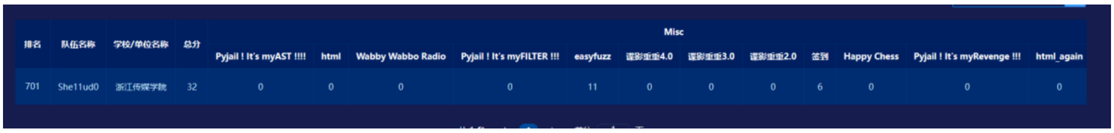
She11ud0 战队 WRITEUP

一、 战队信息

战队名称：**She11ud0**

战队排名：701

二、 解题情况



排名	队伍名称	学校/单位名称	总分	Misc											
				Pyjail ! It's myAST !!!!	html	Wabby Wabbo Radio	Pyjail ! It's myFILTER !!!	easyfuzz	谍影重重4.0	谍影重重3.0	谍影重重2.0	签到	Happy Chess	Pyjail ! It's myRevenge !!!	html_again
701	She11ud0	浙江传媒学院	32	0	0	0	0	11	0	0	0	6	0	0	0

三、 解题过程

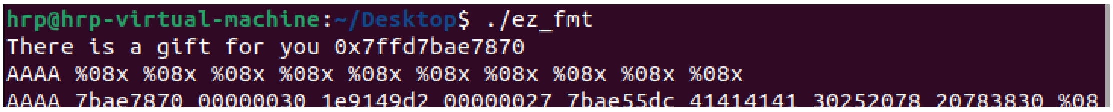
题目序号 5 题目名称 ezfuzz

（题目序号 请参考解题总榜上面的序号）

操作内容：

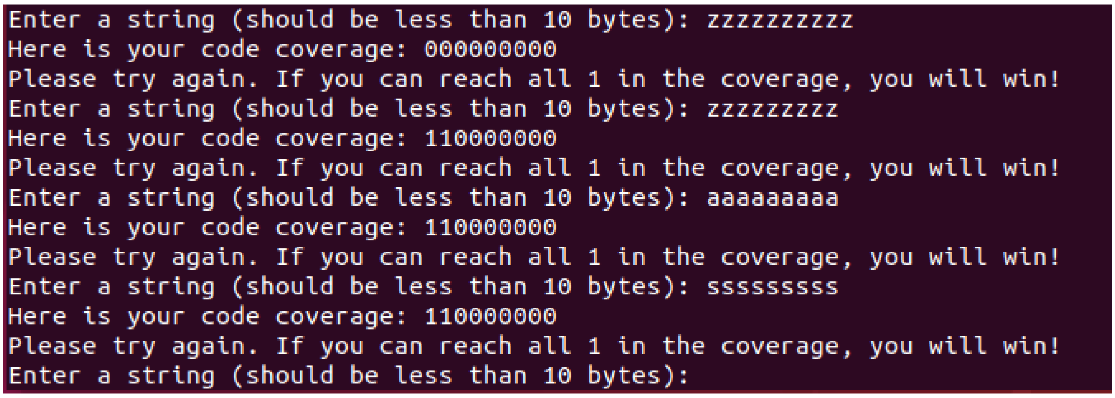
它最多输入 10byte 就是说

一开始我就疯狂手动尝试，发现输入九位字符的时候会被覆盖成 110000000，其他情况不管怎么输入都是九个零



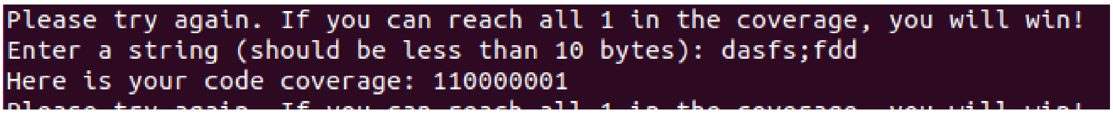
```
hrp@hrp-virtual-machine:~/Desktop$ ./ez_fmt
There is a gift for you 0x7ffd7bae7870
AAAA %08x %08x %08x %08x %08x %08x %08x %08x %08x %08x
AAAA 7bae7870 00000030 1e9149d2 00000027 7bae55dc 41414141 30252078 20783830 %08
```

