hackinglab.cn网络安全实验室基础关

原创

AlcyoneYYXJ 于 2018-10-30 13:22:14 发布 2777 收藏 1

分类专栏： Web安全 WriteUp 文章标签： Web安全 Writeup 入门

本文链接：https://blog.csdn.net/AlcyoneYYXJ/article/details/83540287


Web安全 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏


WriteUp

1 篇文章 0 订阅

订阅专栏

作者：AlcyoneYYXJ

如有错误or不同的思路还请给位指正交流&学习

，

第一题 Key在哪里？

http://lab1.xseclab.com/base1_4a4d993ed7bd7d467b27af52d2aaa800/index.php

题目地址

第二题 再加密一次你就得到Key啦~

再加密一次你就得到key啦~

分值: 150

加密之后的数据为xrlvf23xfqwsxsqf

凯撒密码

在下面的文本框输入明文或密文，点加密或解密，文本框中即可出现所得结果

加密 解密 列出所有组合 位移数(-25~25): 1

密文框:

```
cwqak23ckvbxcxvk
dxrbl23dlwcydywl
eyscm23emxdzezxm
fztdn23fnyeafayn
gaueo23gozfbgbzo
hbvfp23hpagchcap
icwgq23iqbhdidbq
jdxhr23jrciejecr
keyis23ksdjfkfds
lfzjt23ltekglget
mgaku23muflhmhfu
nhblv23nvgminigv
oicmw23owhnjojhw
pjdnx23pxiokpkix
qkeoy23qyjplqljy
rlfpz23rzkqmrmkz
```

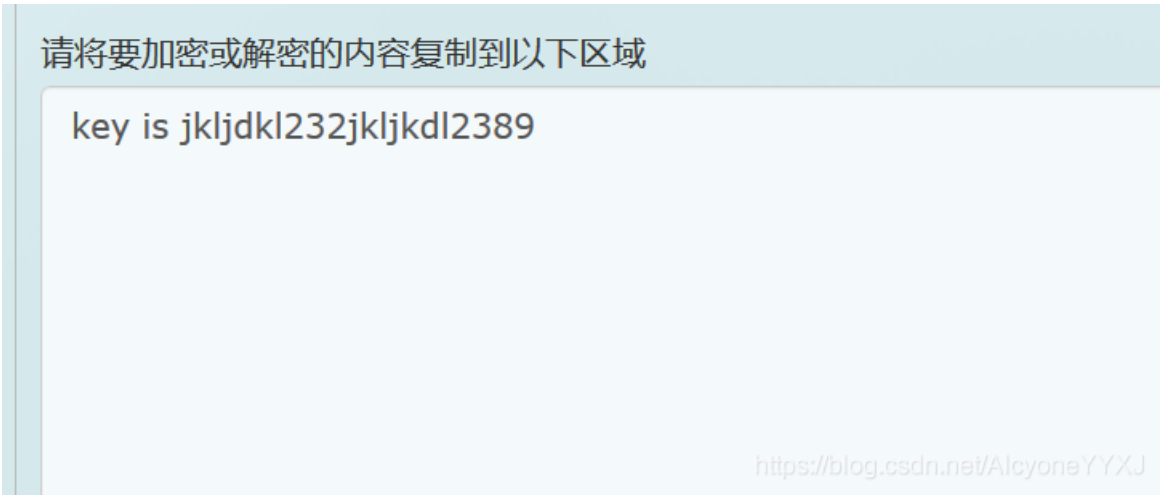

第三题 猜猜这是经过了多少次加密

加密后的字符串为:

