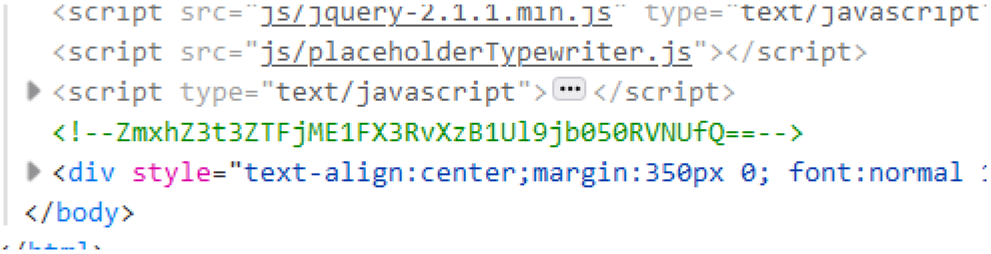
注意事项：编写完 wp 后，保存为 pdf 格式文档上传，文档大小限制在 10M 以内

Web

Sign2

看源码



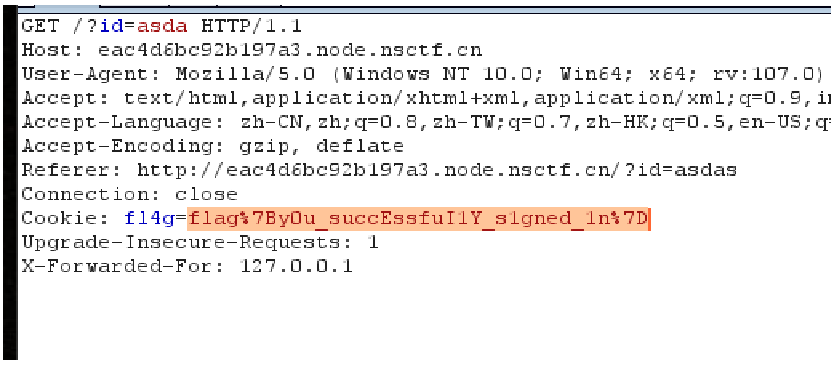
```
    <script src="js/jquery-2.1.1.min.js" type="text/javascript
    <script src="js/placeholderTypewriter.js"></script>
  ▶ <script type="text/javascript"> ••• </script>
    <!--ZmxhZ3t3ZTFjME1FX3RvXzB1Ul9jb050RVNUfQ==-->
  ▶ <div style="text-align:center;margin:350px 0; font:normal :
  </body>
```

Base64 解码

flag{we1c0ME_to_0uR_coNtEST}

假 flag

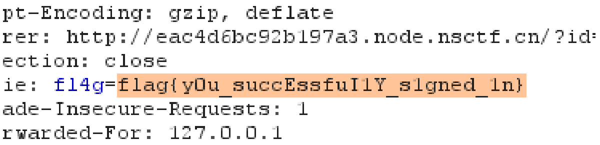
抓包



```
GET /?id=asda HTTP/1.1
Host: eac4d6bc92b197a3.node.nsctf.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,i
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q
Accept-Encoding: gzip, deflate
Referer: http://eac4d6bc92b197a3.node.nsctf.cn/?id=asdas
Connection: close
Cookie: fl4g=flag%7By0u_succEssfuI1Y_s1gned_1n%7D
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
```

