# hw1

0410788 CHING-WEN CHENG

September 29, 2017

## Contents



# 1 Homework1

## 1.1 strings [50]

Use strings to list all printable character in files.

```
strings ./strings | grep "FLAG{"
```

`FLAG{__flag_in_the_file}`

## 1.2 strace [50]

Use strace to trace system calls.

```
strace -s 40 -e write ./strace 2>&1
```

```
write(2, "FLAG{____yaaaa_flag_in_the_stack___}", 36) = -1 EBADF (Bad file descriptor)
write(1, "find the flag in system call!\n", 30find the flag in system call!
) = 30
+++ exited with 0 +++
```

## 1.3 patching [50]

First, we run the program.

```
./patching
```

```
Value = 0x376c8
Go patching the value to 0x00023333
```

We can see that we need to patch `Value` to `0x00023333`. Open `patching` with `emacs` in `hexl-mode`, find `c8 76 03 00`, little endian of `0x376c8`, patch it to `33 33 02 00`, then run the program again.

```
./patched
```

```
Value = 0x23333
FLAG{oa11TH8OwfMEs6ZflBhGF4btUcS1Ds9y}
```

## 1.4 pwntools [50]

Connect to the host, we get see that it is kind of "guess the number" game. We need to guess the correct number from 1 to 50000000, so write a simple binary search.

### 1.4.1 Code

```
from pwn import *
M = 50000000
m = 1
def bs(x):
    global r, M, m
    r.recvuntil("= ")
    r.sendline(str(x))
    L = r.recvline()
    l = L.split()[-1]
    if l == b'big':
        M = x
        bs((M+m)//2)
    elif l == b'small':
        m = x
        bs((M+m)//2)
    else:
        print(L)
        return L

with remote("csie.ctf.tw", 10123) as r:
    bs((m+M)//2)
```

```
[x] Opening connection to csie.ctf.tw on port 10123
[x] Opening connection to csie.ctf.tw on port 10123: Trying 140.112.31.96
[+] Opening connection to csie.ctf.tw on port 10123: Done
b'Success~ FLAG{h02Ooysbv4O5Lf1Fmdrt2QKts7buYz0J}\n'
[*] Closed connection to csie.ctf.tw port 10123
```