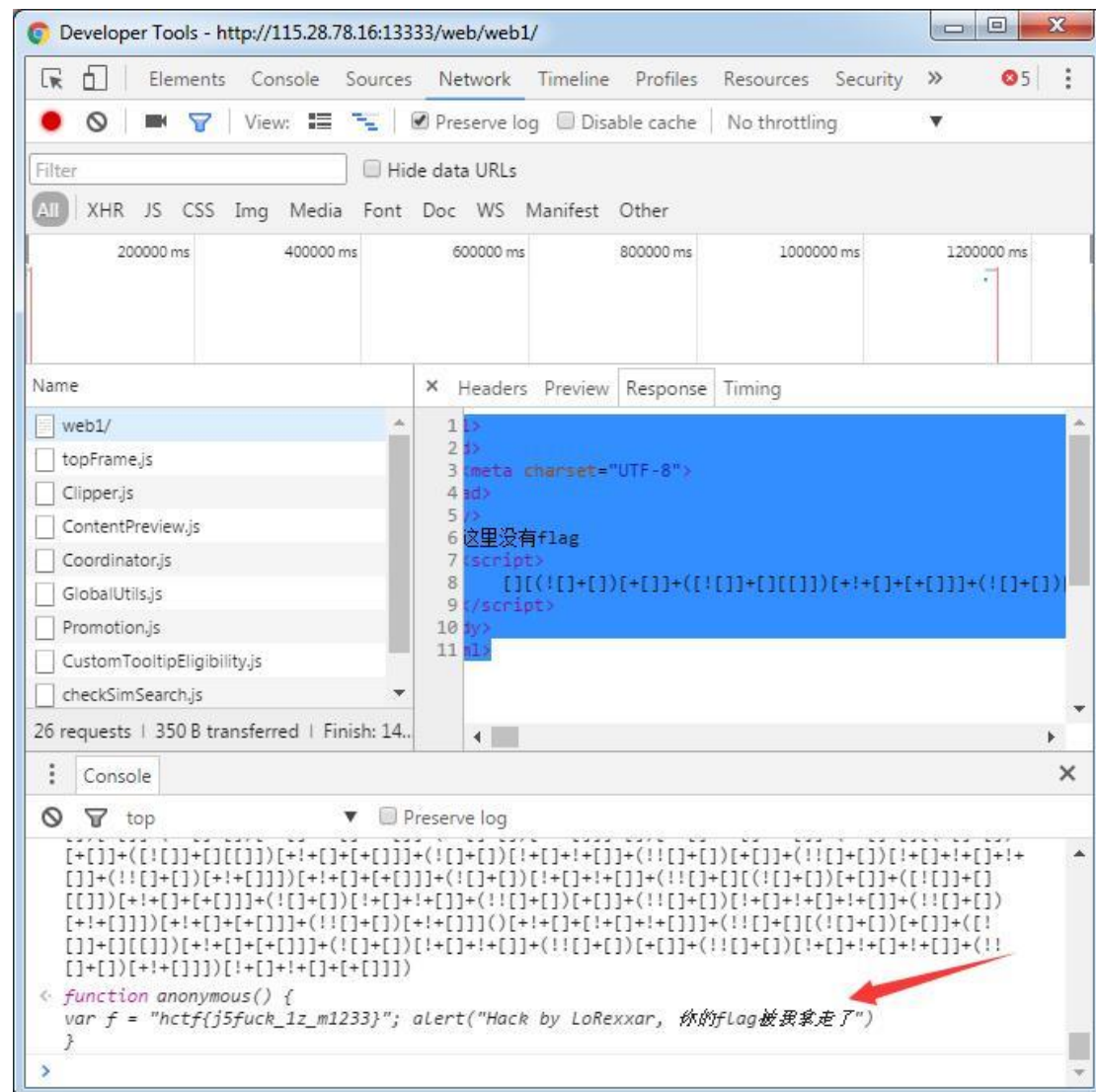


这 TM 是啥

看网页源码 复制出了那段 JSfuck 去掉最后一个 () 放到 Chrome 里 得到 flag



我是谁我在哪???

把 index.html 改成了 .php 发现了一个 302 chrome F12 一看
响应头里出现 flag

The screenshot shows a web browser's developer tools interface. The 'Name' pane on the left lists 'index.php' and 'index.html'. The 'Headers' pane is active, showing the following details:

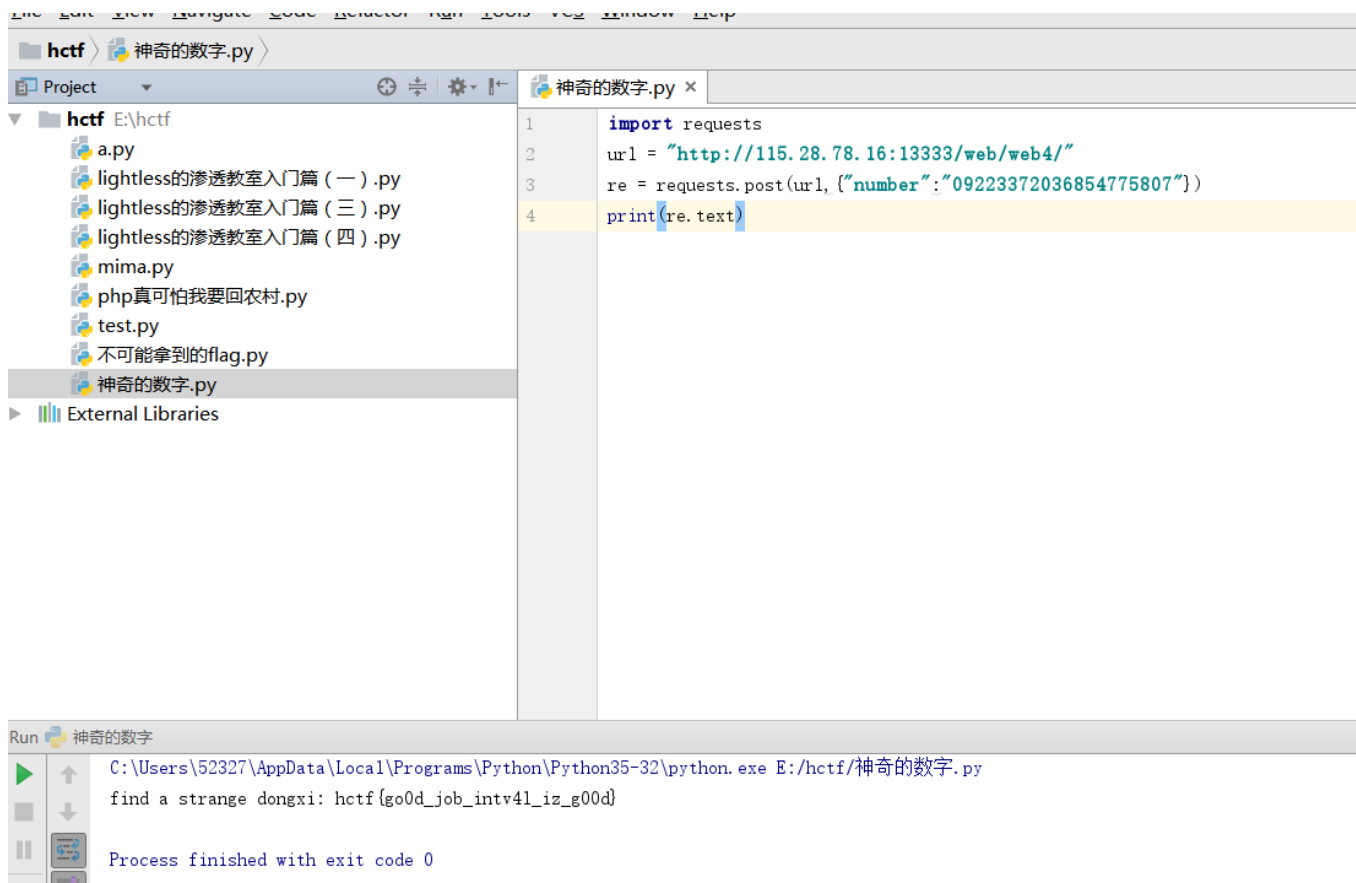
- General:**
 - Request URL: http://115.28.78.16:13333/web/web2/index.php
 - Request Method: GET
 - Status Code: 302 Moved Temporarily
 - Remote Address: 115.28.78.16:13333
- Response Headers:**
 - Connection: keep-alive
 - Content-Type: text/html
 - Date: Wed, 18 Jan 2017 10:15:06 GMT
 - flag: hctf{1t_iz_4_4mall_tr1ck}
 - location: index.html
 - Server: nginx
 - Transfer-Encoding: chunked
 - X-Powered-By: PHP/5.4.41
- Request Headers:**
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 - Accept-Encoding: gzip, deflate, sdch
 - Accept-Language: zh-CN,zh;q=0.8
 - Connection: keep-alive
 - Host: 115.28.78.16:13333
 - Upgrade-Insecure-Requests: 1
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chro

At the bottom, a status bar indicates '2 requests | 244 B transferred | Fi...'.

神奇的数字

```
$n1 = intval($req["number"]);  
$n2 = intval(strrev($req["number"]));
```