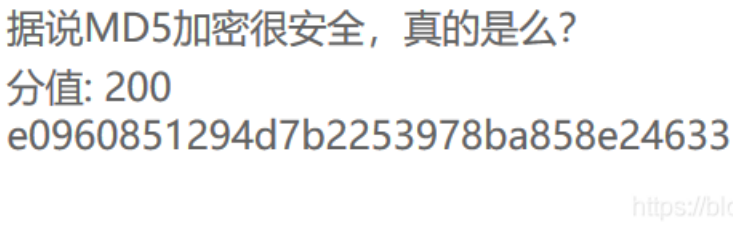
Vm0wd2QyUXlVWGxWV0d4V1YwZDRWMVl3WkRSV01WbDNXa1JTVjAxV2JETlhhMUpUVmpBeFYySkVUbGhoTVVwVVZtcEJlRll5U2tWVWJHaG9UVlZ3
VlZacVFtRlRNbEpJVm10a1dHSkdjRTlaVjNSR1pVWmFkR05GU214U2JHdzFWVEowVjFaWFNraGhSemxWVmpOT00xcFZXbUZrUjA1R1drWndWMDFF
UlRGV1ZFb3dWakZhV0ZOcmFHaFNlbXhXVm1wT1QwMHhjRlpYYlhSWFRWaENSbFpYZUZOVWJVWTJVbFJDVjAxdVVuWlZha1pYWkVaT2NscEdhR2xT
TW1ob1YxWlNTMkl4U2tkWGJHUllZbFZhY1ZadGRHRk5SbFowWlVaT1ZXSlZXVEpWYkZKSFZqRmFSbUl6WkZkaGExcG9WakJhVDJOdFJraGhSazVz
WWxob1dGWnRNWGRVTVZGM1RVaG9hbEpzY0ZsWmJGWmhZMnhXY1ZGVVJsTk5XRUpIVmpKNFQxWlhTa2RqUm14aFUwaENTRlpxUm1GU2JVbDZXa1pr
YUdFeGNHOVdha0poVkRKT2RGSnJhR2hTYXpWeldXeG9iMWRHV25STldHUlZUVlpHTTFSVmFHOWhiRXB6WTBac1dtSkdXbWhaTVZwaFpFZFNTRkpy
TlZOaVJtOTNWMnhXYjJFeFdYZE5WVlpUWVRGd1YxbHJXa3RUUmxweFVtMUdVMkpWYkRaWGExcHJZVWRGZUdOSE9WZGhhMHBvVmtSS1QyUkdTbkpo
UjJoVFlYcFdlbGRYZUc5aU1XUkhWMjVTVGxOSFVuTlZha0p6VGtaVmVXUkhkRmhTTUhCSlZsZDRjMWR0U2tkWGJXaGFUVzVvV0ZsNlJsZGpiSEJI
V2tkc1UySnJTbUZXTW5oWFdWWlJlRmRzYUZSaVJuQlpWbXRXZDFZeGJISlhhM1JVVW14d2VGVXlkR0ZpUmxwelYyeHdXR0V4Y0hKWlZXUkdaVWRP
UjJKR2FHaE5WbkJ2Vm10U1MxUnRWa2RqUld4VllsZG9WRlJYTlc5V1ZscEhXVE5vYVUxWFVucFdNV2h2VjBkS1dWVnJPVlpoYTFwSVZHeGFZVmRG
TlZaUFYyaHBVbGhCZDFac1pEUmpNV1IwVTJ0b2FGSnNTbGhVVlZwM1ZrWmFjVk5yWkZOaVJrcDZWa2N4YzFVeVNuSlRiVVpYVFc1b1dGZFdXbEps
Um1SellVWlNhVkp1UWxwV2JYUlhaREZaZUdKSVNsaGhNMUpVVlcxNGQyVkdWbGRoUnpsb1RWWndlbFl5Y0VkV01ERjFZVWhLV2xaWFVrZGFWM2hI
WTIxS1IyRkdhRlJTVlhCS1ZtMTRVMU14VlhoWFdHaFlZbXhhVjFsc1pHOVdSbXhaWTBaa2JHSkhVbGxhVldNMVlWVXhXRlZyYUZkTmFsWlVWa2O0

```
YWtvMFZUSkdXRk5yYkZKaVIyaFlXV3hvVTFkR1pGZGFSbVJxVFZkU01WVnRlRTloVmtsNFUyNW9WMUpzY0hKV1ZFcFhZekpLUjFkdFJsUlNWRloy
Vm0weE5HUXlWbGRoTTJSV1lsVmFXRlJWVWtkWFZscFhZVWQwV0ZKc2NEQldWM2hQV1ZaYWMyTkhhRnBOYm1nelZXcEdkMUl5UmtkVWF6Vk9ZbGRq
ZUZadE1UUmhNREZIVjFob1ZWZEhhR2hWYkdSVFZqRnNjbHBHVGxoV2JYZ3dWRlphVDJGck1WZGpSRUpoVmxkb1VGWkVSbUZrVmtaeldrWndWMVl4
UmpOV2FrSmhVMjFSZVZScldtaFNia0pQVlcwMVEwMXNXbkZUYm5Cc1VtczFTVlZ0ZEdGaVJrcDBWV3M1V21KVVJuWlpha1poWTFaR2RGSnNaRTVo
ZWxZMlYxUkNWMkl4VlhsVGEyaFdZa2RvVmxadGVHRk5NVnBZWlVkR2FrMVdXbmxXUjNocllVZFdjMWRzYkZkaGExcDJXV3BLUjJNeFRuTmhSMmhU
WlcxNFdGZFdaREJrTWxKelYydFdVMkpHY0hKVVZscDNaVlp3UmxaVVJtaFdhM0F4VlZab2ExZEhTa2RYYmtaVllrZFNSMXBFUVhoV01XUnlUbFpr
VTJFelFscFdiVEIzWlVkSmVWVnVUbGhYUjFKWldXeG9VMVpXVm5GUmJVWlVZa1phTUZwVlpFZGhSbHB5WWtSU1ZtSkhhSEpXYWtwTFZsWktWVkZz
Y0d4aE0wSlFWMnhXWVdFeVVsZFdiazVWWWxkNFZGUldWbmRXYkZsNFdrUkNWMDFzUmpSWGEyaFBWMGRGZVdGSVRsWmhhelZFVmxWYVlXUkZNVmRV
YkZKVFlrZDNNVlpIZUZaT1YwWklVMnRhYWxKRlNtaFdiR1JUVTBaYWMxZHRSbGROYXpWSVYydGFWMVl5U2tsUmFscFhZbGhDU0ZkV1dtdFhSa3B5
WVVkd1UwMXVhRmxXYWtKWFV6Rk9SMWR1VW14U00xSlFWV3BDVjA1R1dsaE9WazVXVFd0d2VWUnNXbk5YYlVWNFkwZG9WMDFXY0doYVJWVjRWakZP
