

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](#)

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/AlcyoneYYXJ/article/details/83540287>

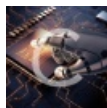
版权



[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

160 毫秒

消息头 Cookie 参数 响应 耗时 堆栈跟踪

▼ 预览

key就在这里中, 你能找到他吗?

▼ 响应载荷 (payload)

```
1 <html>
2   <head>
3     <meta http-equiv="content-type" content="text/html; charset=utf-8">
4   </head>
5   <body>
6     key就在这里中, 你能找到他吗?
7     <!--key is jflsjklejflkdsjfklds-->
8   </body>
```

<https://blog.csdn.net/AlcyoneYYXJ>

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`

<https://blog.csdn.net/AlcyoneYYXJ>

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):

密文框:

```
vwpxzjz3bjdaawbwa j  
cwqak23ckvbxcxvk  
dxrbl23dlwcydywl  
eyscm23emxdzezxm  
fztdn23fnyeafayn  
gaueo23gozfbgbzo  
hbvfp23hpagchcap  
icwgq23iqbhdi dbq  
jdxhr23jrciejecr  
keyis23ksdjfkfds  
lfzjt23ltekglget  
mgaku23muflhmfu  
nhblv23nvgminigv  
oicmw23owhnjojhw  
pjdnx23pxiokpkix  
qkeoy23qyjplqljy  
rlfpz23rzkqmrnkz
```

<https://blog.csdn.net/AlcyoneYYXJ>

第三题 猜猜这是经过了多少次加密

加密后的字符串为:

```
Vm0wd2QyUX1VVGxwV0d4V1YwZDRWMV13WkRSV01WbDNXa1JTVjAxV2JET1hhMUpUVmpBeFYySkVUbGhoTVVwVvZtcEJ1R115U2tWVWJHaG9UV1Z3  
V1ZacVFtR1RNbEpJVm10a1dHskdjRT1aVjNSR1pVwMfKR05GU214U2JHdzFWVEowVjFawFNraGhSemxwVmpOT0xcFZXbUZrUjA1R1drWndWMDFF  
U1RGV1ZFb3dWakZhV0Z0cmFHaFN1bXhXVm1wt1QwMHhjR1pYY1hSWFRwaENSbFpYUZOVWJVWTVJbFJDVjAxdVVuW1Zha1pYwKVaT2NscEdhR2xT  
TW1ob1Yxw1NTMk14U2tkWGJHU11ZbFZhY1ZadGRHRk5SbFowW1VaT1ZXSlZXVEpWykZKSfZqRmFSbU16WkZkaGExcG9WakJhVDJ0dFJraGhSazVz  
WwXob1dGwRnRNGRVTvZGM1RVaG9hbEpzY0ZsWmJGwMhZMnhXY1ZGVVJStk5XRUpIVmpKNFQxW1hTa2RqUm14aFUwaENTR1pxUm1GU2JVbDZXa1pr  
YUdFeGNH0Vdha0poVkrKT2RGSnJhR2hTYXpwe1dXeg9iMWRHV25ST1dHU1ZUV1pHTTFSVmFH0WhiRXB6WTBac1dtSkdXbWhaTVZwaFpFZFNTkpy  
T1Z0aVJt0TNWmnhXYjJFeFdYZE5WV1pUwVVRGd1YxbHJXa3RUUmXweFVtMUDVMkpWykRawGExcHJZVWRGZUD0SE9WZGhhMHBvVmtSS1QyUkdTbkpo  
UjJoVF1YcFd1bGRYzUc5aU1XUkhWMjVTVGx0SFVuT1Zha0p6VgtaVmVXUkhkRmhTTUhcSlZsZDRjMWR0U2tkWGJXaGFUVzVvV0ZsN1JsZGpiSEJI  
V2tkc1UySnJTBuZXTW5oWfdWw1J1RmRzYUZSavJuQ1pwbXRXZDFZeGJIS1hhM1JVVW14d2VGvX1kR0ZpUmxwe1YyeHdXR0V4Y0hKw1ZXUKdaVWRP  
UjJKR2FHaE5WbkJ2Vm10U1MxUnRwa2RqU1d4V11sZG9WR1JYt1c5V1ZscEhXVE5vYVUxWfVucFdNV2h2VjBkS1dWvNjPV1poYTFwSVZHeGFZVmRG  
T1ZaUFYyaHBVbGhCZDFac1pEUmpNV1IwVTJ0b2FGSnNTbGhV1ZwM1ZrWmFjVk5yWkZ0aVJrcDZwa2N4YzFVeVNuS1RiVpYVFc1b1dGZFdxBeps  
Um1Se11VW1NhVkp1UwXwV2JYU1haREZaZuKdSVNSaGhNMUpVV1cxNGQyVkdWbGR0Unpsb1RWwNd1bF15Y0Vkv01ERjFZVWhLV2xaWfVrZGFWM2hI  
WTTXc1TvbKdkB1JTV1hCS17+MTBVMU14V1h0wEdHsE17hYkhVfEcc1nH0VdSbYkaltBaa27HCSkhVbGykv1dMMV1UWYhYp17xYU7L7TmEcl1Vh300
```