Cookie

url 解码



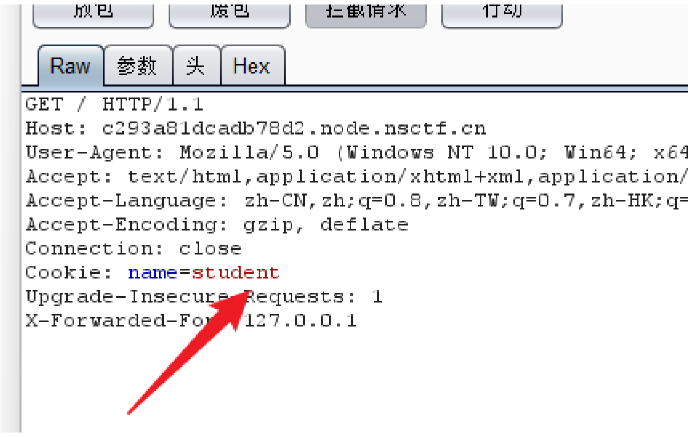
```
pt-Encoding: gzip, deflate
rer: http://eac4d6bc92b197a3.node.nsctf.cn/?id=
ection: close
ie: fl4g=flag{y0u_succEssfuI1Y_s1gned_1n}
ade-Insecure-Requests: 1
rwarded-For: 127.0.0.1
```

flag

flag{y0u_succEssfuI1Y_s1gned_1n}

easy 的简单越权

抓包

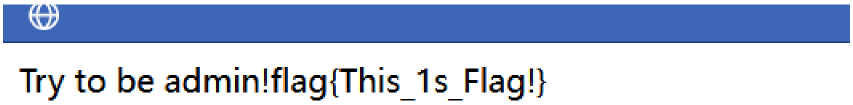


```
GET / HTTP/1.1
Host: c293a81dcadb78d2.node.nsctf.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64
Accept: text/html,application/xhtml+xml,application/
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=
Accept-Encoding: gzip, deflate
Connection: close
Cookie: name=student
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
```

修改 name 为 admin

重放

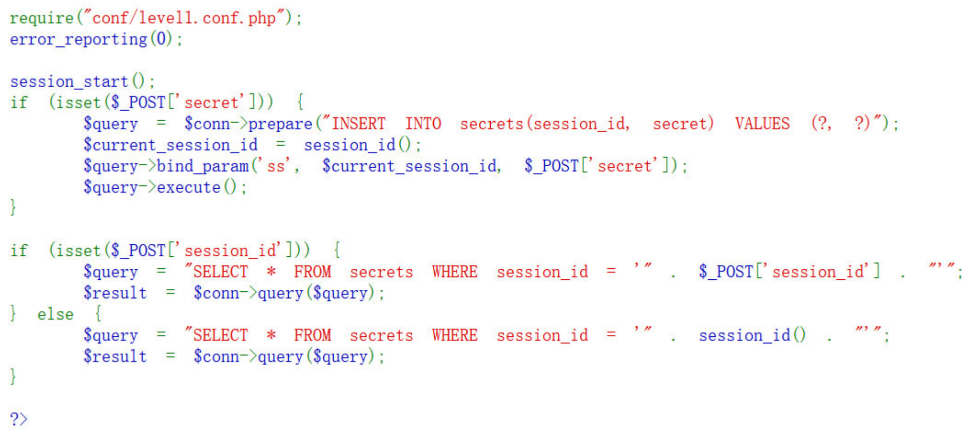
返回 flag



Try to be admin!flag{This_1s_Flag!}

Web3

查看源码

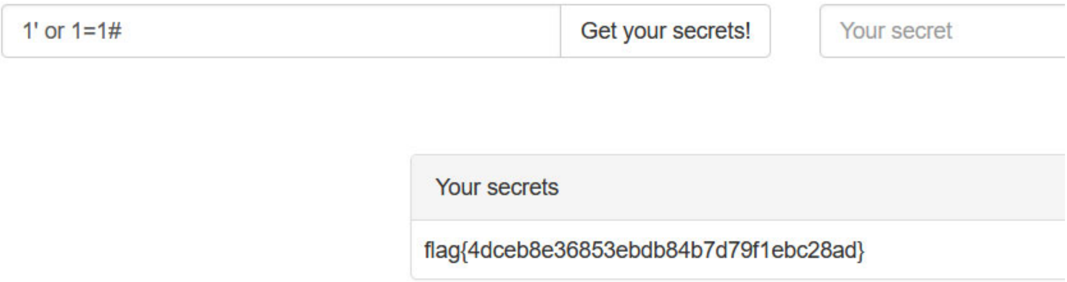


```
require(”conf/level1.conf.php”);
error_reporting(0);

session_start();
if (isset($_POST['secret'])) {
      $query = $conn->prepare(”INSERT INTO secrets(session_id, secret) VALUES (?, ?)”);
      $current_session_id = session_id();
      $query->bind_param('ss', $current_session_id, $_POST['secret']);
      $query->execute();
}

if (isset($_POST['session_id'])) {
      $query = ”SELECT * FROM secrets WHERE session_id = '” . $_POST['session_id'] . ”'”;
      $result = $conn->query($query);
} else {
      $query = ”SELECT * FROM secrets WHERE session_id = '” . session_id() . ”'”;
      $result = $conn->query($query);
}

?>
```

