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

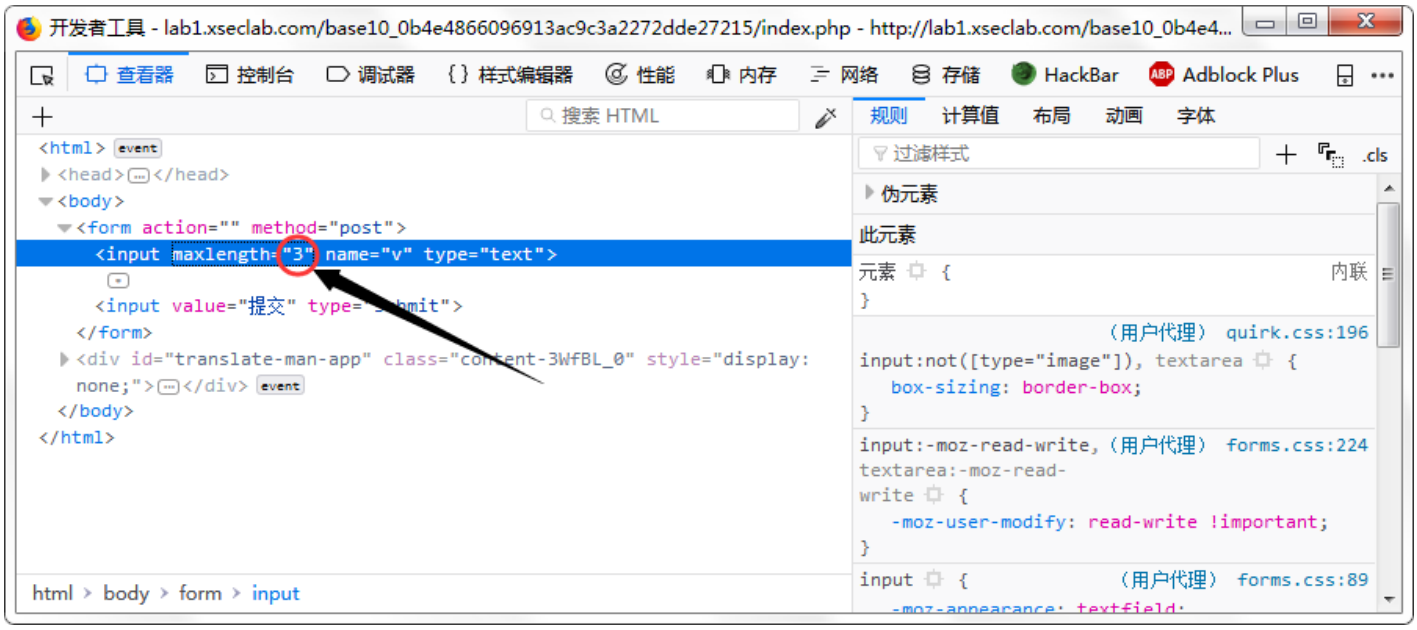
1、比较大小

题目链接：

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

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。