wl1x511yRkUuR1J1V1hC51ZcM1bVn014v1h0wFdnaf1Z0X1mVJfSc1pnoV050X1aw1baaz0nK1v00X1v1u0nV1wV1hK1Zy1oZk1mRfSw1VwazQ0
YTFOR1ZuT1h1r1pYwWtoQ1NwWkdVa2RWTVZwMFVtdG9VR115YUhcVmJHaERUBXhrV1ZGdFJtcE5WUMU13V1RKMGIYrKdTBk5UYkdoV1ZSwndNMVpy
V21Ga1ZrNX1Xa1pPYVZKcmNEW1dhMk40WxpGVmVWtNtVbFJpV1ZwVZGYzFiMWRHwKzKwGJfCHNVbTFZwXsV1dsTmhWa3AxVVd4d1YyS11VbGhh
UkVaYvPVZEtTVk5zYUdoTk1VcFZwBGN4TkdeVzRzFdxR3hyVpOU2IxhHNWbMRXTVZwMFkwZedXR0pHY0Zowk1HUnZwMhhV0ZwclpHR1dWmUpR
V1RCVksWwXhJRWhoUjJot1UwVktNbFp0TVRCVK1VMTRWVmhzVm1FeVvsw1piWfIzWVvA2VRHVkZkR3BTYkhCNFZrY3d0V114V250a1JXaFlWa1Ux
ZGxsV1ZYaFhSbFoxWTBaa1RswX1hRepXTVZwafV6Rkp1R1J1VmxKaVJscF1WR1JHUZA1c1drZFzhM1JXVFZad01GVnRkRz1WUmXwMf1Vw1NWV1pY
YUVSVk1uaGhZekZ3U1ZwDGNFNVDNVWwzVmxSS01HRXhARWhUYkdob1VqQmFwbFp1Y0Zka2JGbDNWmjVLYkZkDFvubGFSV1IzWVZaYwNtTKZiRmRp
UjFFd1ZrUktSMV14VGxsa1JuQk9UVzFvV1ZkV1VrZgtNa1pIVjJ4V1UySkdjSE5WY1RGVFRWw1Z1V042UmXoU2EzQmFwVwMxYjFZeFdYcGhTRXBW
wVRKU1NGVnFsbUZyV5CSV1VWk9WMPHV2xaV2JHTJRUA2RSZVZac1pGZG1SMUp2V1c1d2MySXhVbGRYYm1Sc11rWnNOVmt3Vm10V01ERKZVbXBH
V2xaWGFfEdNbmhoVjBaV2NsceHsbGROTW1oS1YxUkp1Rk14U1hoalJXUmhVbFJXVDFwc2FFT1RNVnAwVfZSQ1ZrMVZNVFJXYkdod1YwWmtTR0ZH
YkZwaVdHaG9wbTE0YzJ0c2NFaFBWm0JUWwtoQ05GwnJZM2RPVmxsNFYyNVNwBUpIYUzoV2FRnu9UV1phV0dNemFGaFniRnA1V1ZwYwEXunRSbk5Y
YkZaWf1US1JNRmRXV2t0ak1WSjFWRzFvVTJKR2NGbFhWm2hoVw0xUmVGZHVsbEppV1ZwaFZtMhhVMU5XV2xoa1J6bG9UV1Z3TUZsV1dsT1dwbHBZ
wVwU1ZrMXVhR2haZwtam1Vsw1dkR05GT1ZkT1ZXd3pwbXhTuzAxSFNYbFnhM1JvWw1zMVZwbHJaRz1XYkZwMfPaGtUazFXyKROV01qVxZa1pL
ZEZwdwJHR1NWU16V1ZaYV1XTnRUA1ppUm1ScFvQrKzKMWXVt001WbDRWRzVXVm1KR1NsaFZiRkpYVjFaYVixbDZsbwX0VjFKSVdXdG9SMVpI
U1hoalNFNVdZbFJHvkZzewVhdGpiRnBwW14a1RswNvRa1pYvKvKaFZqRmtSMWRZY0ZaaWzQ1lwbXRXWdwc1duR1NiR1JxVfZkU2VsbFZaSE5X
TVZwMVVXeEdwMkV4Y0dowFzTU1NaV1phY2xwR1pGaFNNMmg1VmxkMFYxTXhARWRWYkdSwV1tMVnjMvp0TVRCTk1WbDVubGQwV0ZKcmJET1diWEJU
VjJzeF1xTnRbGROYwtaSFdsWmFwmk5zY0VoU2JHUk9UVzFvU2xZeFvrcGxSazE0VTfob2FsS1hhSEJWY1RGd1ZrWmFjMkZGVGxST1ZuQXdwR1pT
UTFack1WwK5WRkpyWwtkb2RswXdxBRUujBaSF1rWndhVmRIYuc5V2JYQkhZekp0ZUd0RmFGQ1diVkpV1d4b2IxbFdar1ZSY1Vab1RXdHdTV1V5
ZEc5V2JvcE1aVWRvVjJKSFVrOVVwbHB6VmpGYvdXRkdHrk5pUm5BMVYxW1dZV0V4VW5SU2JrNV1Za1phV0zSVVNsSk5SbFkyVW10MGfRmV1Ra3BX
Y1hoVf1WwktjMk5HYkZoV00xSm9Xa1JCTVdNeFpISmhSM2hUVFvad2FGwnRNSGhWTVVsNFZXNU9XR0pW2xkVmJYaHpUbFpzVm1GR1RsZG1WWEJK
V1ZwV1QxbFdTa1pYY1doYVpXdGFNMVZzV2xka1IwNUdUbFprVGxawGQzcfDiWghUVXpBeFNGT1liRk5oTwxKV1dXMXpNV1pXykhKYVJ6bFhZa1p3
ZwxZeU5XdFVhekZYWTBoc1YwMXFSa2haVjNoafkyMU9SVkZ0UmX0V01VWxpwbTF3UzFneVRuT1Via3BxVw0xb2NGVnR1SGRsVm1SW1kwmVtWmKpX
V2xoV1J6V1BZV1pLZfZGck9WV1d1a1oyVmpGYwExWxhwbkphUjNST11URndTV1pxU2pSv01WVjVVMnRrYwXORk5WZFPiRkpIVmtaU1YxZHNXbXhX
TURReVZXMRhMVjzV25UmFscF1Wa1ZLYUZacVJtdFNnv1IxVkd4U2FfMXRhRz1XVjNSWfDwZE9jMvp1UmXsaE0xS1ZwBTE0UzAxR2JGw1hhemxY
VFZad1NGWx1jRXXRWtwSVZHCfnwV05VwX0YVZscGhZMnh3UjFwr2FGTk5NbWcxVm14a2QxUXhWwGxUV0docFUwVTFXRmx0TVZOWFJss1hwmjVr
VGxKdGREt1hhMvpyVjBaSmQyTkZhrnBOUm5CM1ZqSnp1Rk5HVm5WwGJHUK9ZbTFvYjFacVFtR1dNazV6WTBwb1UySkhVbGhVVMxaM1ZXeGFjMVZy