看到了 intval 试了一下溢出 Python post 过去出 flag

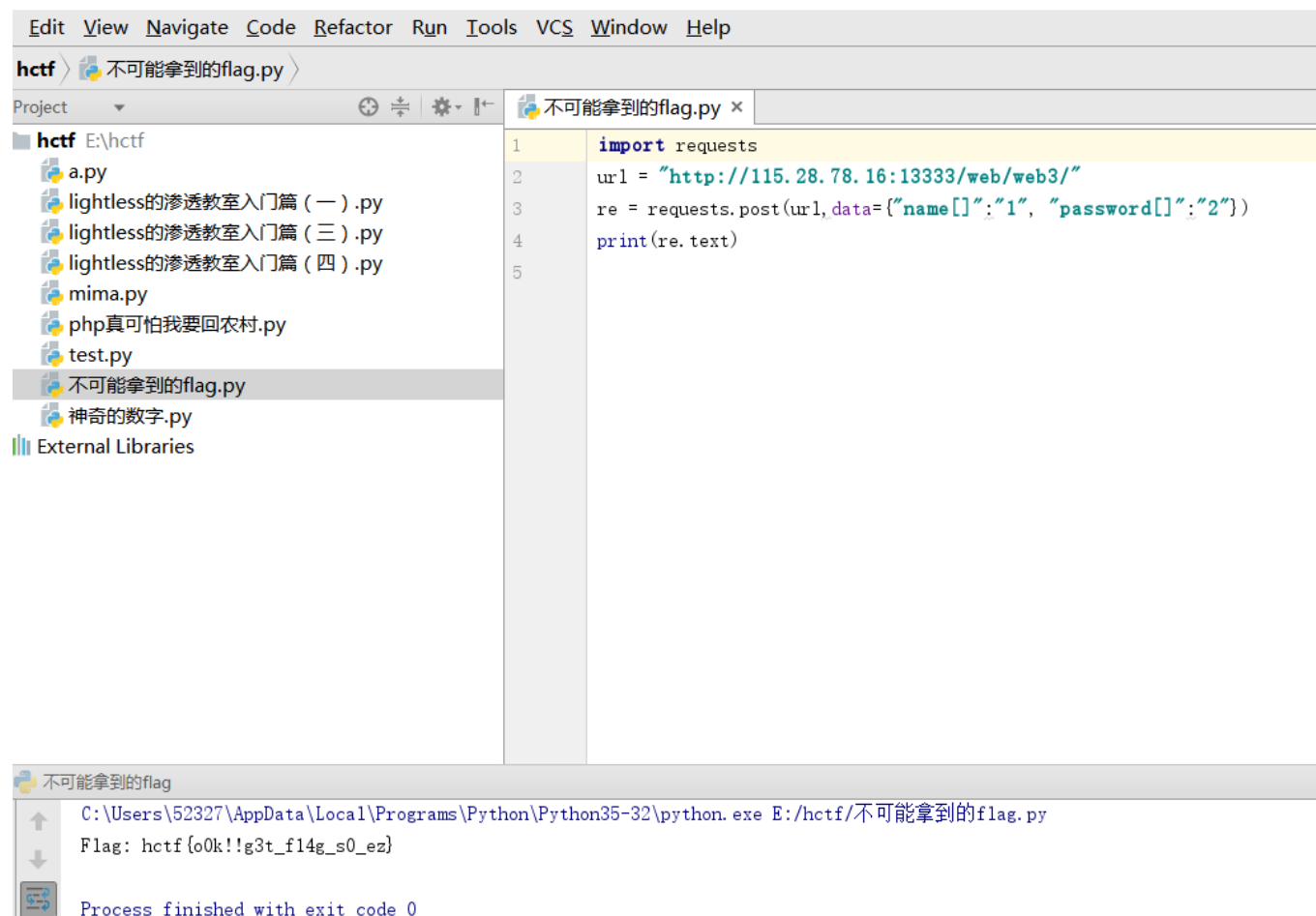


不可能拿到的

flag

```
if (isset($_POST['name']) and isset($_POST['password'])) {
    if ($_POST['name'] == $_POST['password']){
        print 'Your password can not be your name.';
    }else if (sha1($_POST['name']) === sha1($_POST['password'])) {
        die('Flag: '.$flag);
    }else{
        print 'Invalid password';
    }
}
?>
```

