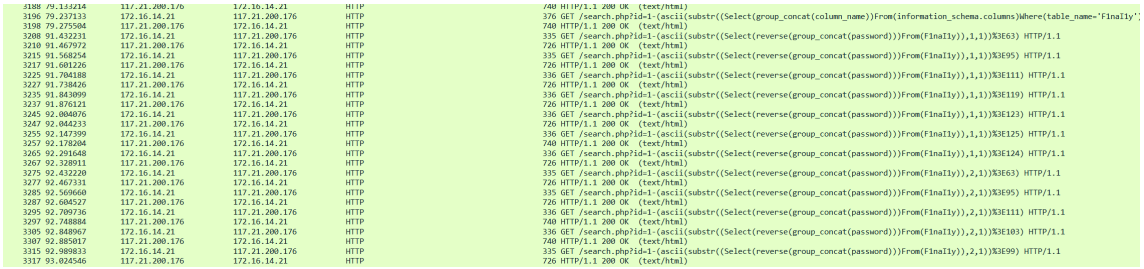
Hgame Week3

与ai聊天

很奇怪，前面试了flag，galf...然后突然就出来了

Blind SQL Injection

1. 把blindsql.pcapng放入wireshark
2. 然后学了盲注是什么?
3. 发现这里：



   出现了一个二分法，比较第i位是否大于某个数，如果判断为真那么它返回长度为726，为假length=740

   然后就可以编写脚本破案了

4. 自己找记录下每一位密码的ascii值不会编，

```
str="""125/102/50/102/97/56/50/57/53/99/56/51/100/45/54/99/97/98/45/56/57/101/52/
45/53/50/55/49/45/55/101/102/97/98/97/98/99/123/103/97/108/102/44/96"""
a=str.split('/')
print(a)
for i in a:
    print(chr(int(i)),end="")
# print(str)
```

结果：`}f2fa8295c83d-6cab-89e4-5271-7efababc{galf`

逆向一下出flag