查询语句，sql 注入，直接尝试万能密码

1’or 1=1#

直接得到 flag



1' or 1=1#

Your secrets

flag{4dceb8e36853ebdb84b7d79f1ebc28ad}

Misc

Txt

记事本打开

查看 flag

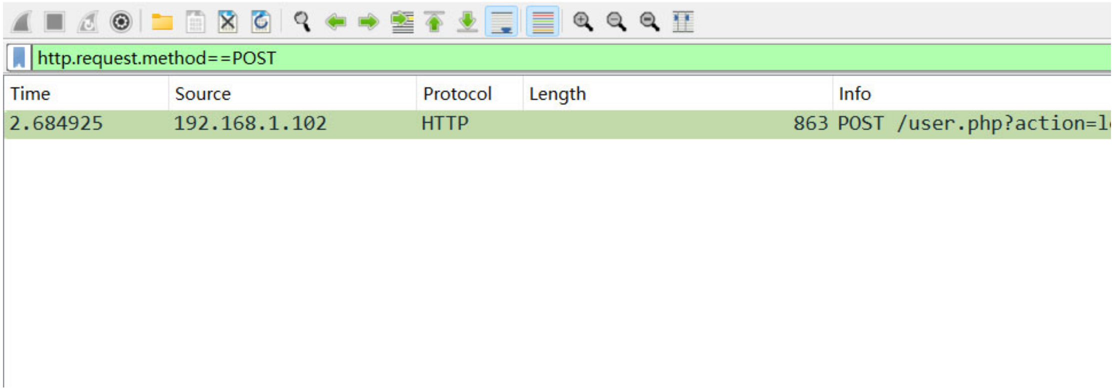
flag{876e28aebf64121ca77a55648992c0d8759f}

流量包

流量分析

Wireshark 打开

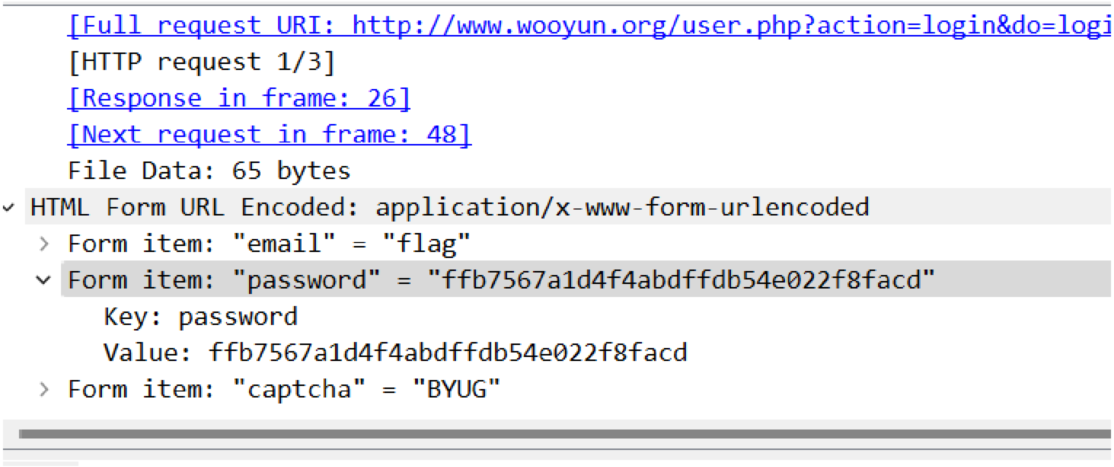
过滤器输入 http.request.method==POST



http.request.method==POST

Time	Source	Protocol	Length	Info
2.684925	192.168.1.102	HTTP	863	POST /user.php?action=l

