 <__libc_start_main@GLIBC_2.34>
00000000000011a9 <main>:
    11b1:       48 8d 05 f1 ff ff ff    lea    -0xf(%rip),%rax        # 11a9 <main>
    1201:       74 2a                   je     122d <main+0x84>
    122b:       eb 33                   jmp    1260 <main+0xb7>

┌──(atlas㉿kali)-[~/Desktop]
└─$ objdump -D redirection| grep redirect_to_success
0000000000001262 <redirect_to_success>:
    12aa:       75 11                   jne    12bd <redirect_to_success+0x5b>
    12bb:       eb 41                   jmp    12fe <redirect_to_success+0x9c>
    12d5:       74 1b                   je     12f2 <redirect_to_success+0x90>
    130b:       74 05                   je     1312 <redirect_to_success+0xb0>
```

Gives 0xB9

so it means when it runs, i just need to add that



```
┌──(atlas㉿kali)-[~/Desktop]
└─$ nc 34.131.133.224 12346

Main function address: 0x558e2dfe01a9
Enter a redirection address (e.g.- 0x33012a): 0x558E2DFE0262
0x558E2DFE0262
Redirecting to address 0x558e2dfe0262!
Error: Could not locate 'flag.txt'
Flag: ACECTF{57up1d_57up1d_h4rry}
```