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。



2、nmap我用过

题目链接：http://www.zzti.edu.cn/

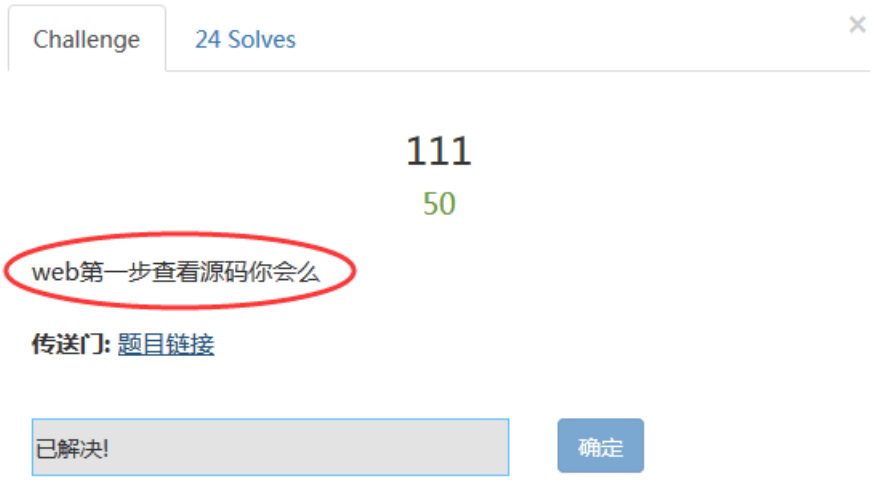
这个题目就是考察nmap的使用,用kali linux 