VG1oT1ZXdzBwVEZvYzFVeVJYbGhTRUpXWwXoTmVga3DXbk5XVmtaMvdRVTfVhVkp1UVhkv1JscFRVVEZHy2sxV1drNVdSa3BZVm01d1YxwkdXbkZU
YTFwc1ZteGFNV1Z0ZudGaFZrBDRVbGhrVjJKVJUQ1p1a3BPw1Vkt1JtRkdrBGRpVmtwV1YxZDBWm1F4WkhOWGEyaHNvAk5DVUZadGVITk9SbGw1
VGxaT1YyS1ZjRwXaV1Zwd1ZqSkdjazVWT1ZwV2J1Qm9WakJrVG1WdFJRzGhSazVwVw01Qk1sWxhXbGRaVjBWNfZXNU9XRmRIZUC5VmExwJNwMfP
VjFkdVpHaFniRmt5V1cxME1HRnJNVmRUyWtaWFZqTm9VRmxXV2twbFJRntFXa1prYudFd2NGaFdSbFpXW1VaSmVGcE1TbwhTTTFKVZGVMfKmlJz
V2tkYVNIQk9WakZhZwZeGFIT1VNVnB5VGxjNVZwWnNXak5VV1ZwaFYwVTFwBfJzWkU1aE0wSkTwmVpXVjFVeFdsafRiR3hVwVpKb1dGbHJXbmRW
Umxwe1YydbBhazFXy0hsVWJGChJZVMRGZDFkwwNGZG1XR2h4V2tSQmVGWxhVbGxUm1ob1RXXMw9WbGRYZEd0aU1rbDRwbTVHwV1KV1dsafpMXAz
VfVad1ZtRkKhR1ZoZwtayVZWZDRjMwxXV2xoaFJYaGFZVEZ3WVZwV1dtdGpiVTVIWVvkb1RsZEZTbEpXY1RGM1V6RktkRlpyYUZwaE1WcF1XV3Rr
VTFaR1ZuT1h1bVjzVm0xU1dsa3dWbXRXTWtwWfVtcE9WV1pzV25wW1ZscEtaVmRHUjFwc2NHbFNnBwd5Vm1wR11XRhARWhXYTJoUVZtdHdUMVpz
VwtaT1JtU1ZVvzFHV2xac2JEU1hhMvp2WwVaS2MxTnNXbGRpVkvAvVZtdGfKMWRIVmtsvWJHUNBVakZLTmxac1kzaG1NVmw1VwXod1VsZEhhRmhX
Y1RGU1RVWndSVkPzY0d4V2F6VjZXV3RhwVdGV1NYbGhSemxYVmpOU1dGZfdaRT1qTVZwMVVteFNhRTB4U2xaV2JURjZUV1V4UjFadVVteFNWR3h3
V1dwQ2QxZHNiR1pWYku1WFRVUkdXV1pXYud0WfJscDBWV3hPVWZac2NHaFpNbgzVwPgd1IyRkdUazVOY1dJefZtMTRhm1F4U1hoavJtaFZZVEpT
V0ZsdGVfdGpNV1YzV2taT2FrMVh1SGxXTWpWUFZERmfKvKzZwKzWv1YxRjNwKJhUzJodFnrV1ViR1JwVjBWS1ZwWnFTbnBsUmtsNFZHNU9VbUpI
Vws5W1YzUmhVMfprYzFkdFJsZE5he1Y2V1RCV2IxVX1Ta2hWYXpsV1ZucEdkbFV5ZUZwbFJswN1ZMGQ0VTJGN1JUQ1dWRVp2WwPKR2MxTnNhR1pp
VjJofFdXdGfTMwRHV2twU2JHUnFUV3RHUjFaSGVGT1ViRnAxVvZoa1YxSnNjR1JwVkvAafkyc3hWmWRyT1ZkU2EzQ1pWmWQwYTJJeVvU1hXR1JZ
WwXoU1ZwVnFRBUZUVm14V1YyMUdW0pGY0RGV1Z6QTFWakpLV1ZKVVfscGxhM0JRv1hwr2Qxt1dub1JrUms1T1RVVndWbF14WkRcaU1VjJNUbFZr
V0dKcmNHR1VWRXBuV1VaYWRHvk1Uaz1Tykd3MVZHeFZOv0ZIU2taa1JteGFwbFp3ZwXacVnRwmxSbHbaWVvkr1UwMH1hRfpxY1hCSfdWwmtXRkpy
WkdoU2F6VndwVzAxUwsxc1dYaFhiR1JhVmpCV05Gw1hOVT1YUm1SSVpVYzVwBuv4V2p0V01GcFRWakZrZFZwSGFGTm1SbXQ1VmxjeE1FMUhsbkp0
Vm1SVV1XdGfXR1pxVg05U1JscHhVMnQwVTAxck5VaFpMxB2VmpBd2VGTnFTbGRXyKvWsvZsUkdXbvZIVGtaaVJswNBvakpvZDFadGVHRmtNV1J1
VjJ0a1dHS1ZXbkZV1ZKfUwW1p1R0ZJVGxWT1ZuQjVwR3hqT1ZaV1duT1h1bKjWwWtad2VswNRNVWRtYkZKe1drZHNwMWRGU2t0V01WcFhwakZw
ZUZkwpPfnVdiVkp4V1dws2IxbFdvbGRYYm1SV1VtMTBOR115Zud0aGf6R11WVzVzV1dKR2NIS1dSM2hoVjBkUmVtTKdar2XYUjJoV1ZsaHdRbVZ
VGtkVWJHeHBVbXmXyJfSWGVfdFdiR1JZVFZod1RswNjRmhaYTJoTFdWwkt0bUpHYUZwaE1YQXpXbGQ0V21Wk5WaGtSbFpVw1d0YVdsZHNwBUzo
TVZsM1RwaEdwMkpyY0Zov2ExWjNWRVpWUZKc1pHcG1WVnBJVjJ0YVQxUnJNWFJoUmXwWf1SukdNMVY2Ums1bFZsSjFWR3hXYVdFe1FuW1dWekI0
V1RGYVixVnWbFJpVkd4d1ZGwMfKmlZXV2xoa1JFS1dUVVJHV1ZawGRHOVdhekYwVvVod1dGwnNjRXRhVjNoSF16R1dJmXBiyUdobGjGbdVwBTF3
UjFswfJYaGFSV2hYwVRkb1VwWnRkSGRVTZwMfPaGtWR1p0WxaV1Z6RkhZV1V4Y2xkVfS1ZG1WR1pNVmpCa1MxTkhwa2RhUm5CcFVqSm9WV1pH
Vwtkao1WbDRXa2hTYTFJe1FuQ1Zha1pLWkRGYVJWSnRkR2x0Vm13e1ZGw1dhMkZGTUhsbFJtaGfZa1pLUTFwV1duTmPwa3B6WtBkNFUyS1dTa1ZX