Y2s1V1RtbFNiWFExVm14amQyVkdTWGxTYmxKVFlXeHdXRmxyWkc5WlZteFZVbTVrVlZKdGVGaFdNblF3WVdzeGNrNVZhRnBoTVhCMlZtcEJkMlZH
VG5SUFZtaG9UVlZ3U1ZkV1VrZFhiVlpIWTBWc1ZHSlhhRlJVVkVaTFZsWmFSMVp0Um10TlYxSllWakowYTFsV1RrbFJiazVXWWtaS1dGWXdXbUZr
UlRWWFZHMW9UbFpYT0hsWFYzUmhZVEZhZEZOc2JHaFRTRUpXV1d0YWQyVnNXblJOVldSVFlrWktlbGRyWkhOV01XUkdVMnQwVjAxV2NGaFdha1pX
WlVaa1dWcEZOVmRpVmtwNFZsZHdTMkl4YkZkVmJHUllZbTFTVjFWdE1UQk9SbGw1WlVkMGFHRjZSbGxXVnpWelZsZEtSMk5JU2xkU00yaG9WakJr
VW1WdFRrZGFSMnhZVWpKb1ZsWnNhSGRSYlZaSFZHdGtWR0pIZUc5VmFrSmhWa1phY1ZOdE9WZGlSMUpaV2tWa01HRlZNWEppUkZKWFlsUldWRlpI
ZUdGT2JVcElVbXhrYVZkSFozcFhiRnBoV1ZkU1JrMVdXbUZTYkZwdldsZDBZVmRzWkhOV2JVWm9UVlpzTTFSV2FFZFdNa3B5WTBab1YyRXhXak5X
UlZwV1pVWmtjbHBIY0dsV1ZuQkpWakowWVZReFVuSk5XRkpvVW14d1dGbHNVa2ROTVZZMlVtczFiRlpzU2pGV1IzaFhZVmRGZWxGdWFGZFdla0kw
V1dwS1QxSXhXblZWYlhoVVVqRktkMVpHV210Vk1XUkhWMnhvYTFKRlNsZFVWVkpIVjBac2NsVnNUbGROVld3MldWVm9kMWRzV1hwaFJYaGhVbXh3
U0ZreWN6VldNVnB6V2tkNGFFMVhPVFZXYlRGM1VqRnNWMkpHWkZSWFIyaHdWV3RhZDFaR2JITmFSRkpWVFZad2VGVnRkREJXUmxwelkwaG9WazFX
U2toV1ZFRjRWakZhY1Zac1drNWliRXB2VjFaa05GUXhTbkpPVm1SaFVtNUNjRlZ0ZEhkVFZscDBaRWRHV0dKV1dsbFdiWFJ2WVRGSmVsRnVRbFpp
VkZaRVZtcEdZVmRGTVZWVmJXeE9WbXhaTVZaWGVHOWtNVlowVTJ4YVdHSkhhRmhaYkZKSFZURlNWbGR1VGs5aVJYQXdXa1ZhVDFSc1dYaFRXR2hY
WWtkUk1GZFdaRWRUUms1eVlrWkthVkl4U2xsWFYzaFRVbXN4UjJORlZsUmlSMUp4VkZaa1UwMVdWblJsUlRsb1ZtdHNORlV5Tlc5V01VcHpZMGhL
VjFaRmNGaFpla3BMVWpGa2RGSnNVbE5XUmxveVZtMHdlRTVIVVhsV2JHUm9UVEpTV1ZsdE1WTlhSbEpZWkVoa1ZGWnNjRWxaTUZwUFZqRlpkMVpx
VmxkV00yaFFWMVphWVdNeVRraGhSbkJPWW0xbmVsWlhjRWRrTVU1SVUydG9hVkpyTlZsVmJGWjNWVEZhZEUxSVpHeFNWRlpKVld4b2IxWXhaRWho
UjJoV1lrZFNWRlpxUm5OamJHUjFXa1prVGxZemFGZFdWRW8wVkRKR2NrMVdaR3BTUlVwb1ZteGFXbVF4YkhKYVJYUlRUV3MxUmxWWGVGZFdNVnB5
WTBac1YySllRa05hVlZwTFZqRk9kVlJ0UmxOaWEwcDNWMWN4TUZNeFVsZFhibEpPVTBkb1ZWUldaRk5YUmxwMFRsWmtXRkl3Y0VsV1Z6QTFWMnhh
UmxkcVRscGhhMXBvVmpCVmVGWldWblJoUlRWb1pXeFdNMVp0TUhoTlIwVjRZa1prVkZkSGVHOVZibkJ6Vm14YWNsWnJkRlZTYkhCWldsVmtSMkZy
TVZoa1JGcGFWbFpWTVZaVVNrdFhWMFpIWTBaa2FFMVlRakpYVjNCTFVqSk5lRlJ1VG1oU01taFZWV3hXZDFkR1pGaGxSemxWWWxaYVNGWXlkRmRW
TWtwV1YyNUdWVlp0VWxSYVYzaHlaREZ3UlZWdGFGZGhNMEY0VmxaYWIyRXhaRWhUYTJSWVltdHdWMWxYZEdGaFJtdDVZek5vVjAxWFVqQlphMXBQ
VlRKRmVsRnRPVmROVm5CVVZXcEtVbVZXVW5WVWJHaFlVakZLYjFaWGVHOVZNazVYWWtoT1YxWkZXbFJVVmxwSFRrWlplVTFVUW1oU2JIQXdWbGQw
YzFkSFJuSk9WRTVYWVd0d1NGa3llRTlrUjBaSFkwZDRhRTFZUWpWV2JYQkRXVlpWZVZSdVRtcFNWMmhVV1d0Vk1XTkdXblJrU0dSWFlrWnNORmRy
VWtOWGJGbDRVbXBPVldKR2NISldNR1JMWXpGT2NrOVdaR2hOVm5CTlZqRmFZVmxYVWtoV2ExcGhVbFJzVkZscmFFSmtNV1J6Vm0xR2FFMVdjRmxW
TW5SaFlXeEtXR1ZIUmxWV1JUVkVXbFphVjFJeFNsVmlSa1pXVmtSQk5RPT0=
```

