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

本文链接：https://blog.csdn.net/qq_36119192/article/details/102719130

目录

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

1：key又又找不到了

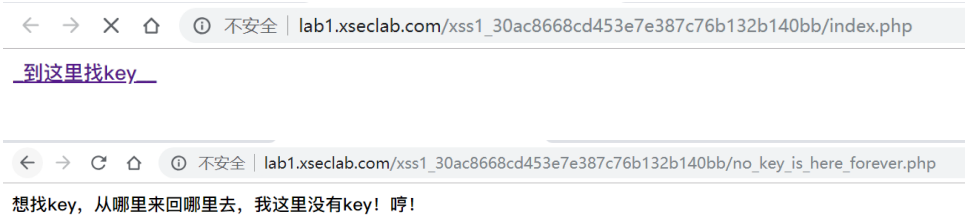
小明这次哭了，key又找不到了！！！ key啊，你究竟藏到了哪里，为什么我看到的页面上都没有啊！！！！！！

通关地址：http://lab1.xseclab.com/xss1_30ac8668cd453e7e387c76b132b140bb/index.php

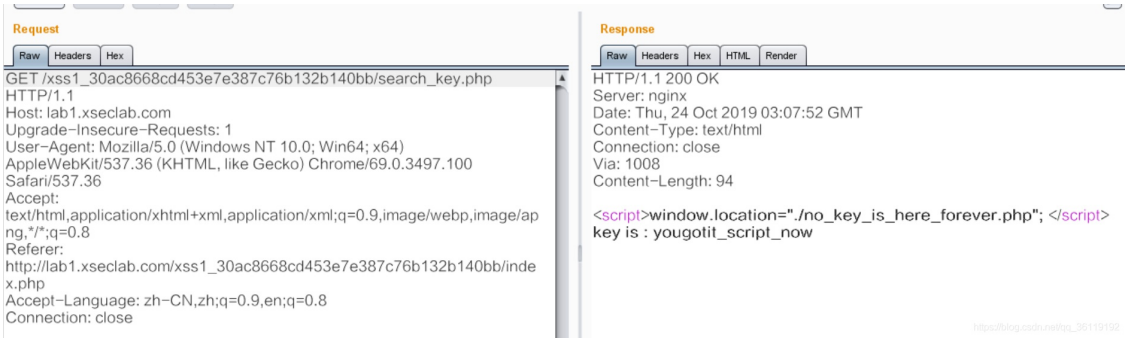
Poc：

这道题考察的是

访问通关地址



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

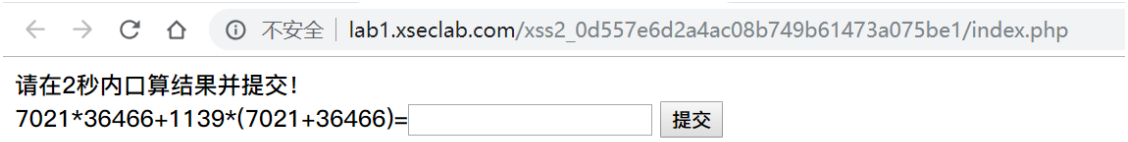
小明要参加一个高技能比赛，要求每个人都要能够快速口算四则运算，2秒钟之内就能够得到结果，但是小明就是一个小学生没有经过特殊的培训，那小明能否通过快速口算测验呢？

通关地址：http://lab1.xseclab.com/xss2_0d557e6d2a4ac08b749b61473a075be1/index.php

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



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

```
# -*- 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])
```

```
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
```


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？

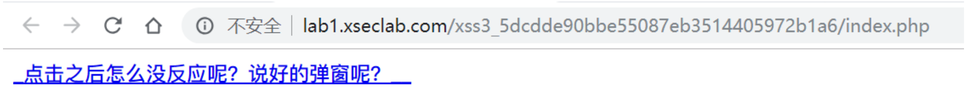
提交说明：提交前14个字符即可过关

通关地址：http://lab1.xseclab.com/xss3_5dcdde90bbe55087eb3514405972b1a6/index.php

Poc:

这题考察的是js的驾驭能力

访问通关地址

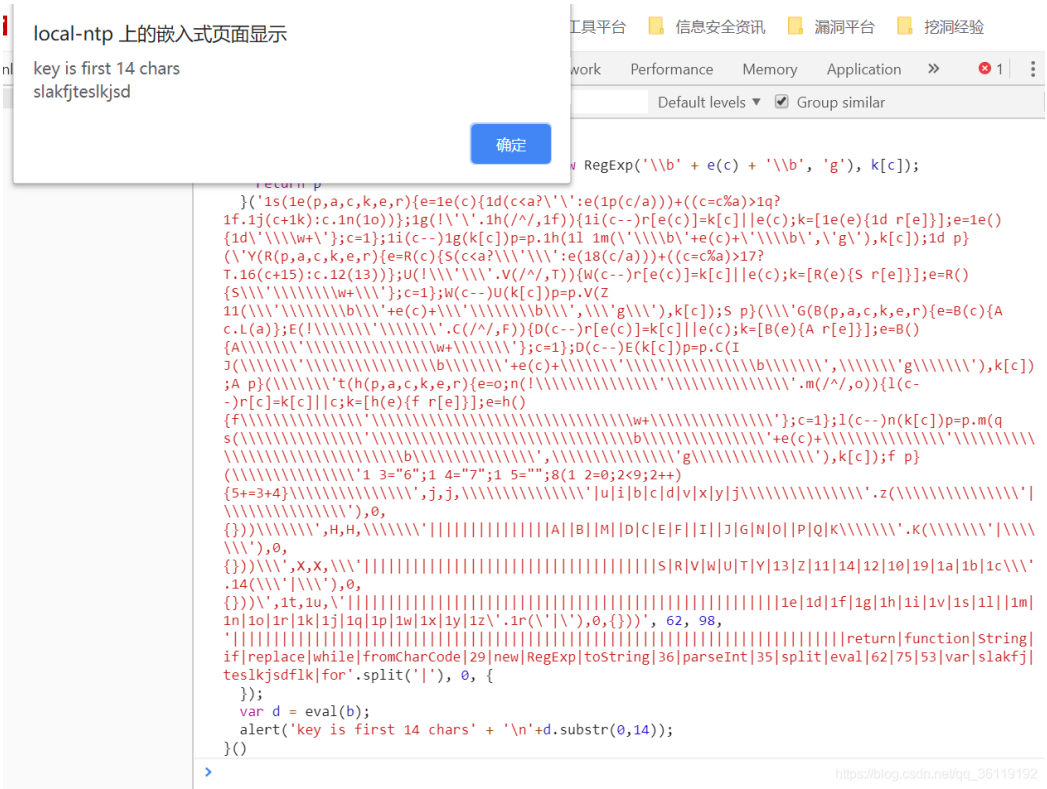


右键查看源代码发现变量a其实是一个匿名函数，而且js里面也禁用了一些常用的弹出对话框的函数

由于js是基于客户端浏览器的，所以我们把代码复制下来，去掉前后的<script></script>，美化成如下

```
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.toStr
    };
    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： slakfjteslkjsd



5：逗比验证码第一期

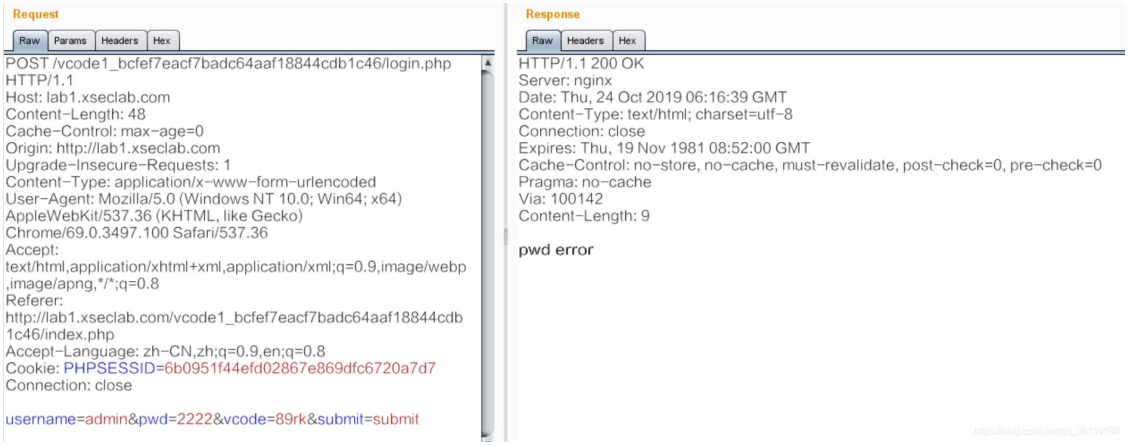
逗比的验证码，有没有难道不一样吗？

通关地址：http://lab1.xseclab.com/vcode1_bcfef7eacf7badc64aaf18844cdb1c46/index.php