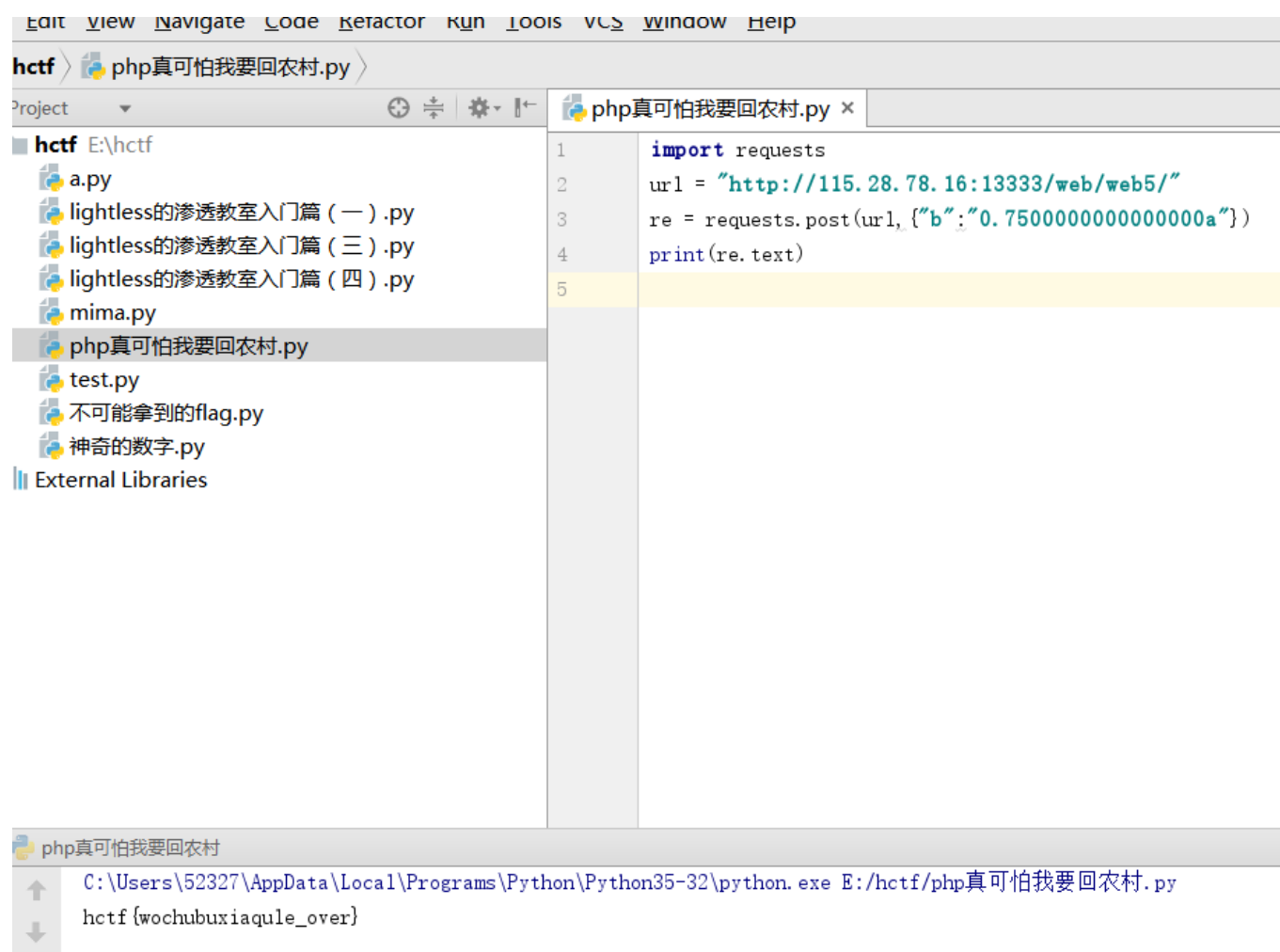
看到 Sha1 直接 post 数组上去 依旧 Python



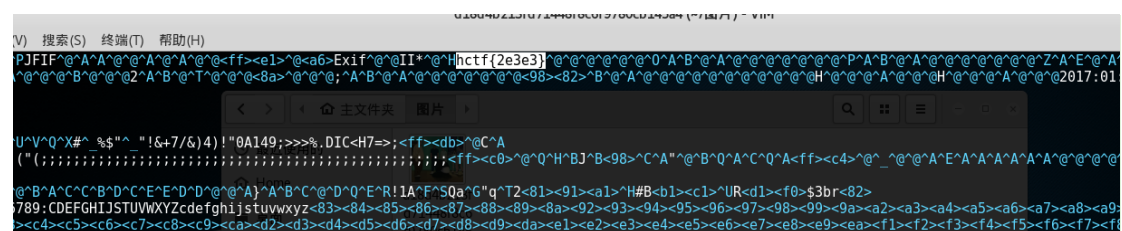
php 真可怕我要回农村

```
$a= "0.1";
$b= $_POST['b'];
if($b != ''){
    if(is_array($b)){
        echo "Something error!";
        exit;
    }
    else if(!is_numeric($b)){
        $c = (int)(( $a + $b ) * 10);
        if($c == "8" && $b[10] == false){
            echo $flag;
        }
        else{
            echo "noflag";
            exit;
        }
    }
}
```