查看表单值 pasword 密码



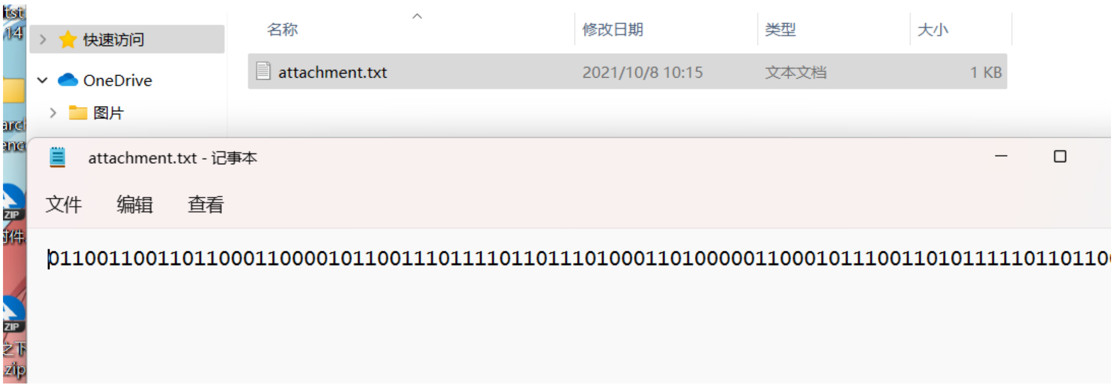
```
    [Full request URI: http://www.wooyun.org/user.php?action=login&do=logi
    [HTTP request 1/3]
    [Response in frame: 26]
    [Next request in frame: 48]
    File Data: 65 bytes
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "email" = "flag"
  ⌄ Form item: "password" = "ffb7567a1d4f4abdffdb54e022f8facd"
       Key: password
       Value: ffb7567a1d4f4abdffdb54e022f8facd
  › Form item: "captcha" = "BYUG"
```