YwtvMFZUSkdXRk5yYkZKaVIyaF1XV3hVTFkR1pGZGF5bVJxVFZkU01WVnR1RTloVmtsNFUyNw9WMUpzY0hKV1ZFcFhZekPLUjFkdFJSU1NWR1oy
Vm0weE5HUX1WbGRoTTJsv1lsVmFXR1JwVWtkwFZscFhZVWQwV0ZKc2NEQ1dWM2hQV1ZaYwMyTkhhRnBOYm1ne1ZXcEdkMU15UmtkVWF6V6k9ZbGRq
ZUZadE1UUmhNREZIVjFob1ZWZEhhR2hwYkdSVFZqRnNjbHBHVgXoV2JY3dWR1phVDJGck1WZGpSRUpoVmxkb1VGWkVsbUzrVmtaelDrWndWMV14
Ump0V2FrSmhVMjFSZVZScldtaFNia0pQV1cwmVEwMXNXbkZUYm5Cc1VtczFTV1Z0ZEdGaVJrcDBWV3M1V21KVVJUw1pha1poWTFaR2RGsNnaRtVo
ZwxZM1YxUkNwMk14V1hsVGEyaFdZa2RvVmxadGVHRk5NvNBZw1Vkr2FRmVdXbmxXUjNoc11VZFdjMwRzYkZkaGExcDJXV3BLUjJNeFRuTmhSMmhU
W1cxNFdGZFdaREJrTwXkelYydfVMkphY0hKVZscdNaV1p3UmxavVJtaFdhM0F4V1Zab2ExZehTa2RYYmtaV11rZFNsMxBFUvhoV01XUn1UbFpr
VTJFe1FscFdiVEIzW1VksmVWVnVubGhYUjFKWldXeg9VMvpXVm5GUmJVW1VZa1phTUzWV1pFZGhSbHB5WwtSU1ZtSkhhSEpXYWtwTFZsWktWVkJz
Y0d4aE0wS1FwMnhXWvdFeVVsZfdiazVwWwXkNFZGU1dwbmRXYkZsNFdrUkNwMDFzUmpSWGEyaFBWmGRGZVdGsvRsmwhhe1ZFVmxwYV1XUKZNVmRV
YkZKVF1rZDNV1pIZUZaT1YwWk1VMnRhYwXKR1NtaFdiR1JUVTBaYwMxZHRsbGROYXpwsVYydgFwMv15U2tsUmFscFhZbGhDU0ZkV1dtdFhSa3B5
WVvd1UwMXVhRmxXYWtKwFV6Rk9SMWR1Vw14U00xS1FwV3BDVjA1R1dsae9WazVXVfd0d2VWUnNXbk5Y1VWNFKwZG9WMDFXy0doYVjVjRwWakZP
Y2s1V1RtbFNiWfExVm14amQyVkdTWGxTYmxKVF1XehdXRmxyWkc5W1ZteFZVbTVrV1ZKdGVGaFDbN1F3WVdzeGNrNVZhrnBoTVhCM1ZtcEjKMLZH
VG5SUFZtaG9UV1Z3U1ZkV1VrZfhiV1pIWTBwc1ZHS1hhR1JVvKvaTFzSWMFSMvp0Um10T1YxS11WakowYTFsV1RrbFJiazVXWwtaS1dGWXdxBUzr
U1RWwFZHMW9UbFpYt0hswFYzUmhZVEZhzEZ0c2JHaFRTRUpXV1d0YwQyVnNXb1JOV1dSVF1rWkt1bGRyWkhOV01XUkdVMnQwVjAxV2NGaFdhA1pX
W1Vaa1dWcEZOVmRpVmtwNFZsZhdTMk14YkZkVmjHU11ZbTFTVjFwde1UQk9SbGw1W1VkmGFHRjZSbGxXVnpwe1ZsZetSMk5JU2xkU00yaG9WakJr
Vw1WdFRrZGFSMnhZVWpKb1ZswNnhSGRSY1ZaSFZhdGtWR0pIZUc5VmFrSmhwa1phY1Z0dE9WZG1SMUpaV2tWa01HR1ZNWepUkZKwF1sU1dWR1pI
ZUdGT2JvcElVbXhrYVZkSFozcFhiRnBoV1ZkU1JrMvDxBUZTYkZwd1dsZDBZVmRzWkhOV2JVWm9Uv1pzTTFsv2FFZfNa3B5WTBab1YyRXhXak5X