Post 的数字后面加个字母绕过 is_numeric



Explorer 的图库之一



Vim 一看直接出

Explorer 的图库之二

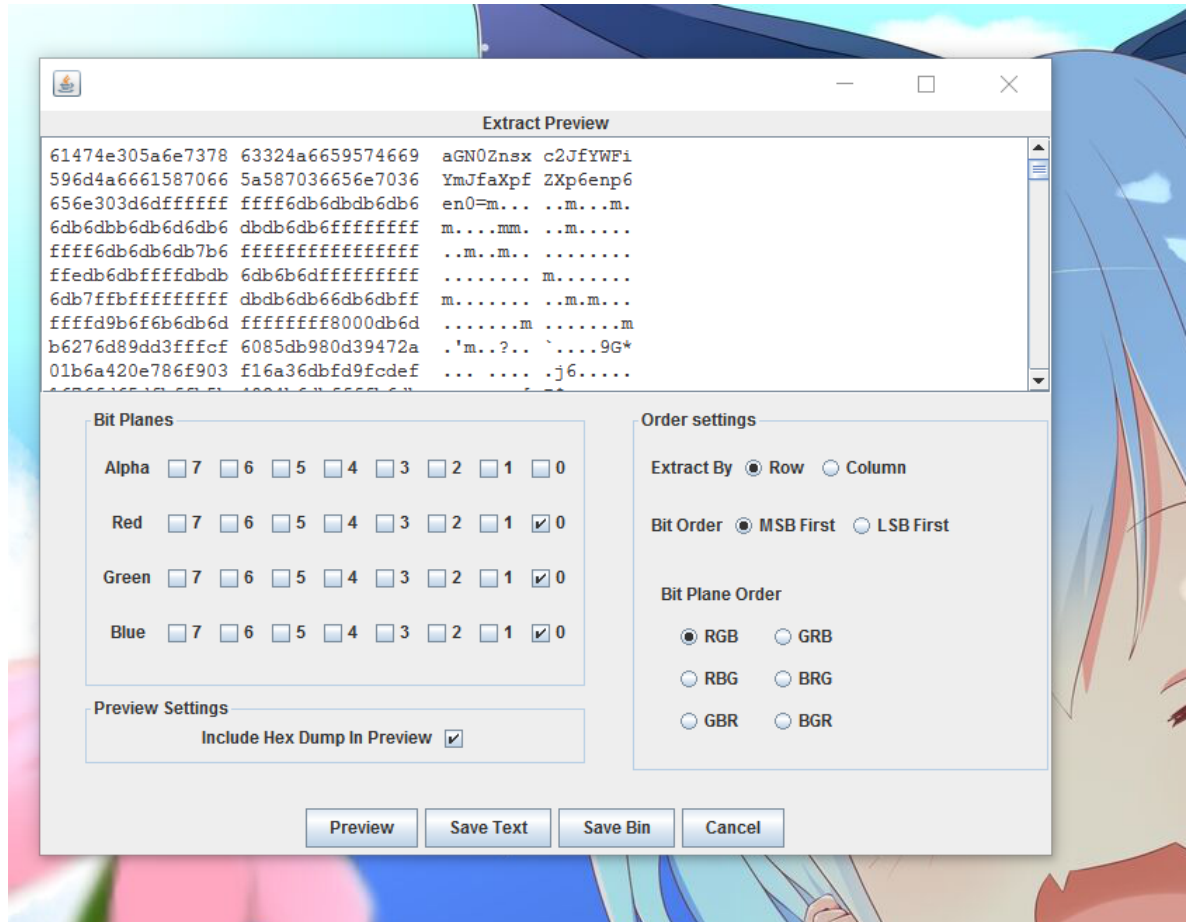
```
root@kali: ~/桌面
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~/桌面# binwalk 1
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
45654       0xB256      gzip compressed data, from Unix, last modified: 20
17-01-15 08:19:26
45801       0xB2E9      PNG image, 1500 x 1072, 8-bit/color RGB, non-inter
laced
45842       0xB312      Zlib compressed data, default compression
root@kali:~/桌面# dd if=1 of=3 skip=45654 bs=1
记录了1428939+0 的读入
记录了1428939+0 的写出
1428939 bytes (1.4 MB, 1.4 MiB) copied, 2.1207 s, 674 kB/s
root@kali:~/桌面# gunzip -c 3.gz
1.txt0000766000175000017500000000003113036630207012250 0ustar lorexxarlorexxarh
ctf{nizhldao tuzh0ngm4}

gzip: 3.gz: decompression OK, trailing garbage ignored
root@kali:~/桌面#
```

Binwalk 一看把 dd 出 gz

Explorer 的图库之三

Binwalk 然后 dd 分离出 PNG 图片 stegsolve 看最低位 最前面那段复制出来 base64 解码得 flag



请输入要进行编码或解码的字符：

aGN0Znsxc2JfYWF1YmJfaXpfZXp6enp6en0=

编码

解码

☐ 解码结果以16进制显示

Base64编码或解码结果：

hctf{lsb_aabbb_iz_ezzzzzz}

密码学教室入门（一）

在线网站 n e d c 全丢就去出结果

of RSA.

n=

5487b497826693313feceaca5b5868add959b85a8fd82c62245ac5ef0

(hex string is expected)

d=

28b95b7e3159a851cbf537e007ae49864b7dbb93fc370a5

(hex string is expected)

e=

190a000845e9c8c2059242835432326369aaf8c7ca85e685bba968b3e

(hex string is expected)

Input data (hex string is expected):

23091e42fa7609c73f1941b320fad6d2ff6e47be588d1623f970f1fee7ab
d221c9834b208f3c888902fe87ca76ec1e1363757d93c6e25c49f1c61c
72b141c0b8848b54a117427d8e30eeab89694eb5f849cafecb0e5361b
9b2b0e3f89e0fdbcc66a6aad4a1a4a85d828083a01a5d569b7eeb6f91
51794453382b524aa52993f9

Mode:

- ☐ Encrypt
☒ Decrypt
☐ Sign

Calculate

Output:

6867616d657b7273615f31735f763372795f65347379217d

16进制到文本字符串的转换，在线实时转换

16进制到文本字符串的转换，在线实时转换

6867616d657b7273615f31735f763372795f65347379217d

16进制转字符

字符转16进制

清空结果

hgame{rsa_1s_v3ry_e4sy!}

密码学教室入门（二）

接完提交发现 8s 不对 就猜是 1s 提交 正确

encrypted text. If you want to know more, I highly recommend this **book**.

m1frj {Hfjxfw_hnumjw_8x_ozxy_ktw_kzs}

Use key:

Encrypt / Decrypt

Output:

hgame{Caesar_cipher_8s_just_for_fun}

密码学教室入门（三）

维吉尼亚密码 一开始纸笔手推 根据字母个数猜测 一个字母的为 a 或 l 两个的为 in is as at 之类的 推出密钥为 bcdef 然后看到了最开始的 DR. manette 百度了一下 出来双城记 翻译了一下得 flag