flag{ffb7567a1d4f4abdffdb54e022f8facd}

crypto

encode

打开文本文件，一串二进制

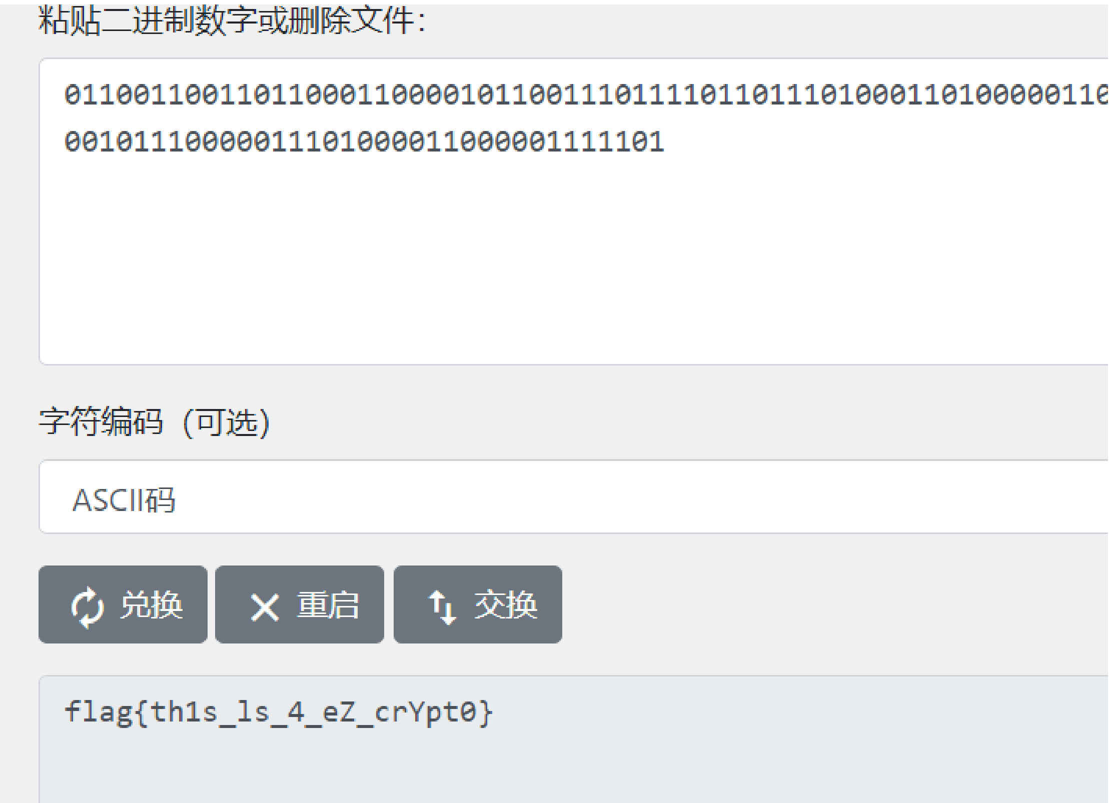


名称	修改日期	类型	大小
attachment.txt	2021/10/8 10:15	文本文档	1 KB

```
011001100110110001100001011001110111101101110100011010000011000101110011010111110110110
```

打开二进制转换网站

选择 ascii 码转换得到 flag


粘贴二进制数字或删除文件:

```
0110011001101100011000010110011101111011011101000110100000110
0010111000001110100001100000111101
```

字符编码（可选）

ASCII码

```
flag{th1s_ls_4_eZ_crYpt0}
```

简单的密码

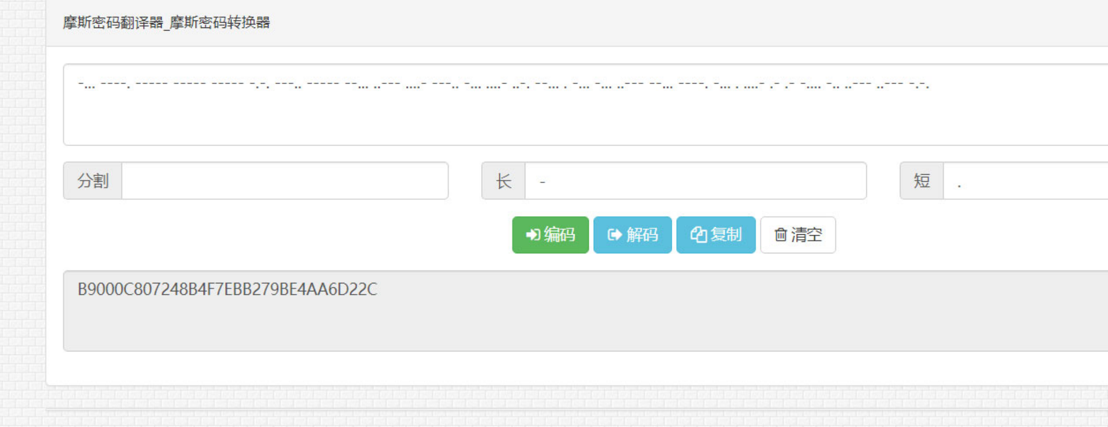
打开文件查看全是 AB

开始找半天资料，以为是培根，试了好多次但是不行

后来发现后边的位数不对，想起了摩斯电码

直接把 A 替换成.把 B 替换成-空格分割

摩斯解密网站


摩斯密码翻译器_摩斯密码转换器

```
-... ----. ----- ----- ----- -.-. ---.. ----- --... ..--- ....- ---.. -... ....- ..-. --... . -... -... ..--- --... ----. -... . ....- .- .- -.... -.. ..--- ..--- -.-.
```

分割:

长: -

短: .

```
B9000C807248B4F7EBB279BE4AA6D22C
```

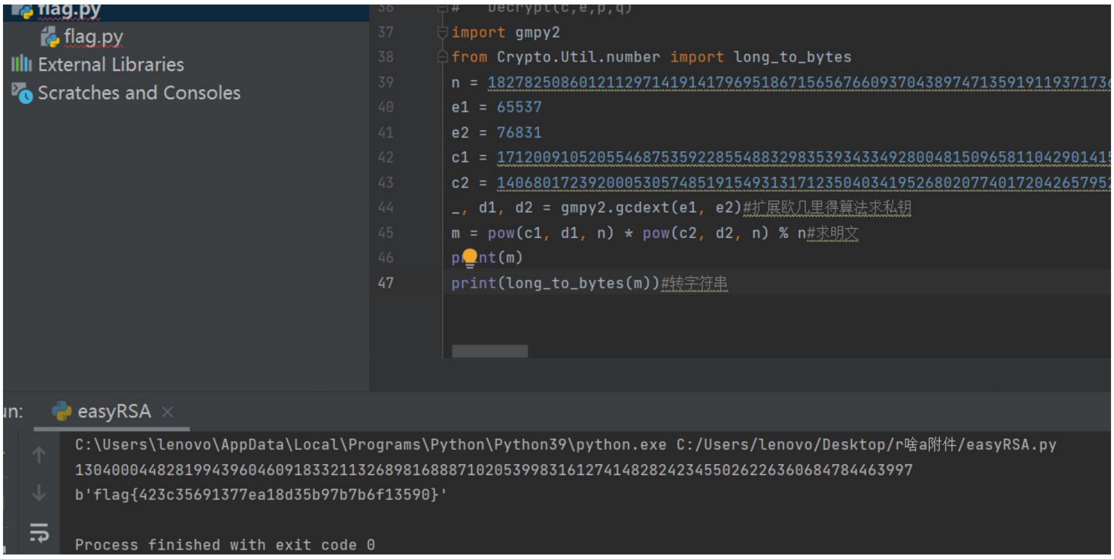
得到

Flag{B9000C807248B4F7EBB279BE4AA6D22C}

babyeayrsa

从给出的两个文本文件，根据给出的公钥和密文找出 n，e1,e2,c1，c2

根据给出的公钥和密文，使用欧几里得算法求私钥然后解出明文



```
#    Decrypt(c,e,p,q)
import gmpy2
from Crypto.Util.number import long_to_bytes
n = 18278250860121129714191417969518671565676609370438974713591911937173
e1 = 65537
e2 = 76831
c1 = 1712009105205546875359228554883298353934334928004815096581104290141
c2 = 1406801723920005305748519154931317123504034195268020774017204265795
_, d1, d2 = gmpy2.gcdext(e1, e2)#扩展欧几里得算法求私钥
m = pow(c1, d1, n) * pow(c2, d2, n) % n#求明文
print(m)
print(long_to_bytes(m))#转字符串
```

```
C:\Users\lenovo\AppData\Local\Programs\Python\Python39\python.exe C:/Users/lenovo/Desktop/r啥a附件/easyRSA.py
13040004482819943960460918332113268981688871020539983161274148282423455026226360684784463997
b'flag{423c35691377ea18d35b97b7b6f13590}'

Process finished with exit code 0
```