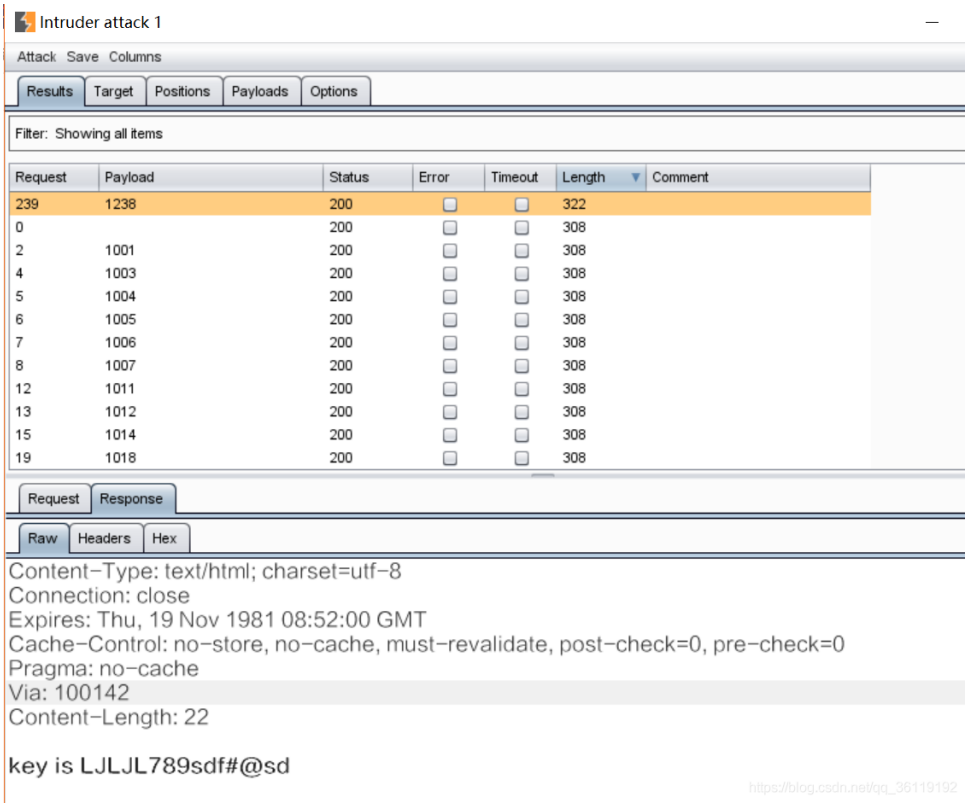
Poc：

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



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：LJLJL789sdf#@sd



6：逗比验证码第二期

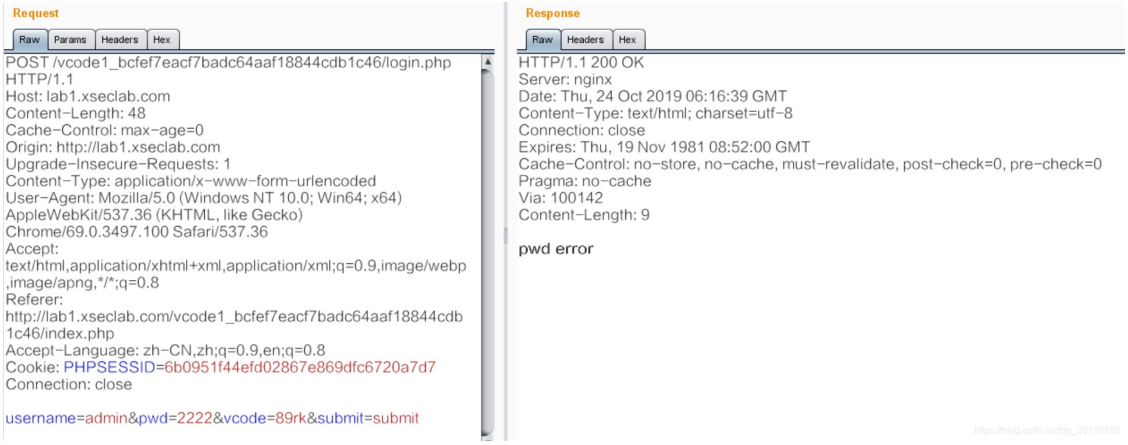
验证便失效的验证码

通关地址：http://lab1.xseclab.com/vcode2_a6e6bac0b47c8187b09deb20babc0e85/index.php

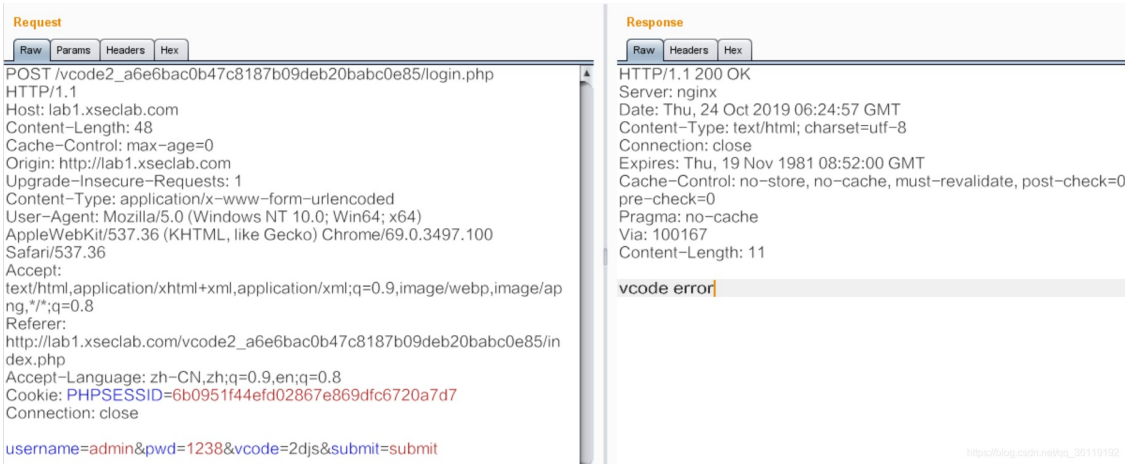
Poc：

这题考察的是选手对于图形验证码的绕过，以及爆破

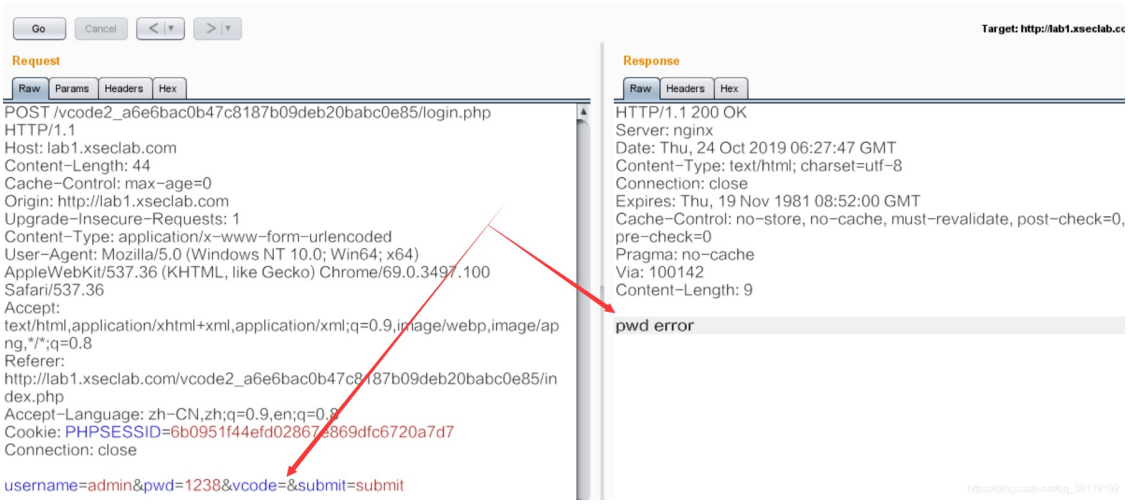
访问通关地址，输入任意的4位数字进行登录，返回pwd error