U1ZwV1pVWmtjbHBIY0dsV1ZuQkpWakowVZReFVuSk5XRkpvVw14d1dGbHNva2ROTVZZM1VtczFiR1pzU2pGV1IzaFhZVmRGZwGdWFGZFd1a0kw
V1dwS1QxSxhXb1ZwY1hoVvVqRktkMvPHV210V1XUkhWmnhvYTFKR1NsZFVWkpIvJbac2NsVnNUbGROV1d3M1dWw9kMWRzV1hwaFJYaGhVbXh3
U0ZreWn6V1dNvNB6V2tkNGFFMvHPVfZXY1RGM1VqRnNwMkPHWkZSWFIyaHdWV3RhZDFaR2JITmFSRkpWVFZad2VGvnrkREJXUmxwe1kwaG9WazFX
U2toV1ZFRjRwWakZhY1Zac1drNw1iRXB2VjFaa05GUXhTbkpPvm1SaFvtNUNjR1Z0ZEhkVFZscDBaRWRHV0dKV1dsbFdiWfJ2WVRGSmVsRnVRbFpp
VkJaRVZtcEdZVmRGTvZwVmjXeE9WbXhaTVZawGVH0wtNVlowVTJ4YvdHskhhRmhaYkZKSfZUR1NwBGR1VGs5aVJYQxdXa1ZhVDFSc1dYaFRXR2hY
WwtkUk1GZFdaRWUms1eV1rWkthV14U2xsWfYzaFRvbxN4UjJor1ZsUm1SMUp4VkJaa1UwMvdWb1JsU1Rsb1ZtdHNOR1V5T1c5V01VcHpZMGhL
VjFaRmNGaFp1a3BMVWpGa2RGsnVbE5XUmxveZtMhd1RTVIvVhsV2JHUm9UVEpTV1ZsdE1WT1hSbEpZwKvOa1ZGwnNjRWxaTUzWUFZqR1pkMvpx
VmxkV00yaFFWmVphWdNeVRraGhSbkJPwW0xbmVsw1hjRWRrTVU1SVUydg9hVkpYt1ZsVmJGwjNWVEZhZEUxSVpHeFNWR1pKv1d4b2IwxhARwho
UjJoV11rZFNWR1pxUm50amJHUjFXa1prVGxZemFGZfdWRW8wVkrR2NRmVdaR3BTU1Vwb1ZteGfXbVf4YkhKvYJYU1RUV3MxUmXwWwGVZfdNvNB5
WTBac1YyS11Ra05hV1ZwTFZqRk9kV1J0UmX0aWewcDNwMwN4TUzNeFVsZFhibEpPVTBkb1ZwU1daRk5YUmXwMFRswmtXRk13Y0VsV1Z6QTFWmhh
UmXkVRscGhhMXbVmpCvmVGWldWb1JoU1Rwb1pXefDNMvp0TuhoT1IwVjRZa1prVkJkSGVHOVZibk16Vm14YWNsWnJkR1ZTYkhCw1dsVmtSMkZy
TVZoa1JGcGFwBfpwTVZaVvNrdFhWmfIwTBaa2FFMV1RakpYVjNCTFVqSk51R1J1VG1oU01taFZwV3hXZDFkR1pGaGxSemxwWwxaYVNGWx1kRmRW
TWtwV1YyNUdWV1p0VwXsYVYzaH1aREZ3U1ZwdGFGZGhNMEY0VmxayWIYRXhaRwhUYTJSWV1tdHdWmWxYZEdGaFJtdDVZek5vVjAxwFVqQ1phMXBQ
V1RKRmVsRnRPVmROVm5CVVZxcEtVbVZXVw5WVWJHaF1VakZLYjfaWGVHOVZNazVYwWtoT1YxWkZXBFJVMxwSFRrW1p1VTFVUW1oU2JiQXdWbGQw
YzFkSFJusK9WRTVYwVd0d1NGa311RT1rUjBaSFkwZDRhRTFZUwPwV2JYQkRXV1pWZVZsdVrtcfNwMmhV1d0Vk1XTkdXb1JrU0dSWF1rWnNORmRy
Wwt0WJGJbDRVbXBPV1dKR2NIS1dNR1JMwXpGT2NR0VdaR2hOVm5CT1ZqRmFZVmxYVWtoV2ExcGhVbFJzVkJzscmFFSmtNV1J6Vm0xR2FFMvdjRmxW
TW5SaF1XeEtXR1ZIUmxwV1JUvkvXbFphVjFJeFNsVm1Sa1pXVmtSQk5RPT0=