这个末尾的=给人直觉这是base64 又说多次加密
而且base64就是越加密越长，那就把这些多次base64解码
越解越短，最终得到



第四题 据说MD5加密很安全，真的是吗？



在线查询MD5

结果就是key

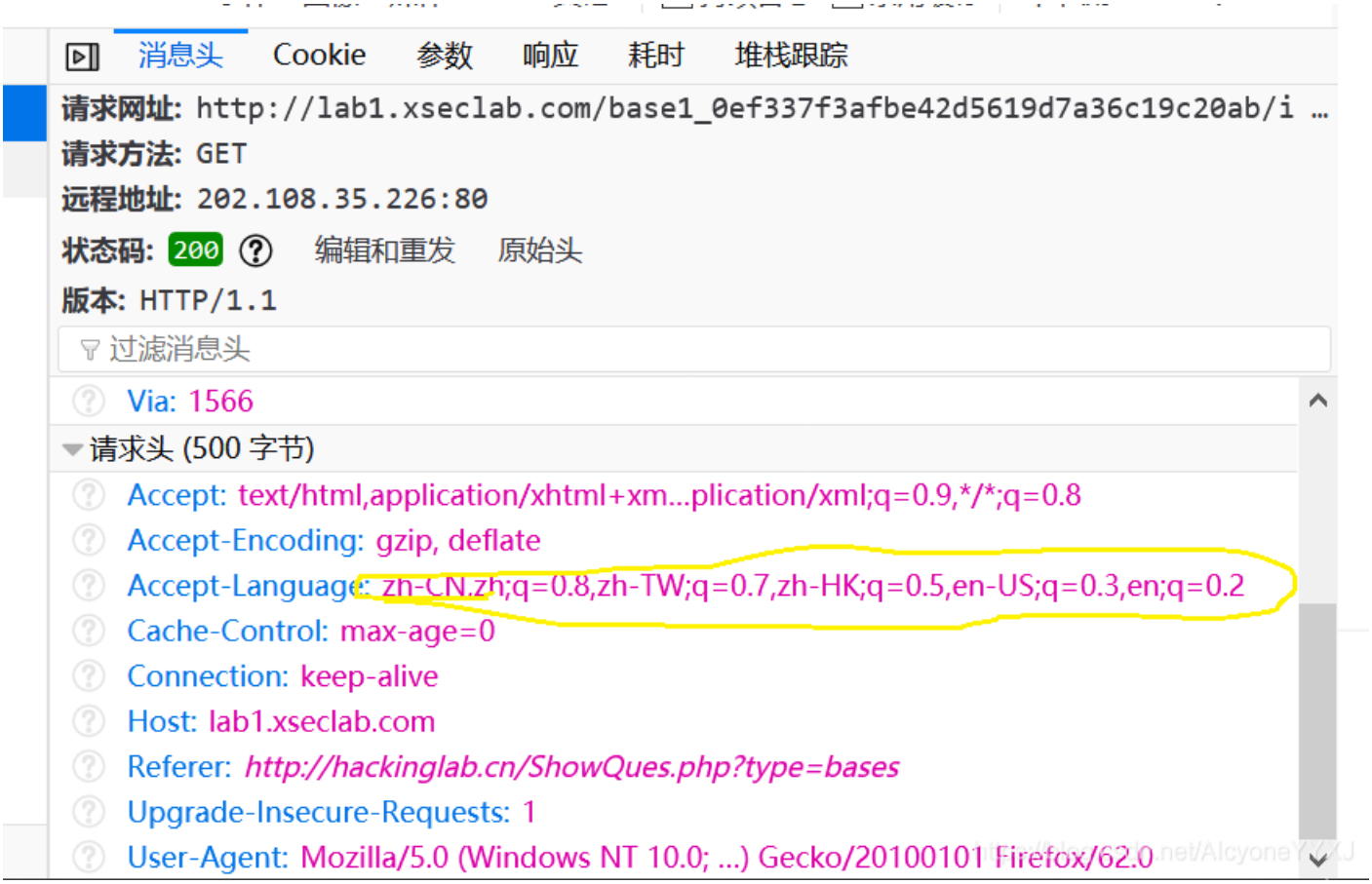
第五题 种族歧视

种族歧视

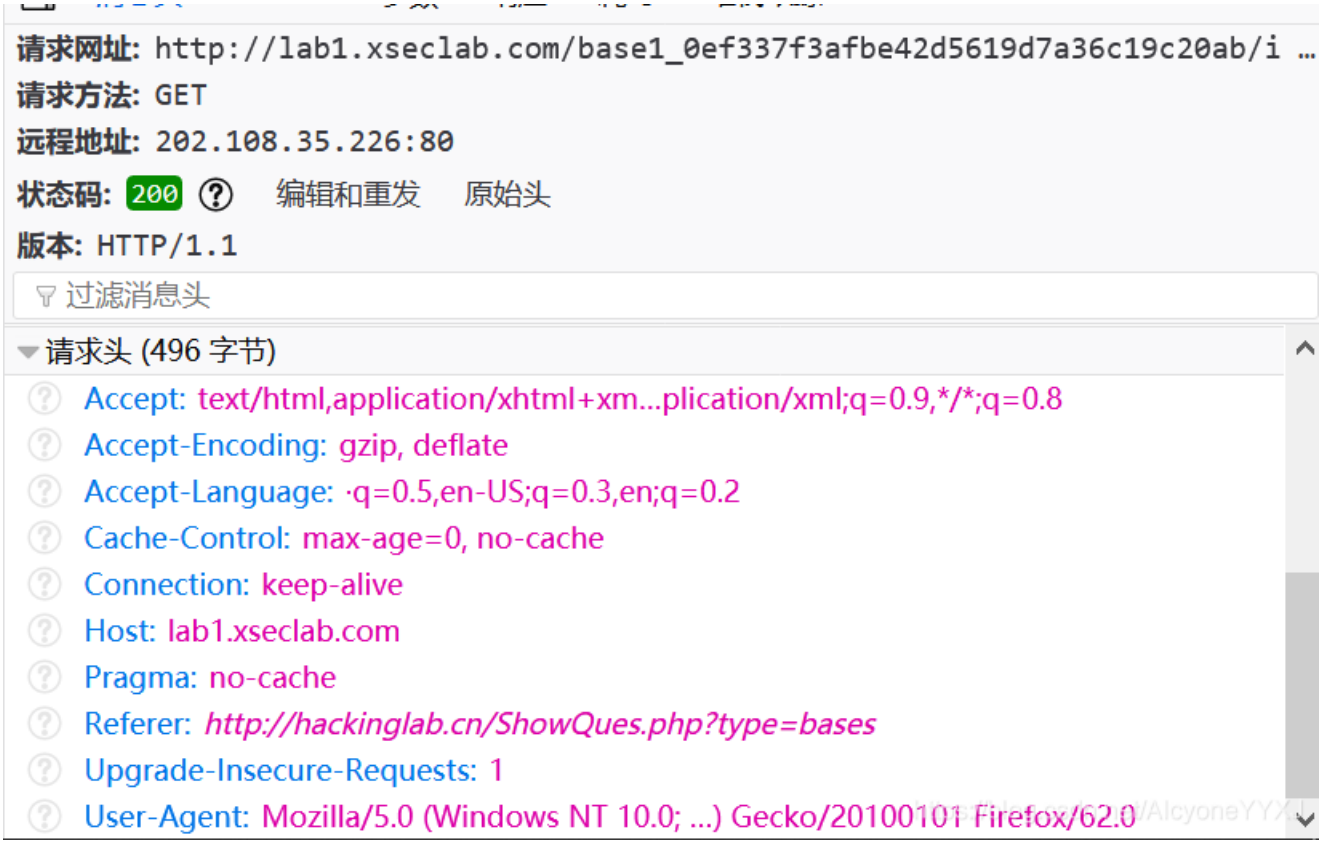
分值: 300

小明同学今天访问了一个网站，竟然不允许中国人访问！太坑了，于是小明同学决心一定要进去一探究竟！

http://lab1.xseclab.com/base1_0ef337f3afbe42d5619d7a36c19c20ab/index.php



把这里的中文都去掉



得到的响应也就变了

第六题 HAHA浏览器

HAHA浏览器

分值: 200

据说信息安全小组最近出了一款新的浏览器，叫HAHA浏览器，有些题目必须通过HAHA浏览器才能答对。小明同学坚决不要装HAHA浏览器，怕有后门，但是如何才能过这个需要安装HAHA浏览器才能过的题目呢?

通关地址

http://lab1.xseclab.com/base6_6082c908819e105c378eb93b6631c4d3/index.php

修改这个这HAHA

得到

预览

恭喜您，成功安装HAHA浏览器！key is: meiyouHAHAliulanqi

响应载荷（payload）

```
<html>
   <head>
        <meta http-equiv="content-type" content="text/html;charset=utf-8">
    </head>
    <body>
      恭喜您，成功安装HAHA浏览器！key is: meiyouHAHAliulanqi
```


第七题 Key究竟在哪里呢？

key究竟在哪里呢?

分值: 200

上一次小明同学轻松找到了key，感觉这么简单的题目多无聊，于是有了找key的加强版，那么key这次会藏在哪里呢?

通关地址

http://lab1.xseclab.com/base7_eb68bd2f0d762faf70c89799b3c1cc52/index.php

第八题 Key又找不到了

key又找不到了

分值: 350

小明这次可真找不到key去哪里了，你能帮他找到key吗?