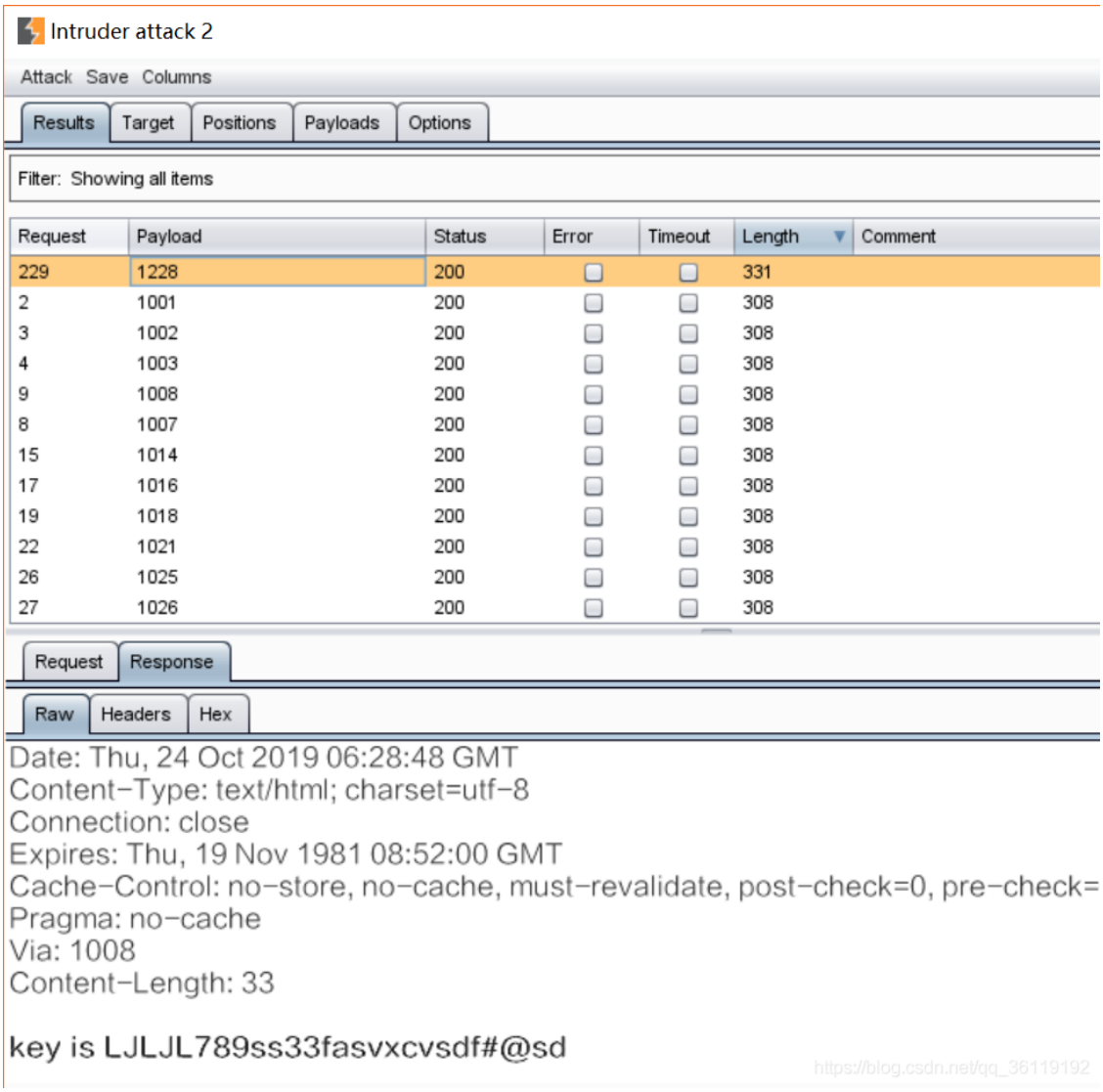
重放，返回的是vcode error。可知验证码验证一次即失效了



尝试删除vcode参数的值，重放，返回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：LJLJL789ss33fasvxcvsdf#@sd



7：逗比的验证码第三期（SESSION）

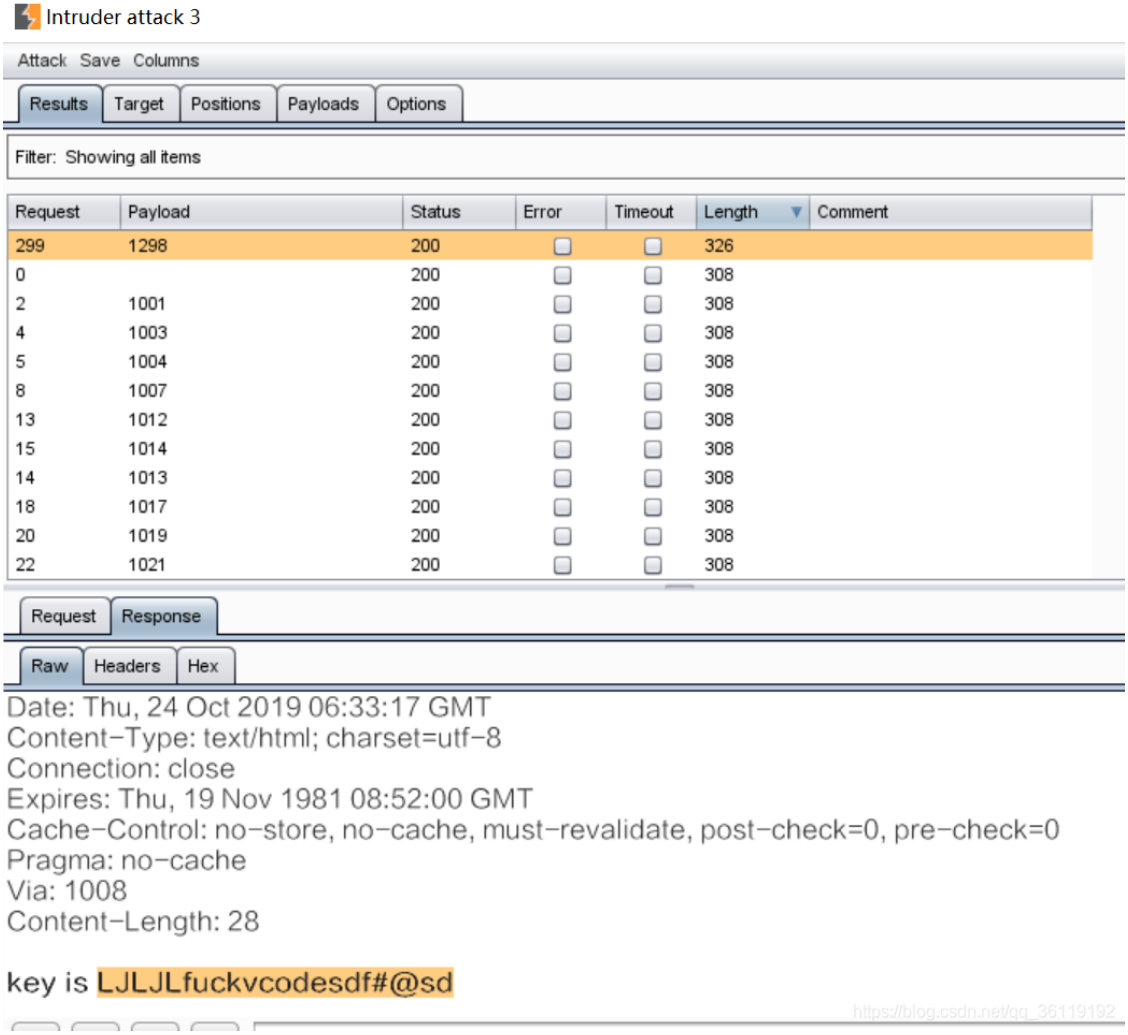
尼玛，验证码怎么可以这样逗比。。验证码做成这样，你家里人知道吗？

通关地址：http://lab1.xseclab.com/vcode3_9d1ea7ad52ad93c04a837e0808b17097/index.php

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：LJLJLfuckvcodesdf#@sd



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