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

请将要加密或解密的内容复制到以下区域

key is jkljdkl232jkljdkl2389

<https://blog.csdn.net/AlcyoneYYXJ>

第四题 据说MD5加密很安全，真的是吗？

据说MD5加密很安全，真的是么？

分值: 200

e0960851294d7b2253978ba858e24633

<https://blog.csdn.net/AlcyoneYYXJ>

在线查询MD5

密文: e0960851294d7b2253978ba858e24633

类型: 自动 [帮助]

查询 加密

查询结果:

bighp

<https://blog.csdn.net/AlcyoneYYXJ>

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！

<https://blog.csdn.net/AlcyoneYYXJ>

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

The screenshot shows the network tab of a browser's developer tools. The selected request is for the URL `http://lab1.xseclab.com/base1_0ef337f3afbe42d5619d7a36c19c20ab/i ...`. The request method is GET, and the status code is 200. The 'Accept-Language' header is highlighted in yellow and contains the value `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`. Other headers include 'Via: 1566', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8', 'Accept-Encoding: gzip, deflate', 'Cache-Control: max-age=0', 'Connection: keep-alive', 'Host: lab1.xseclab.com', 'Referer: http://hackinglab.cn/ShowQues.php?type=bases', 'Upgrade-Insecure-Requests: 1', and 'User-Agent: Mozilla/5.0 (Windows NT 10.0; ...) Gecko/20100101 Firefox/62.0'.

消息头	Cookie	参数	响应	耗时	堆栈跟踪
请求网址: http://lab1.xseclab.com/base1_0ef337f3afbe42d5619d7a36c19c20ab/i ...					
请求方法: GET					
远程地址: 202.108.35.226:80					
状态码: 200 ⓘ 编辑和重发 原始头					
版本: HTTP/1.1					
⌵ 过滤消息头					
ⓘ Via: 1566					
▼ 请求头 (500 字节)					
ⓘ Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8					
ⓘ Accept-Encoding: gzip, deflate					
ⓘ 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					
ⓘ Cache-Control: max-age=0					
ⓘ Connection: keep-alive					
ⓘ Host: lab1.xseclab.com					
ⓘ Referer: http://hackinglab.cn/ShowQues.php?type=bases					
ⓘ Upgrade-Insecure-Requests: 1					
ⓘ User-Agent: Mozilla/5.0 (Windows NT 10.0; ...) Gecko/20100101 Firefox/62.0					

把这里的中文都去掉

请求网址: http://lab1.xseclab.com/base1_0ef337f3afbe42d5619d7a36c19c20ab/i ...
请求方法: GET
远程地址: 202.108.35.226:80
状态码: 200 ⓘ 编辑和重发 原始头
版本: HTTP/1.1

过滤消息头

请求头 (496 字节)

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
- Accept-Encoding: gzip, deflate
- Accept-Language: zh-CN;q=0.5,en-US;q=0.3,en;q=0.2
- Cache-Control: max-age=0, no-cache
- Connection: keep-alive
- Host: lab1.xseclab.com
- Pragma: no-cache
- Referer: http://hackinglab.cn/ShowQues.php?type=bases
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; ...) Gecko/20100101 Firefox/62.0

得到的响应也就变了

预览

key is: *(TU687jksf6&*

响应载荷 (payload)

```
1 <html>
2   <head>
3     <meta http-equiv="content-type" content="text/html; charset=utf-8">
4   </head>
5   <body>
6     key is: *(TU687jksf6&*
```

<https://blog.csdn.net/AlcyoneYYXJ>

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

<https://blog.csdn.net/AlcyoneYYXJ>

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

消息头 Cookie 参数 响应 耗时 堆栈跟踪

请求网址: http://lab1.xseclab.com/base6_6082c908819e105c378eb93b6631c4d3/i ...