flag{423c35691377ea18d35b97b7b6f13590}

新型加密解密

打开文档查看密文只有 ZX

猜测摩斯密码

Z 换成.X 换成-

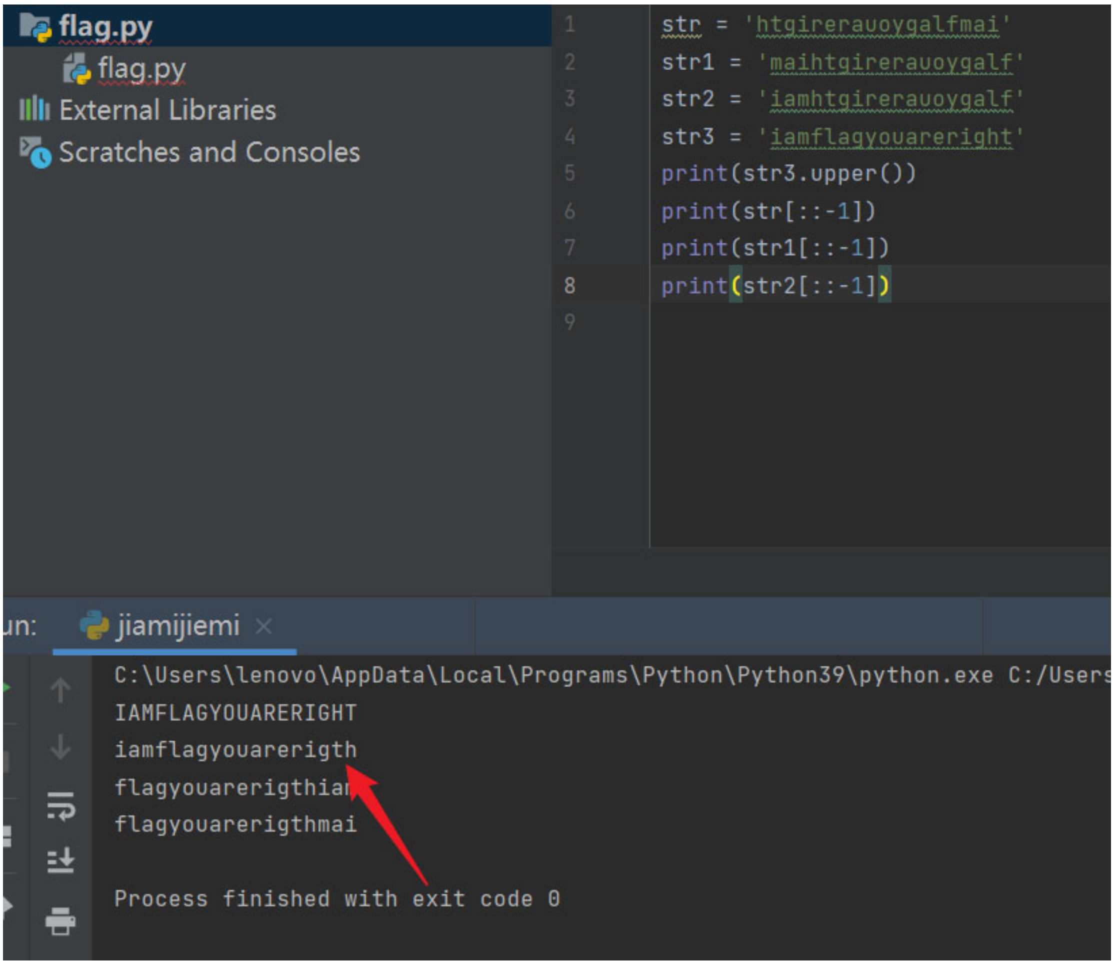
```
密文: .... - --. .. .-. . .-. .- ..- --- -.-- --. .- .-.. ..-. -- .
.... - --. .. .-. . .-. .- ..- --- -.-- --. .- .-.. ..-. -- .- ..
HTGIRERAUOYGALFMAI
htgirerauoygalfmai
```

然后解密出

HTGIRERAUOYGALFMAI

小写发现里边好像有 flag 但是倒过来了

然后逆序字符串



```
str = 'htgirerauoygalfmai'
str1 = 'maihtgirerauoygalf'
str2 = 'iamhtgirerauoygalf'
str3 = 'iamflagyouareright'
print(str3.upper())
print(str[::-1])
print(str1[::-1])
print(str2[::-1])
```

```
C:\Users\lenovo\AppData\Local\Programs\Python\Python39\python.exe C:/Users
IAMFLAGYOUARERIGHT
iamflagyouarerigth
flagyouarerigthiam
flagyouarerigthmai

Process finished with exit code 0
```

第二个就是 flag

Flag{ iamflagyouarerigth}