Poc：

这道题考察的是

未完待续。。

9：逗比的手机验证码

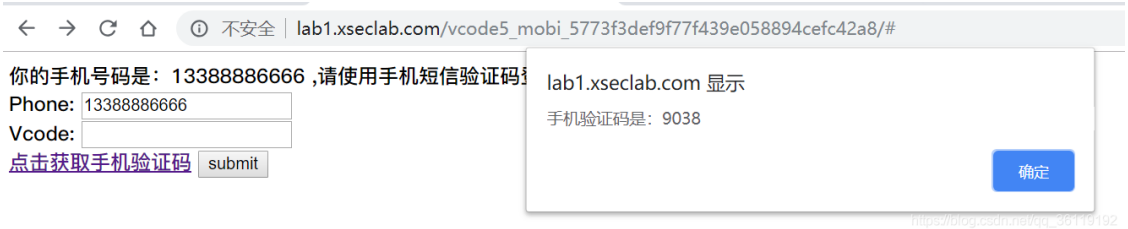
你的手机号码是13388886666，验证码将会以弹窗的形式给出

通关地址：http://lab1.xseclab.com/vcode5_mobi_5773f3def9f77f439e058894cefc42a8/

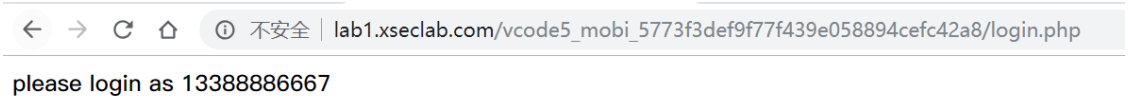
Poc：

这道题考察的是对手机验证码处的逻辑漏洞

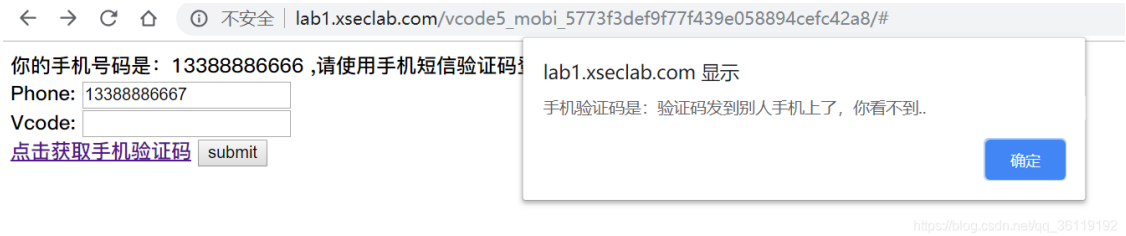
访问通关地址，点击获取验证码弹出手机验证码是9038



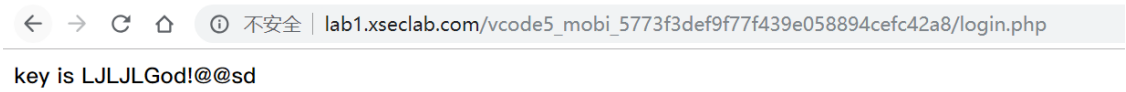
输入9038登录，提示 please login as 13388886667



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