或windows系统的nmap工具扫描，输入扫描命令：nmap 202.196.32.7

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。

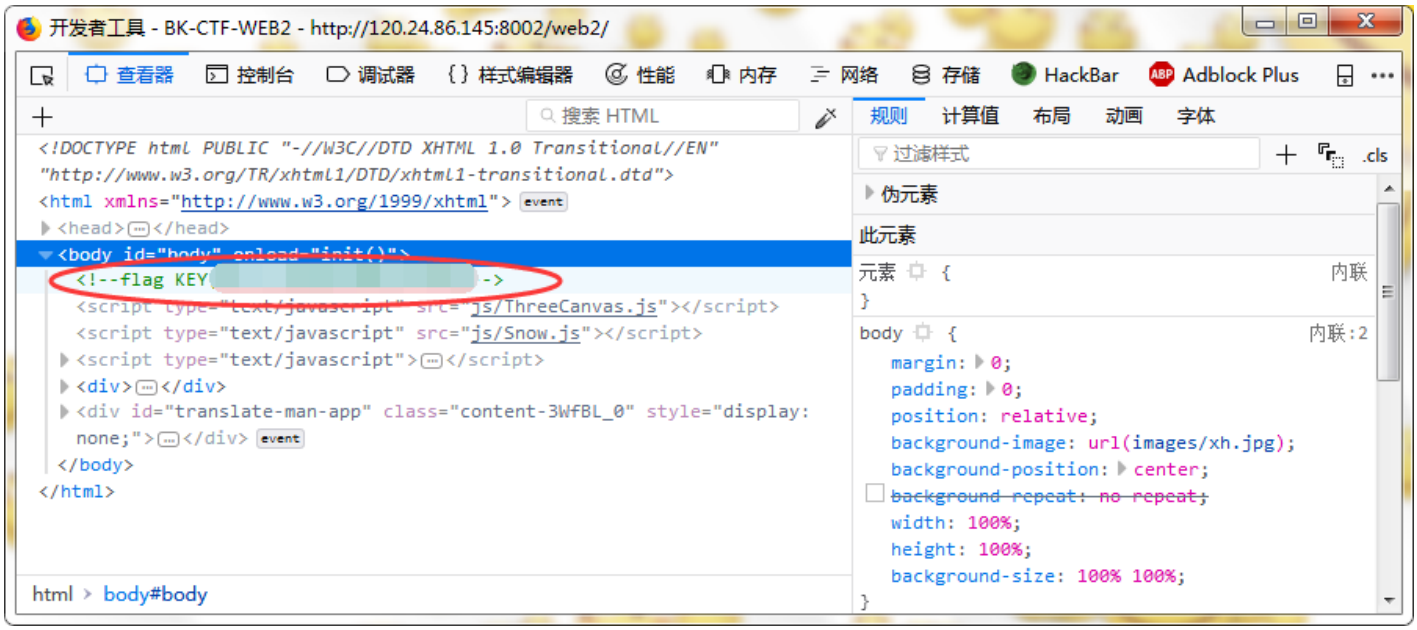
```
root@wendy:~# nmap 202.196.32.7

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