请求方法: GET

远程地址: 202.108.35.226:80

状态码: 200 ⓘ 编辑和重发 原始头

版本: HTTP/1.1

过滤消息头

Via: 1529

请求头 (500 字节)

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
- Accept-Encoding: gzip, deflate
- 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
- Cache-Control: max-age=0
- Connection: keep-alive
- Host: lab1.xseclab.com
- Referer: http://hackinglab.cn/ShowQues.php?type=bases
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0

修改这个这HAHA

JS XHR 字体 图像 媒体 WS 其他 | 持续日志 禁用缓存 | 不节流 HAR

消息头 Cookie 参数 响应 耗时 堆栈跟踪

请求网址: http://lab1.xseclab.com/base6_6082c908819e105c378eb93b6631c4d3/i ...

请求方法: GET

远程地址: 202.108.35.226:80

状态码: 200 ⓘ 编辑和重发 原始头

版本: HTTP/1.1

过滤消息头

请求头 (522 字节)

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
- Accept-Encoding: gzip, deflate
- 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
- Cache-Control: max-age=0, no-cache
- Connection: keep-alive
- Host: lab1.xseclab.com
- Pragma: no-cache
- Referer: http://hackinglab.cn/ShowQues.php?type=bases
- Upgrade-Insecure-Requests: 1
- User-Agent: HAHA/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0

得到

▼ 预览

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

▼ 响应载荷 (payload)

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

<https://blog.csdn.net/AlcyoneYYXJ>

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这次会藏在哪儿呢?

通关地址

<https://blog.csdn.net/AlcyoneYYXJ>

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

消息头 Cookie 参数 响应 耗时 堆栈跟踪

请求网址: [http://lab1.xseclab.com/base7_eb68bd2f0d762faf70c89799b3c1cc52/i ...](http://lab1.xseclab.com/base7_eb68bd2f0d762faf70c89799b3c1cc52/i...)
请求方法: GET
远程地址: 202.108.35.226:80
状态码: 200 ⓘ 编辑和重发 原始头
版本: HTTP/1.1

过滤消息头

▼ 响应头 (203 字节)

- Connection: keep-alive
- Content-Encoding: gzip
- Content-Type: text/html
- Date: Tue, 23 Oct 2018 02:45:44 GMT
- Key: kjh%#\$%FDjjj**
- Server: nginx
- Transfer-Encoding: chunked
- Via: 1529

▼ 请求头 (500 字节)

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

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

<https://blog.csdn.net/AlcyoneYYXJ>

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

Go Cancel < > Follow redirection Target: <http://lab1.xseclab.com> ⓘ ?

Request

Raw Headers Hex

GET /base8_0abd63aa54bef0464289d6a42465f354/search_key.php HTTP/1.1

Response

Raw Headers Hex HTML Render

HTTP/1.1 302 Found

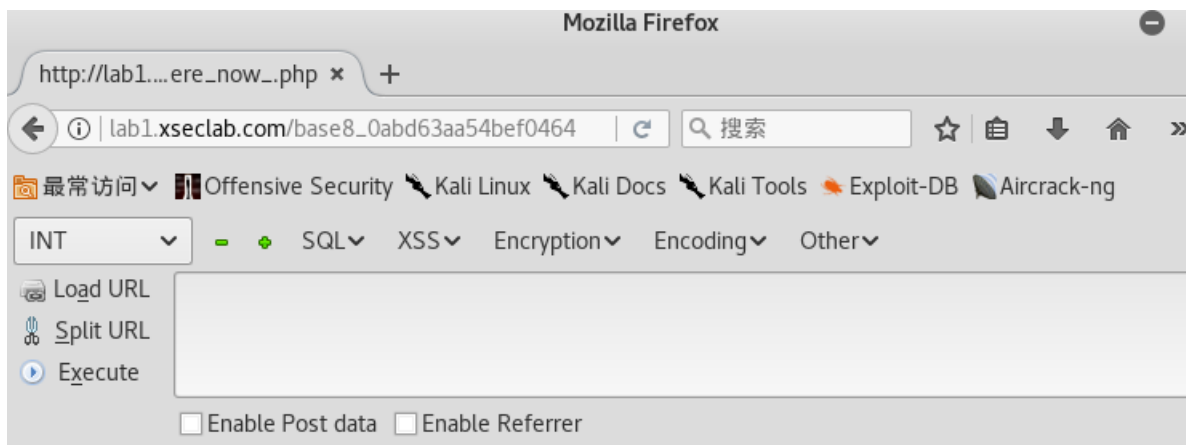
```
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://lab1.xseclab.com/base8_0abd63aa54bef0464289d6a42465f354/index.php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

<https://blog.csdn.net/AlcyoneYYXJ>

跳转到这个php页面



key: ohHTTP302dd

<https://blog.csdn.net/AlcyoneYYXJ>

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

<https://blog.csdn.net/AlcyoneYYXJ>

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



请求方法: GET

远程地址: 202.108.35.226:80

状态码: 200 ? 编辑和重发 原始头

版本: HTTP/1.1

过滤消息头

请求头 (517 字节)

? Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
? Accept-Encoding: gzip, deflate
? 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
? Cache-Control: max-age=0
? Connection: keep-alive
? Cookie: Login=0
? Host: lab1.xseclab.com
? Referer: http://hackinglab.cn/ShowQues.php?type=bases
? Upgrade-Insecure-Requests: 1
? User-Agent: Mozilla/5.0 (Windows NT 10.0; ...) Gecko/20100101 Firefox/62.0

看到这个就想估计改成1就行了

预览

key is: yescookieedit7823789KJ

响应载荷 (payload)