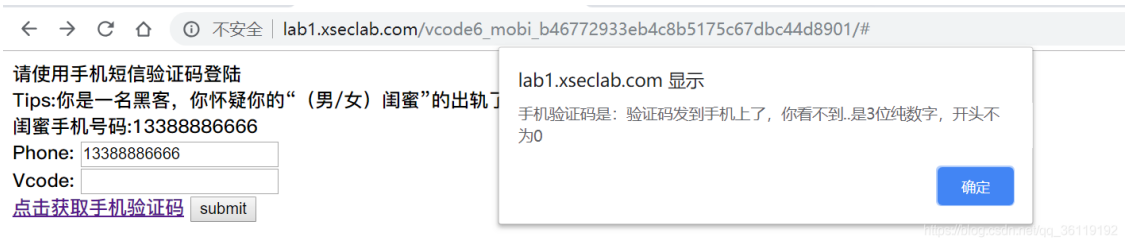
Tips:你是一名黑客，你怀疑你的“（男/女）闺蜜”的出轨了，你要登陆TA手机的网上营业厅查看详单，一探究竟！ 闺蜜手机号码:13388886666

通关地址：http://lab1.xseclab.com/vcode6_mobi_b46772933eb4c8b5175c67dbc44d8901/

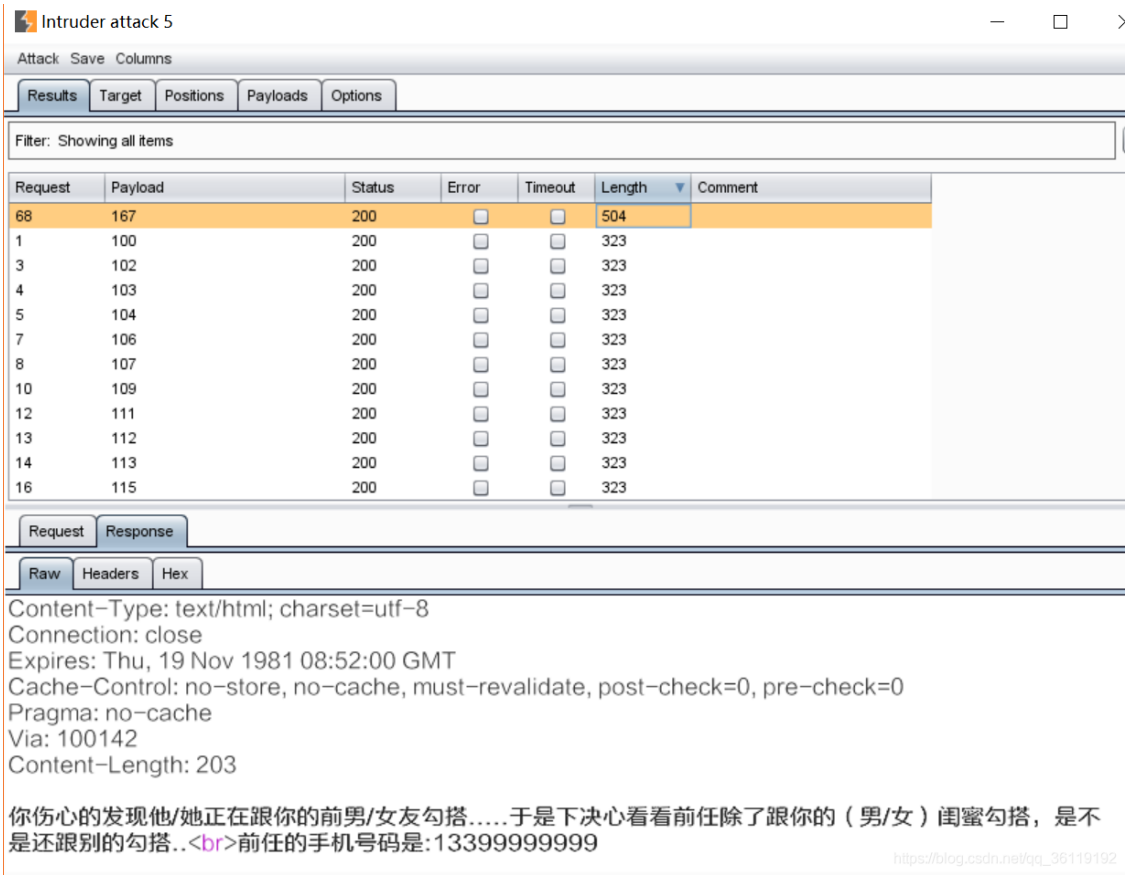
Poc：

这道题考察的是对手机验证码的爆破

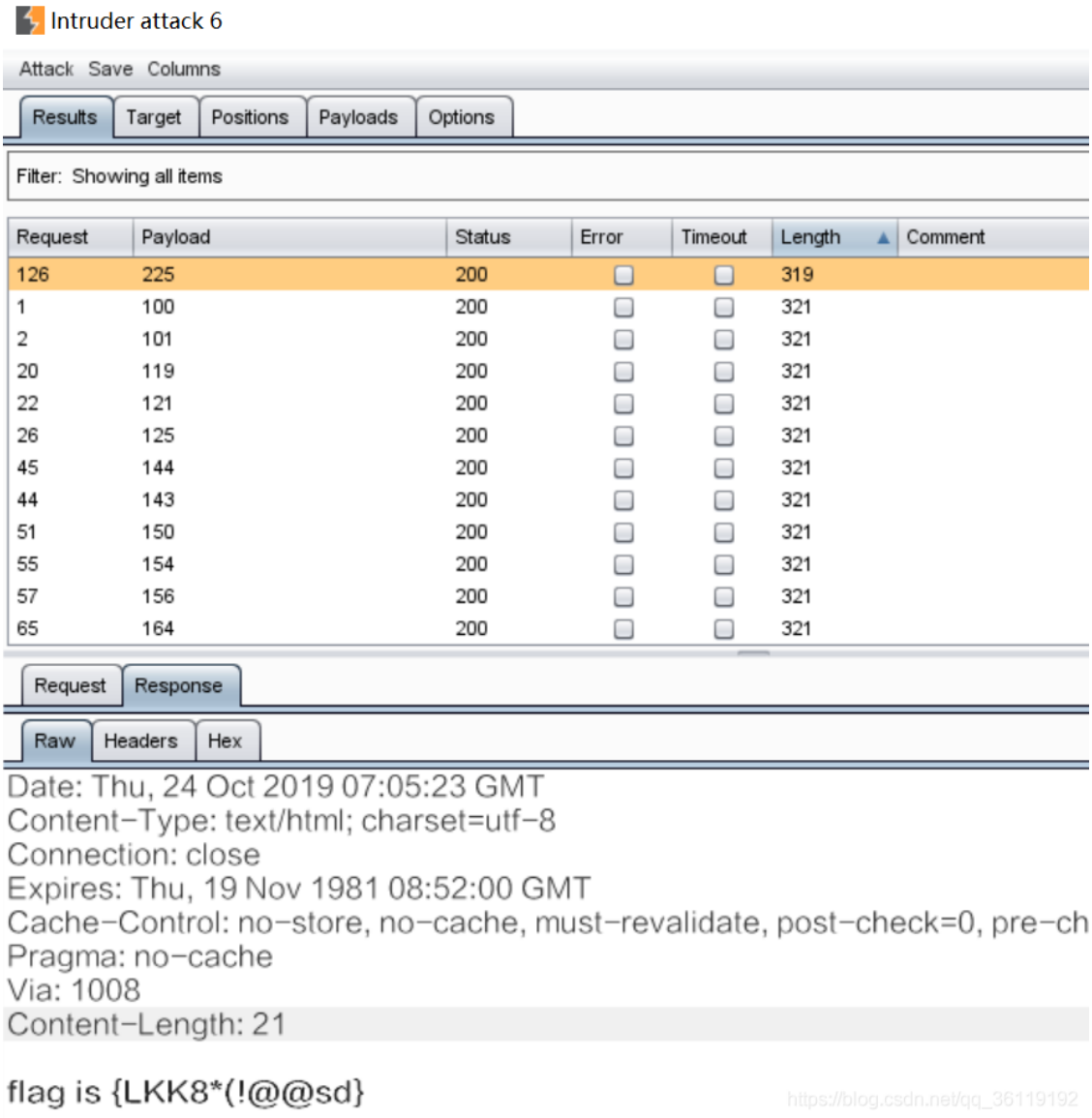
访问通关地址，点击获取手机验证码，返回如图



很自然的想到了对验证码的爆破，结果得到了下面的结果



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



11：验证码识别

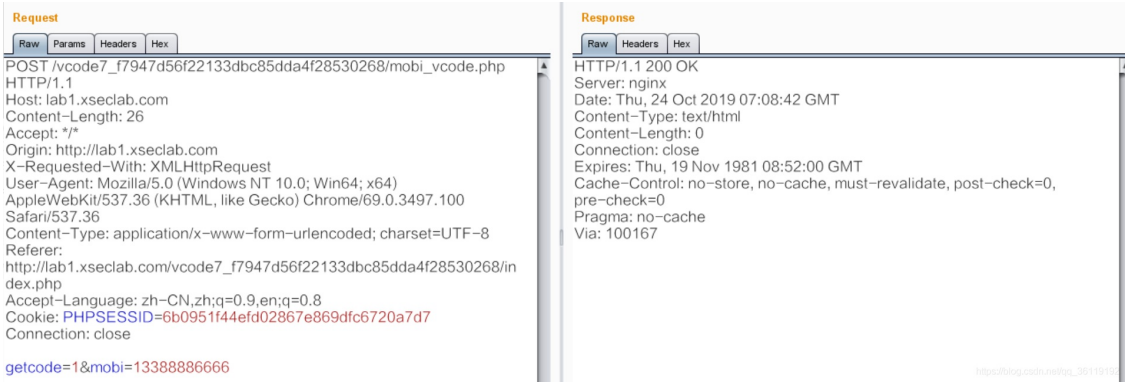