通关地址

http://lab1.xseclab.com/base8_0abd63aa54bef0464289d6a42465f354/index.php

此处怀疑藏了一个网页但是很快跳转了

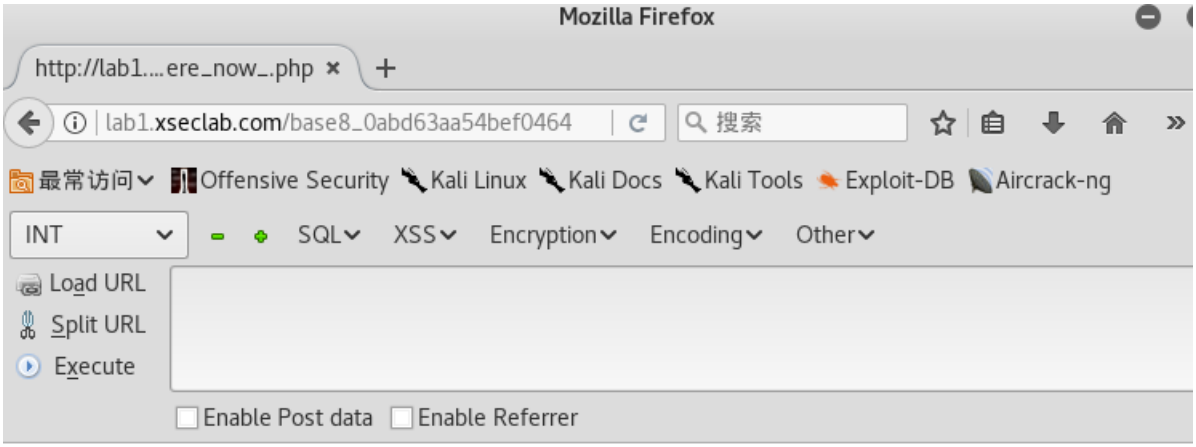
拦截之后发给repeater,点Go一步一步来

```
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://lab1.xseclab.com/base8_0abd63aa54bef0464289d6a42465f354/index.php
Connection: close
Upgrade-Insecure-Requests: 1
```

```
Server: nginx
Date: Tue, 23 Oct 2018 02:52:06 GMT
Content-Type: text/html
Connection: close
Location:
http://hacklist.sinaapp.com/base8_0abd63aa54bef0464289d6a42465f354/index_
no_key.php
Via: 1524
Content-Length: 224

<html>
  <head>
    <meta http-equiv="content-type" content="text/html;charset=utf-8">
  </head>
  <body>
    <a href="./key_is_here_now_.php">___</a><!--都告诉了到这里找key的啦-->
  </body>
</html>
```