又尝试胡乱打了几下发现同是九位，输入 `asdf'fdd` 就可以覆盖最高位的 0 了好神奇，

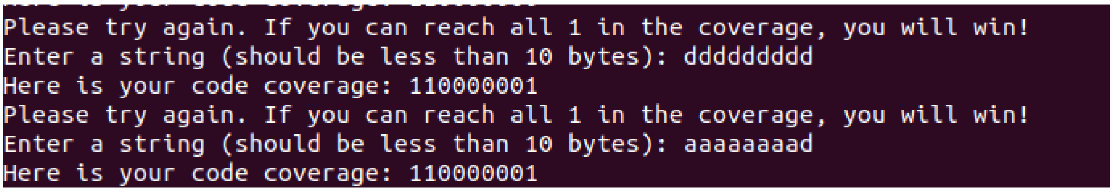


```
Enter a string (should be less than 10 bytes): zzzzzzzzzz
Here is your code coverage: 000000000
Please try again. If you can reach all 1 in the coverage, you will win!
Enter a string (should be less than 10 bytes): zzzzzzzzz
Here is your code coverage: 110000000
Please try again. If you can reach all 1 in the coverage, you will win!
Enter a string (should be less than 10 bytes): aaaaaaaaa
Here is your code coverage: 110000000
Please try again. If you can reach all 1 in the coverage, you will win!
Enter a string (should be less than 10 bytes): sssssssss
Here is your code coverage: 110000000
Please try again. If you can reach all 1 in the coverage, you will win!
Enter a string (should be less than 10 bytes):
```

又又再次多次尝试发现最后一位是 d，对应的最后一位就是 1。同时只要输入是九位，不管输入的前两位怎么变，覆盖率前两位都是 11。



```
Please try again. If you can reach all 1 in the coverage, you will win!
Enter a string (should be less than 10 bytes): dasfs;fdd
Here is your code coverage: 110000001
```



```
Please try again. If you can reach all 1 in the coverage, you will win!
Enter a string (should be less than 10 bytes): ddddddddd
Here is your code coverage: 110000001
Please try again. If you can reach all 1 in the coverage, you will win!
Enter a string (should be less than 10 bytes): aaaaaaaad
Here is your code coverage: 110000001
```

所以说覆盖率后七位和输入的后七位一一对应。误打误撞知道最后一位是 d，那我们只需要爆破一下中间的六位就行。

综上，我们只要保证一共输入九位，最后一位是 d。只需要尝试对应位值为 0 的位，对应位是 1，那么就是已经找到了正确的值不需要遍了。

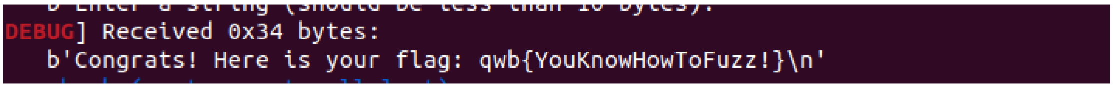
如该题使用自己编写的脚本代码请详细写出，不允许截图

```
from pwn import *
from string import printable
io=remote('120.24.69.11',12199)
context.log_level='debug'

cover=[1,1,0,0,0,0,0,0,1]
payload=bytearray(b'aaaaaaaad')
io.recvuntil('bytes): ')
i=0

while True:
    ch=printable[i]
    i=(i+1)%len(printable)
    j=cover.index(0)
    payload[j]=ord(ch)
    print (payload)
    io.sendline(payload)
    io.recvuntil(b'coverage: ')
    received_data = io.recvline().strip().decode()
    cover = []
    for item in received_data:
    cover.append(int(item))
    if cover.count('1')==9:
        break
io.interactive()
```

flag 值：



```
   b'Enter a string (should be less than 10 bytes):
DEBUG] Received 0x34 bytes:
   b'Congrats! Here is your flag: qwb{YouKnowHowToFuzz!}\n'
```