[redacted]

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/

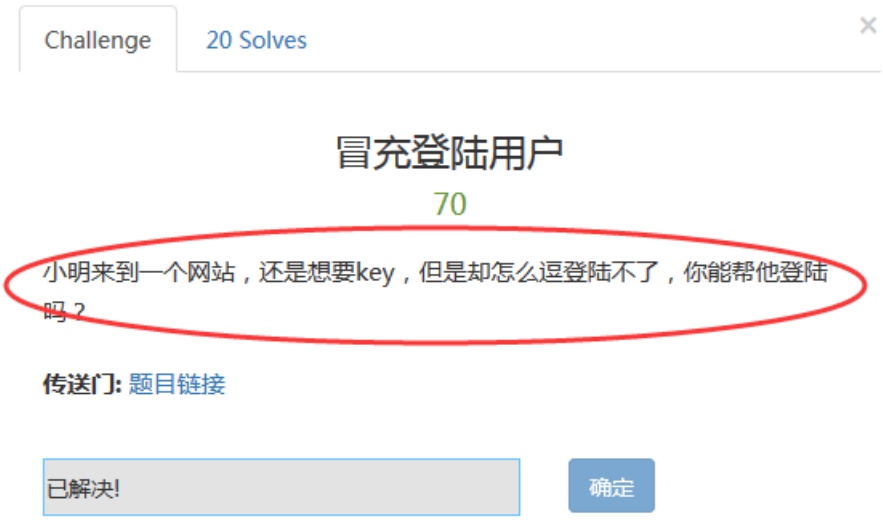


用F12打开开发者工具即可得到答案。



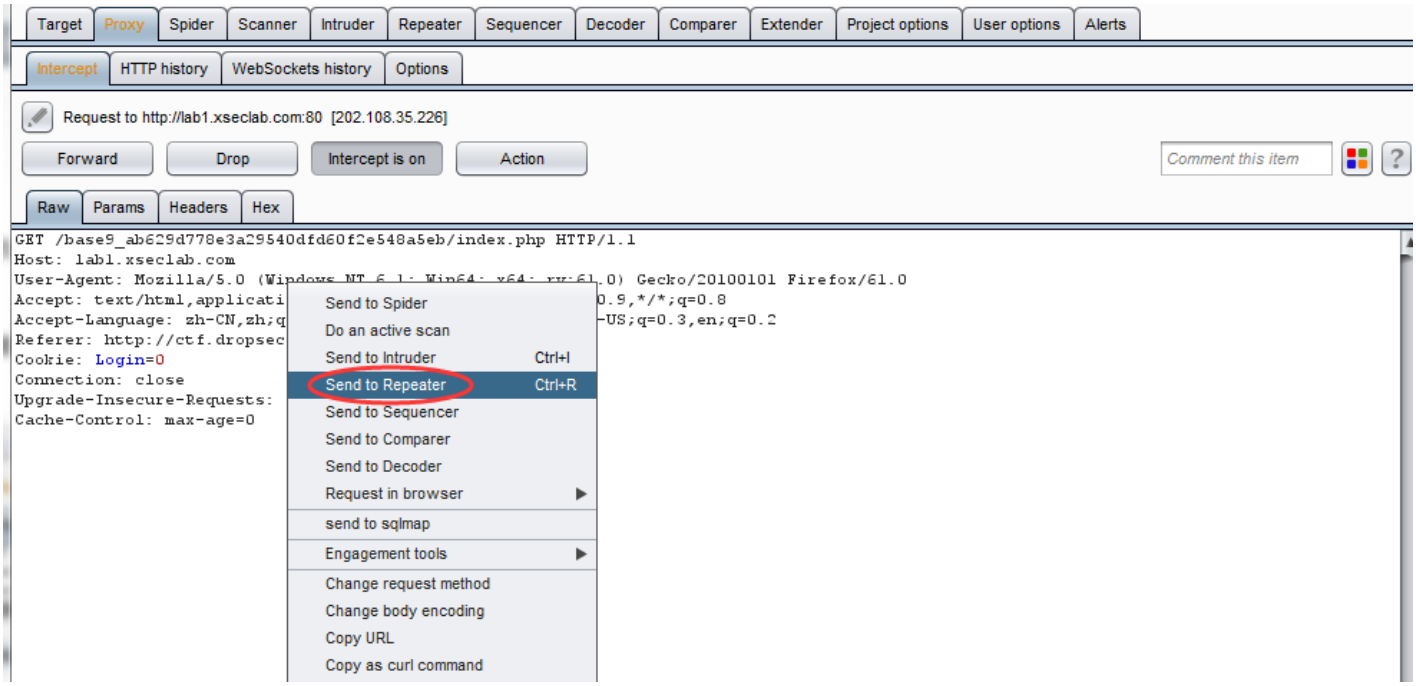
4、冒充登录用户