ai du 百度 主角叫曼内特的书 百度一下

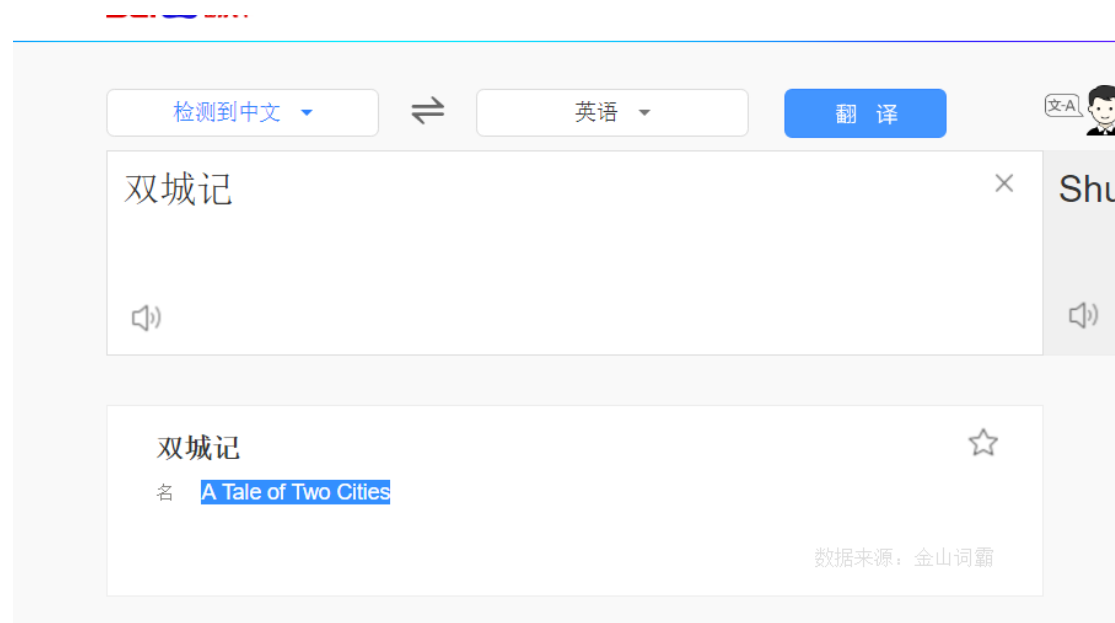
网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»

百度为您找到相关结果约8,590个 搜索工具

[《双城记》中曼内特医生折射的博爱主义光辉_免费下载_百度文库](#)
2013年8月29日 - 摘要:从《双城记》中主人公曼内特医生的角度分析狄更斯的博爱主义精神。
曼内特受侯爵兄弟迫害,在巴士底狱度过了 18 年冤狱。在得知未来的女婿达奈就...
[wenku.baidu.com/link?u...](#) - 百度快照 - 评价

[曼内特医生折射的博爱主义光辉 - 道客巴巴](#)
2014年1月18日 - 第11卷第3期浙江树人大学学报V01.11,No.32011年5月
JOURNALOFZHEJIANGSHURENUNIVERSITYMay2011文学研究曼内特医生折射的博爱主义
光辉贺润东(长沙理工大...
[www.doc88.com/p-665199...](#) - 百度快照 - 1079条评价

[【混乱的曼内特】2016最新混乱的曼内特mp3下载_喜马拉雅听](#)