```
1 <html>
2   <head>
3     <meta http-equiv="content-type" content="text/html; charset=utf-8">
4   </head>
5   <body>
6     key is: yescookieedit7823789KJ
```

<https://blog.csdn.net/AlcyoneYYXJ>

第十题 比较数字大小

比较数字大小

分值: 100

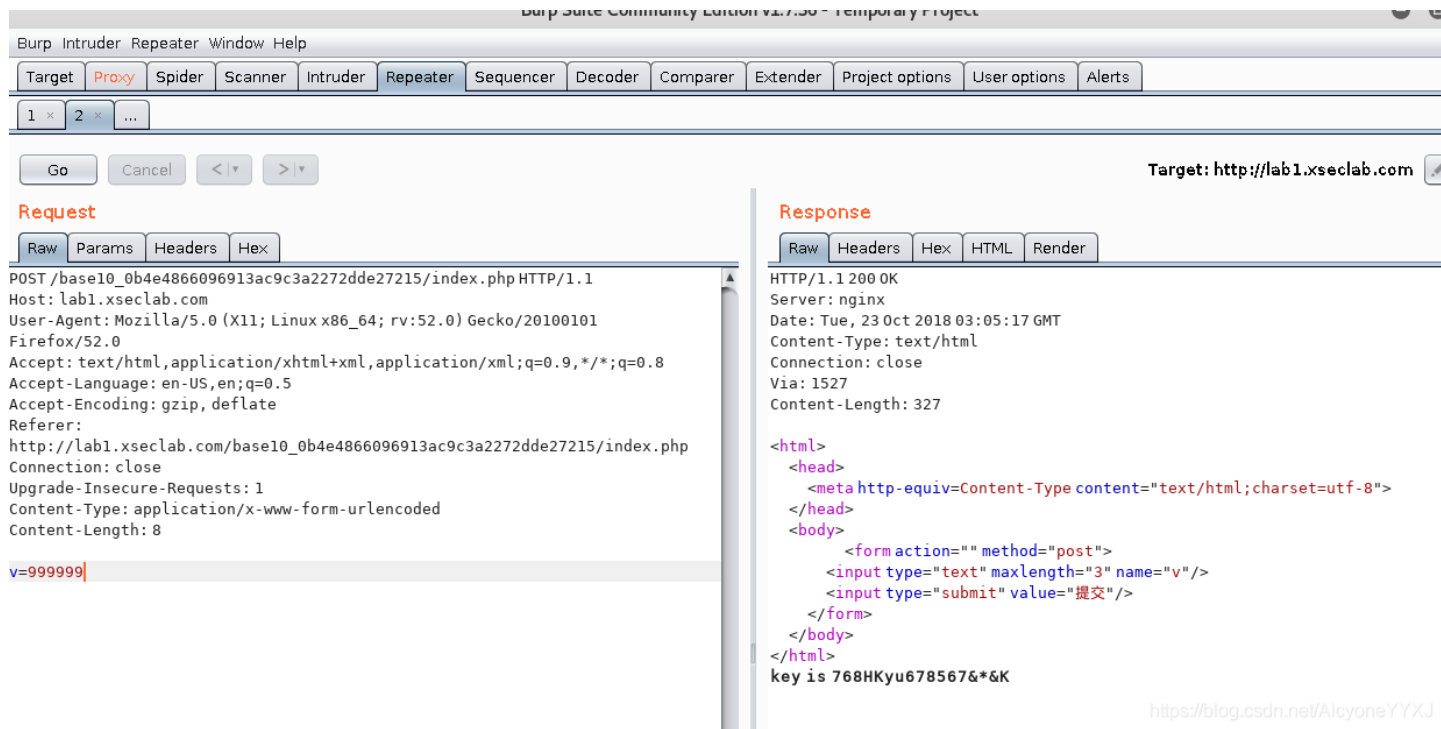
只要比服务器上的数字大就可以了!

通关地址

<https://blog.csdn.net/AlcyoneYYXJ>

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



<https://blog.csdn.net/AlcyoneYYXJ>

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

<https://blog.csdn.net/AlcyoneYYXJ>

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

查看源代码

消息头	Cookie	参数	响应	耗时	堆栈跟踪
▼ 预览					

必须从本地访问!

```
▼ 响应载荷 (payload)
10 <body>
17
18 <?php
19 //print_r($_SERVER);
20 $arr=explode(',',$_SERVER['HTTP_X_FORWARDED_FOR']);
21 if($arr[0]=='127.0.0.1'){
22     //key
23     echo "key is ^&*(UIHKJjkadshf";
24 }else{
25     echo "必须从本地访问! ";
26 }
```

<https://blog.csdn.net/AlcyoneYYXJ>

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

<https://blog.csdn.net/AlcyoneYYXJ>

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  
https://blog.csdn.net/AlcyoneYYXJ
```

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.

<https://blog.csdn.net/AlcyoneYYXJ>

那就访问login.php

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

right! key is UIJ%%IOOqweqwdsf

<https://blog.csdn.net/AlcyoneYYXJ>