跳转到这个php页面



key: ohHTTP302dd

第九题 冒充登陆用户

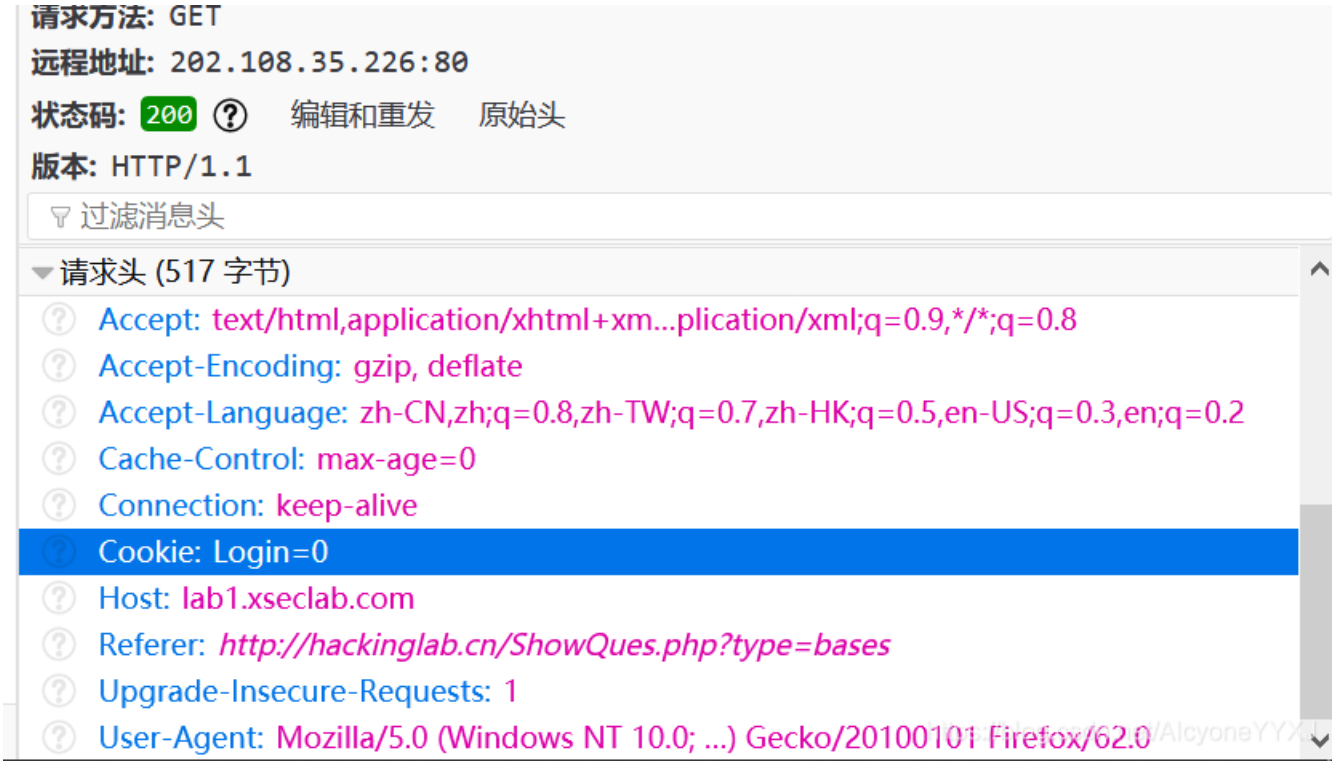
冒充登陆用户

分值: 200

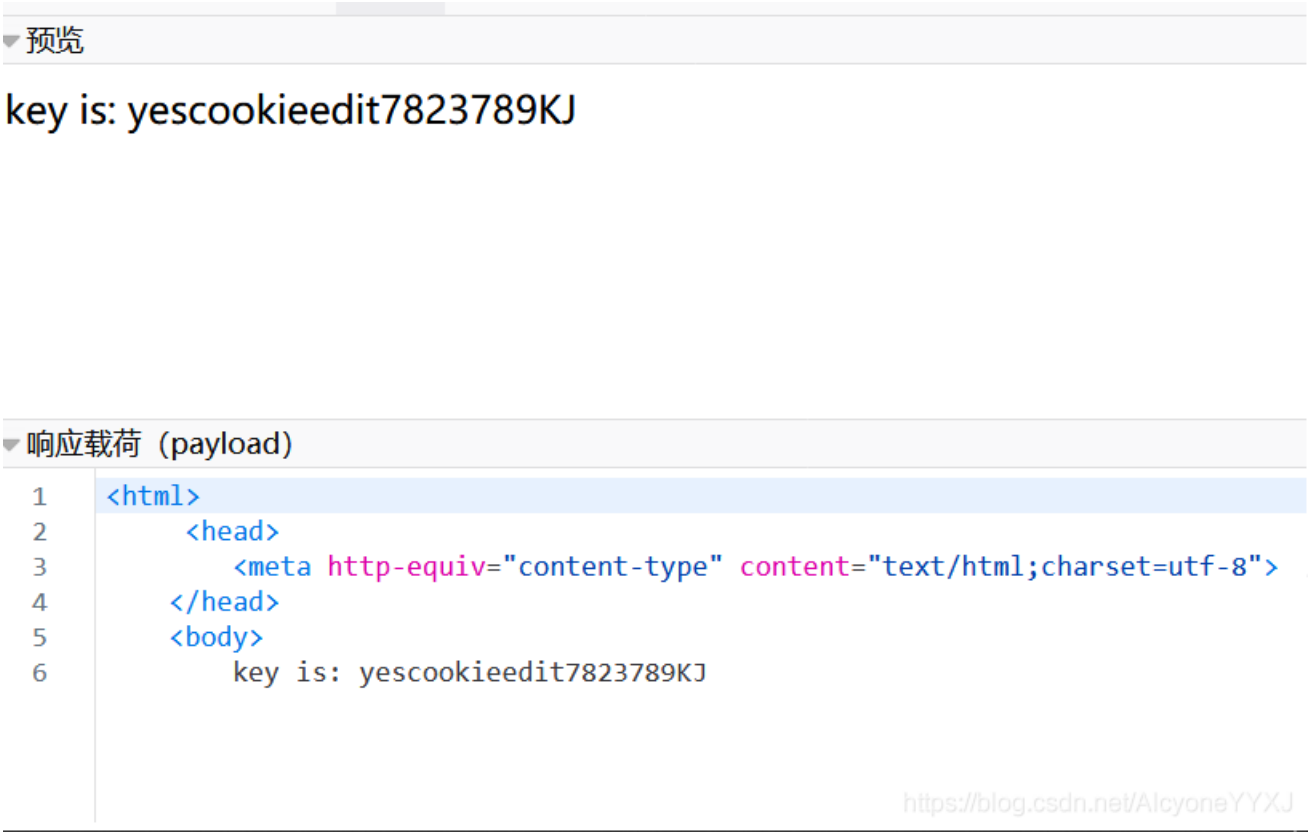
小明来到一个网站，还是想要key，但是却怎么逗登陆不了，你能帮他登陆吗?