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

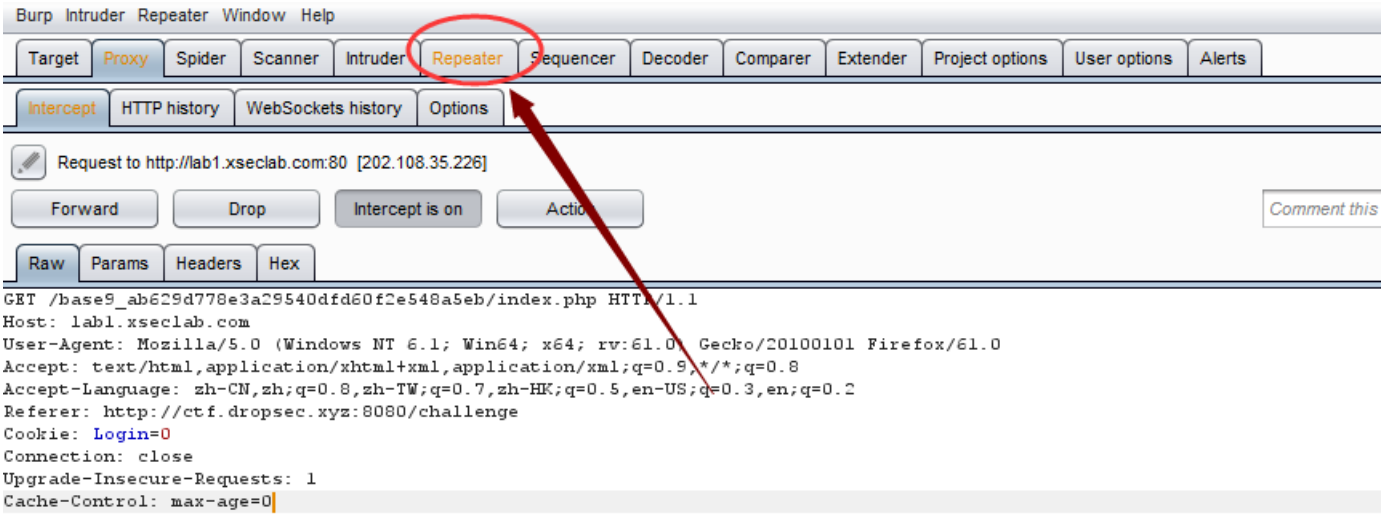


您还没有登陆呢！

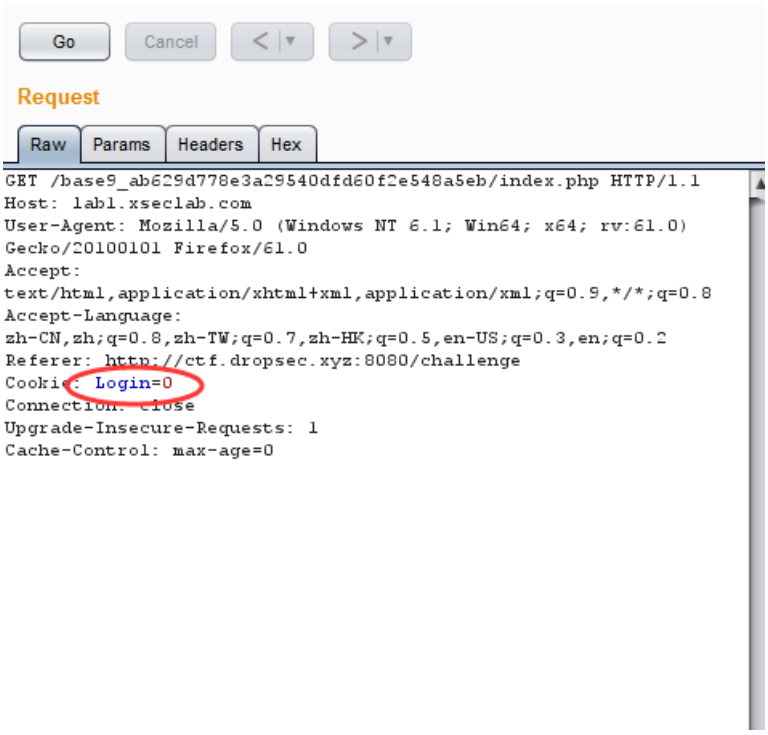
本题主要考察抓包工具 burpsuite的使用。

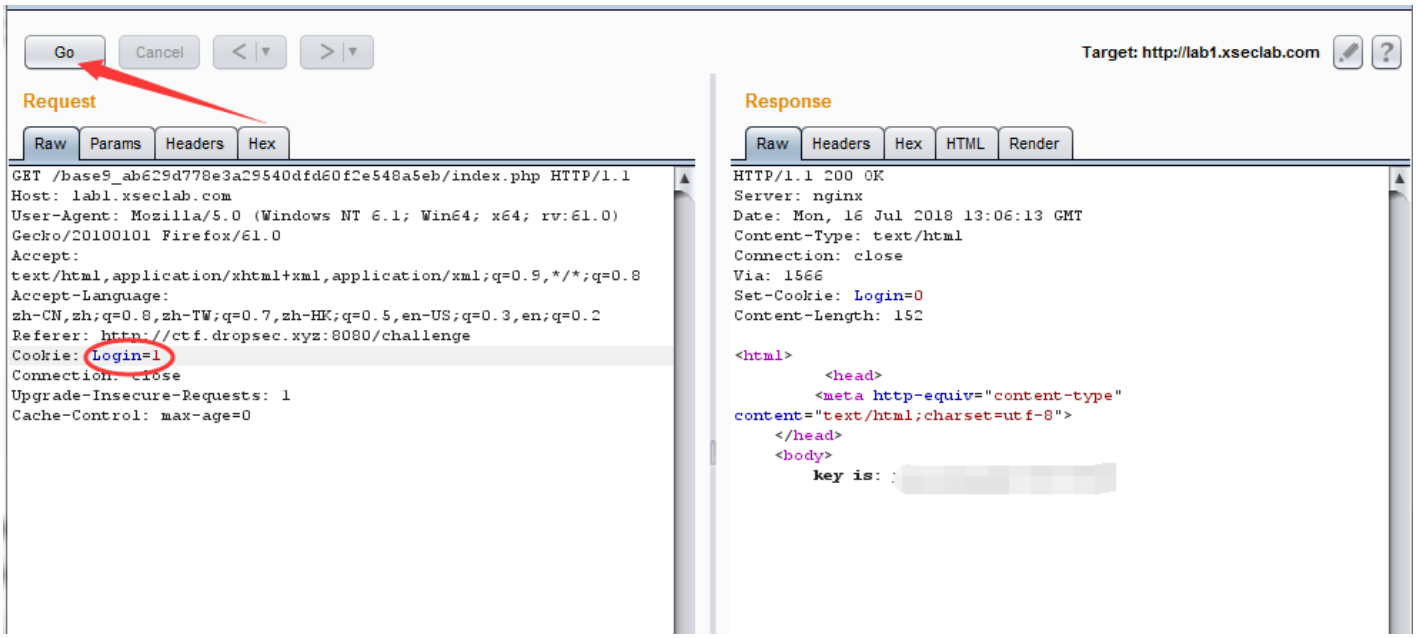