检测到中文 ⇌ 英语 翻译

双城记 ×

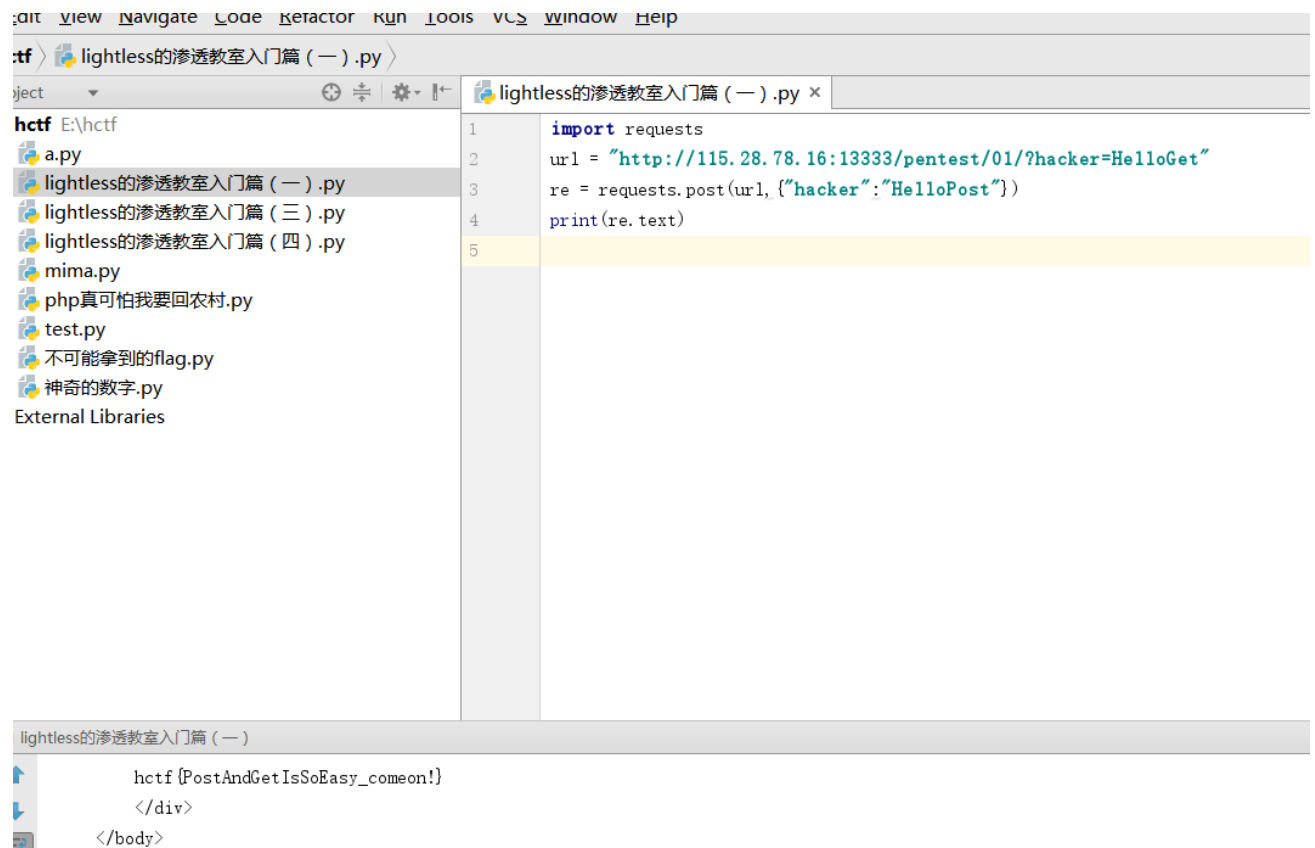
Shu

双城记 ☆

名 [A Tale of Two Cities](#)

数据来源：金山词霸

lightless 的渗透教室入门篇（一）



The screenshot shows the PyCharm IDE interface. The top menu bar includes 'File', 'Edit', 'View', 'Navigate', 'Code', 'Refactor', 'Run', 'Tools', 'VCS', 'Window', and 'Help'. The title bar indicates the file is 'lightless的渗透教室入门篇（一）.py'. The left sidebar shows a project view with the following files: 'a.py', 'lightless的渗透教室入门篇（一）.py' (selected), 'lightless的渗透教室入门篇（三）.py', 'lightless的渗透教室入门篇（四）.py', 'mima.py', 'php真可怕我要回农村.py', 'test.py', '不可能拿到的flag.py', and '神奇的数字.py'. The main editor area displays the following Python code:

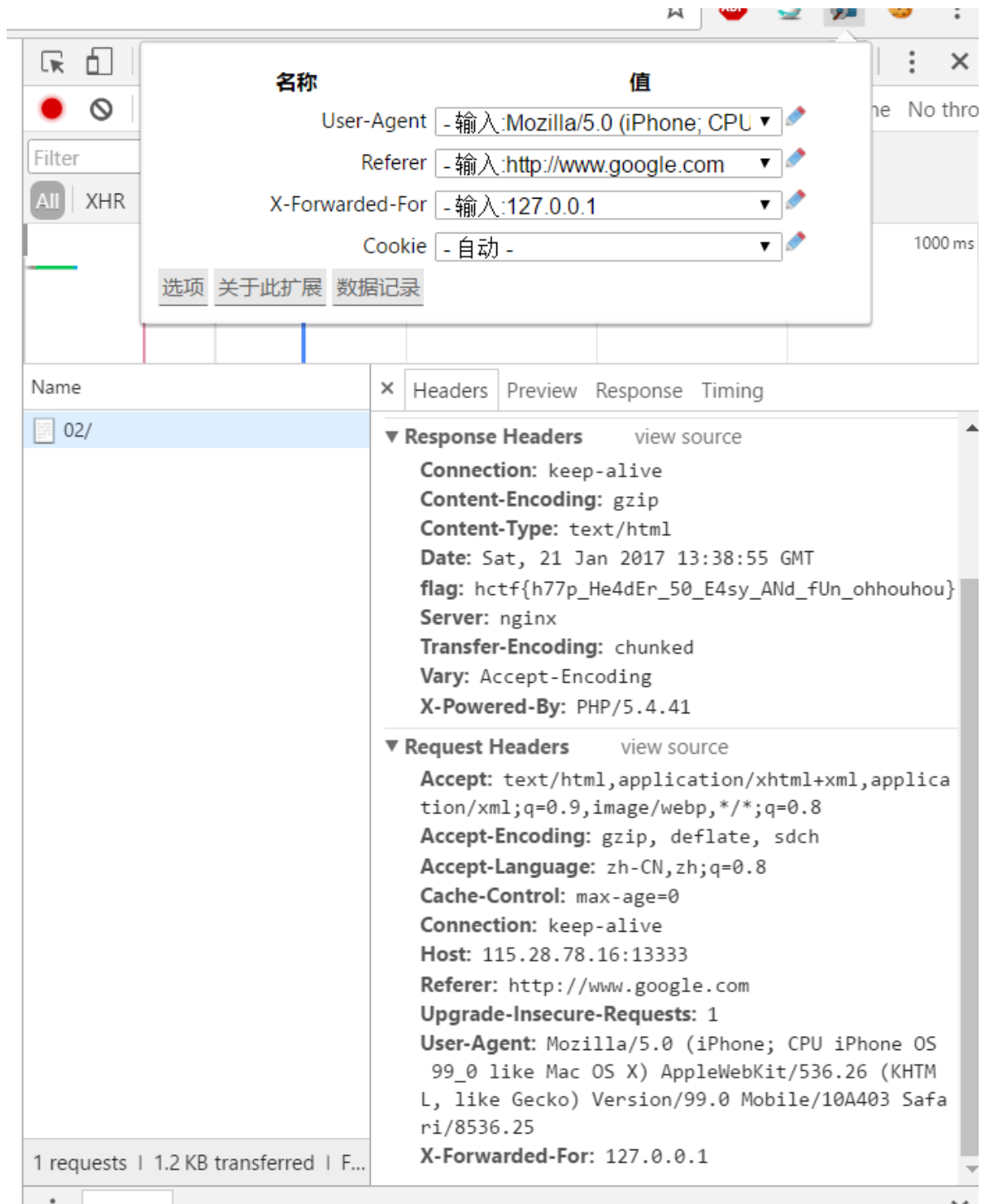
```
1 import requests
2 url = "http://115.28.78.16:13333/pentest/01/?hacker=HelloGet"
3 re = requests.post(url, {"hacker": "HelloPost"})
4 print(re.text)
5
```