通关地址

http://lab1.xseclab.com/base9_ab629d778e3a29540dfd60f2e548a5eb/index.php



看到这个就想估计改成1就行了



第十题 比较数字大小

比较数字大小

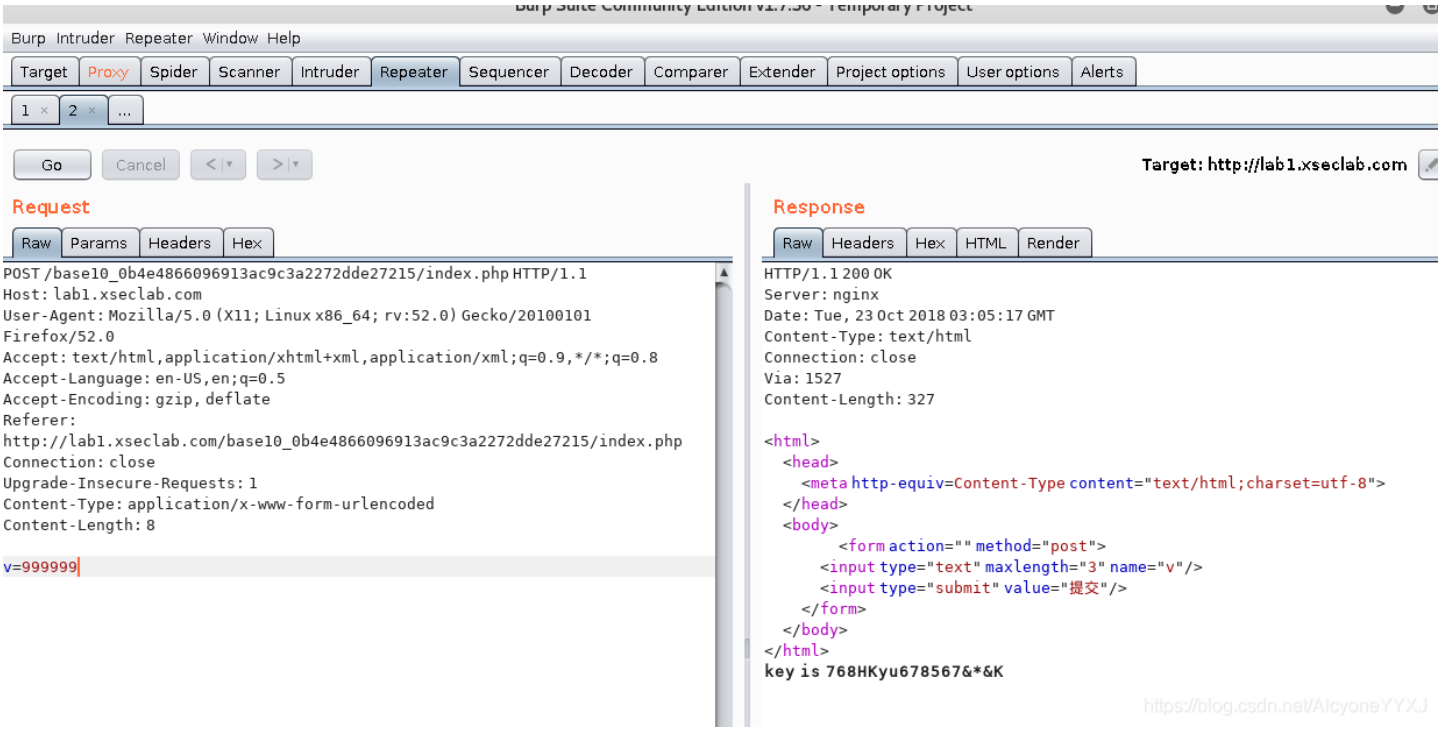
分值: 100

只要比服务器上的数字大就可以了!

通关地址

http://lab1.xseclab.com/base10_0b4e4866096913ac9c3a2272dde27215/index.php

发现对输入字符有长度限制，所以拦截后修改



另一个思路，直接修改前端的限制

提交后出现flag

第十一题 本地的诱惑

本地的诱惑

分值: 200

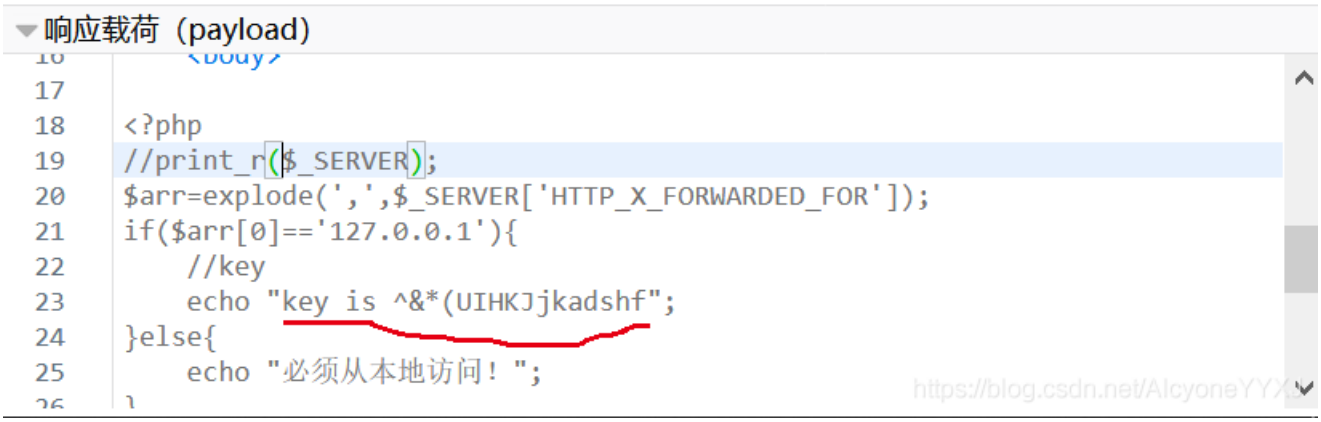
小明扫描了他心爱的小红的电脑，发现开放了一个80端口，但是当小明去访问的时候却发现只允许从本地访问，可他心爱的小红不敢让这个诡异的小明触碰她的电脑，可小明真的想知道小红电脑的80端口到底隐藏着什么秘密(key)?

通关地址

http://lab1.xseclab.com/base11_0f8e35973f552d69a02047694c27a8c9/index.php

查看源代码

必须从本地访问!



第十二题 就不让你访问

就不让你访问

分值: 150

小明设计了一个网站，因为总是遭受黑客攻击后台，所以这次他把后台放到了一个无论是什么人都找不到的地方....可最后还是被黑客找到了，并被放置了一个黑页，写到:find you ,no more than 3 secs!

通关地址

http://lab1.xseclab.com/base12_44f0d8a96eed21afdc4823a0bf1a316b/index.php

看提示是robots.txt

然后直接访问这个文件http://lab1.xseclab.com/base12_44f0d8a96eed21afdc4823a0bf1a316b/robots.txt

```
User-agent: *
Disallow: /
Crawl-delay: 120
Disallow: /9fb97531fe95594603aff7e794ab2f5f/
Sitemap: http://www.hackinglab.sinaapp.com/sitemap.xml
```


那就再访问这个文件夹

http://lab1.xseclab.com/base12_44f0d8a96eed21afdc4823a0bf1a316b/9fb97531fe95594603aff7e794ab2f5f/

得到

---

you find me,but I am not the login page. keep search.

那就访问login.php

http://lab1.xseclab.com/base12_44f0d8a96eed21afdc4823a0bf1a316b/9fb97531fe95594603aff7e794ab2f5f/login.php

right! key is UIJ%%IOOqweqwsdf