Tips:验证码依然是3位数

通关地址：http://lab1.xseclab.com/vcode7_f7947d56f22133dbc85dda4f28530268/index.php

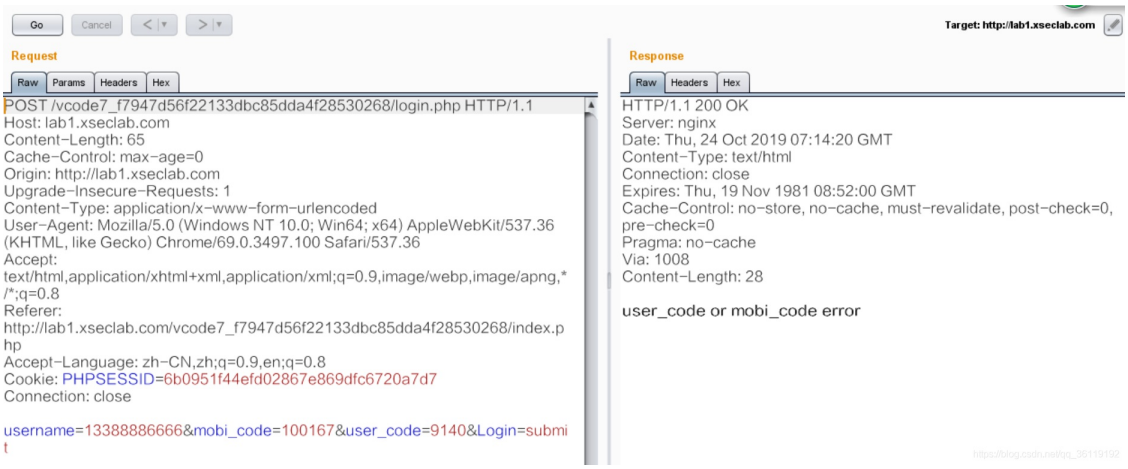
Poc：

这道题考察是的对图形验证码的破解和对手机验证码的爆破

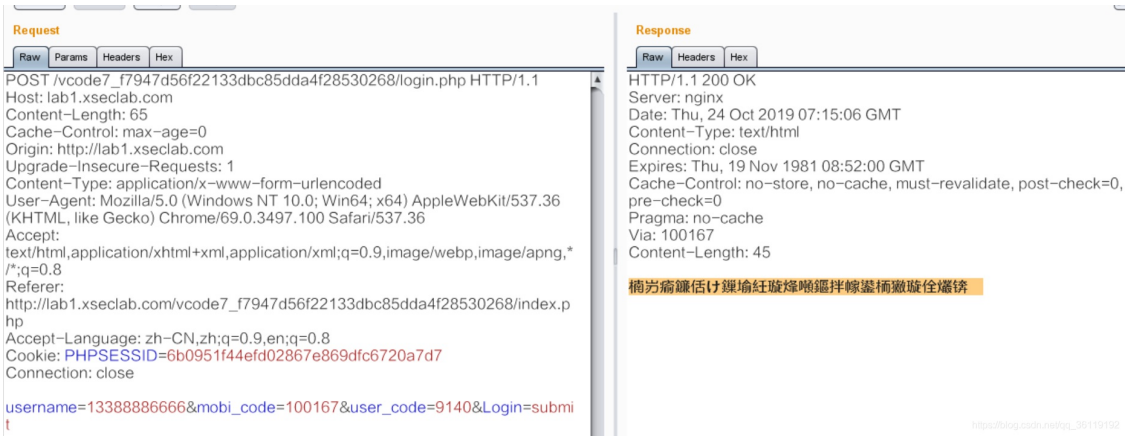
访问通关地址点击获取验证码，但是并不知道验证码是多少，用bp抓包，返回包中也没有验证码



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_f123c17dd9c3633346701017791939 98/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：myxsstestst art!

13：XSS基础2:简单绕过

很容易就可以过关.