The bottom status bar shows the output of the script:

```
lightless的渗透教室入门篇（一）
hctf {PostAndGetIsSoEasy_comeon!}
</div>
</body>
```

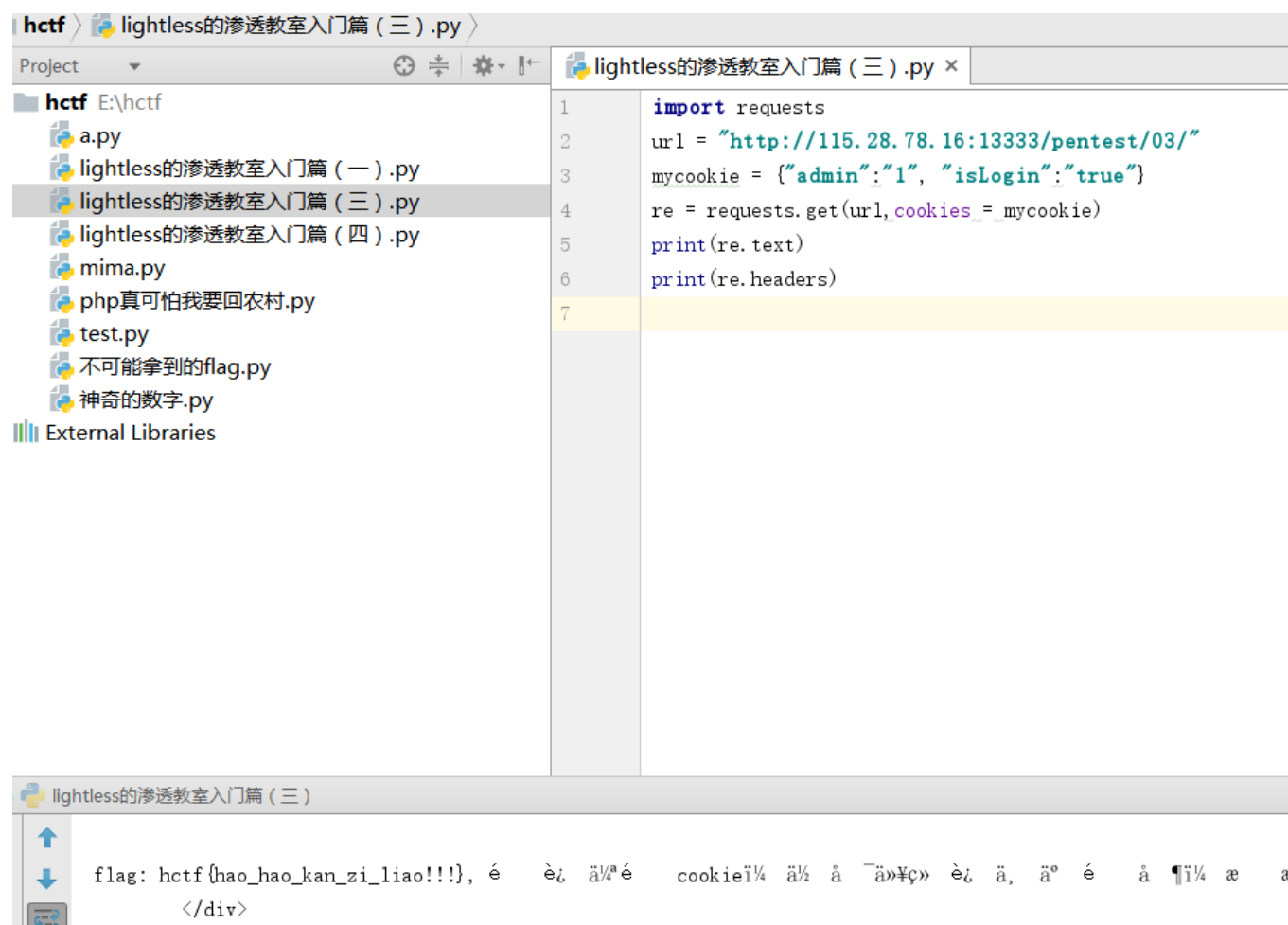
lightless 的渗透教室入门篇（二）

Chrome 插件修改 HTTP 请求头得 flag



lightless 的渗透教室入门篇（三）

根据题目要求 继续 Python



lightless 的渗透教室入门篇 (四)

一开始没第二个提示一脸懵逼 感觉自己好像是对的 然后看了看提示 改了改 依旧 Python