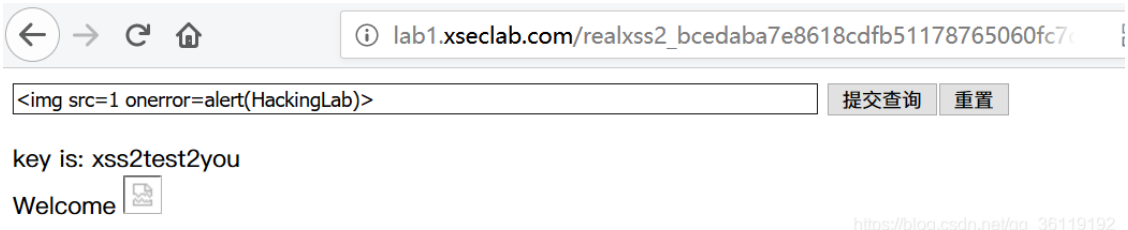
通关地址：http://lab1.xseclab.com/realxss2_bcedaba7e8618cdfb51178765060fc7d/index.php

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

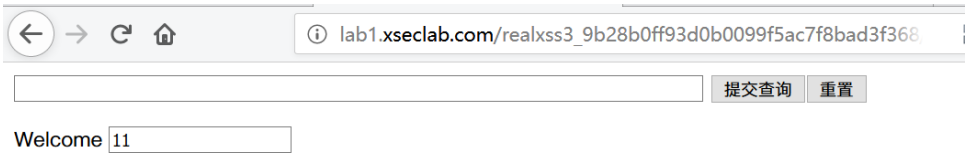
XSS基础3:检测与构造
Tips:不是很难

通关地址：http://lab1.xseclab.com/realxss3_9b28b0ff93d0b0099f5ac7f8bad3f368/index.php

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



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

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