抓包后右键点击Send to Repeater，点击Repeater按钮，



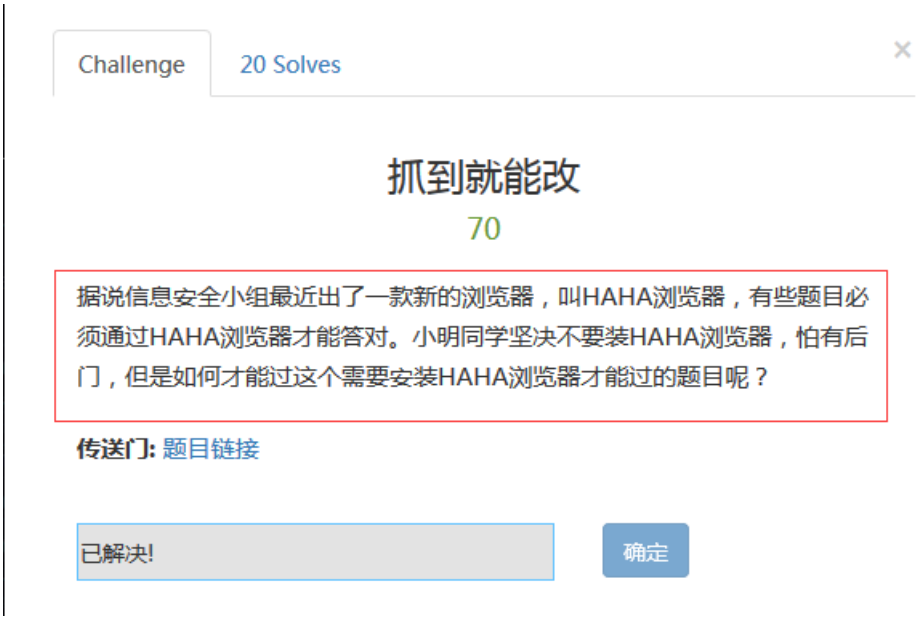
看到下面的界面，Cookie：Login=0，把“0”改成“1”，然后点击“go”,即可得到key。





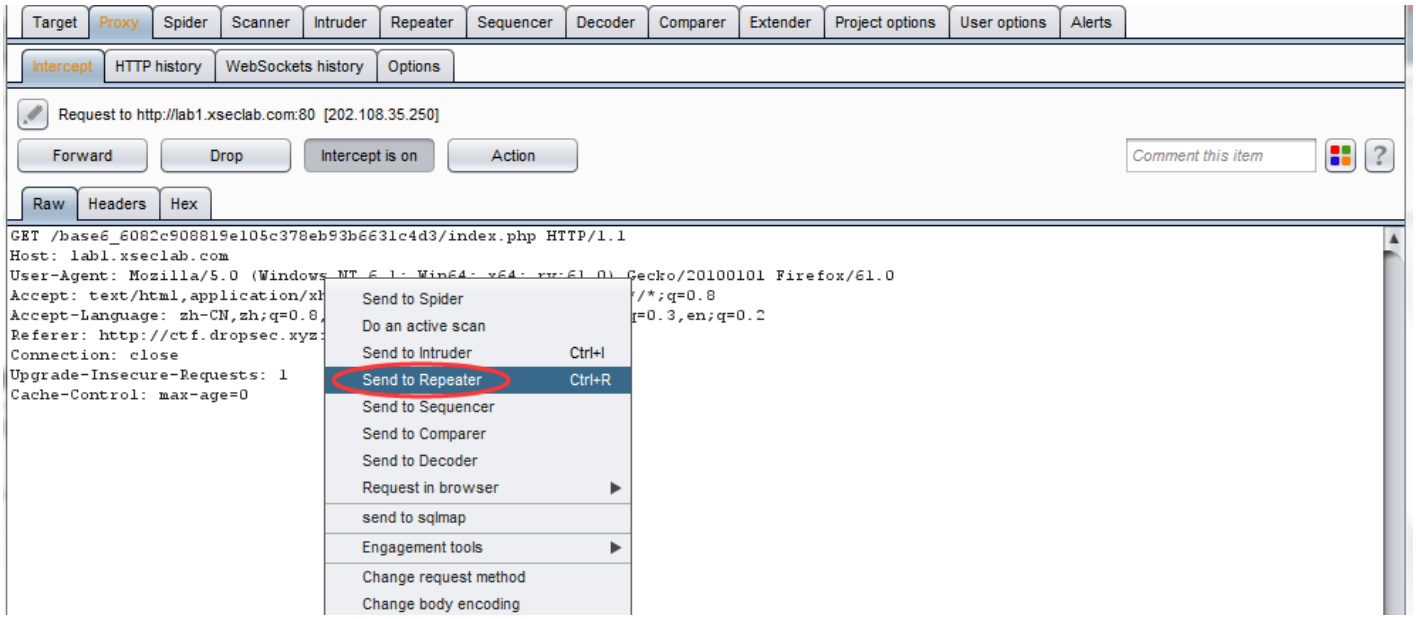
5、抓到就能改

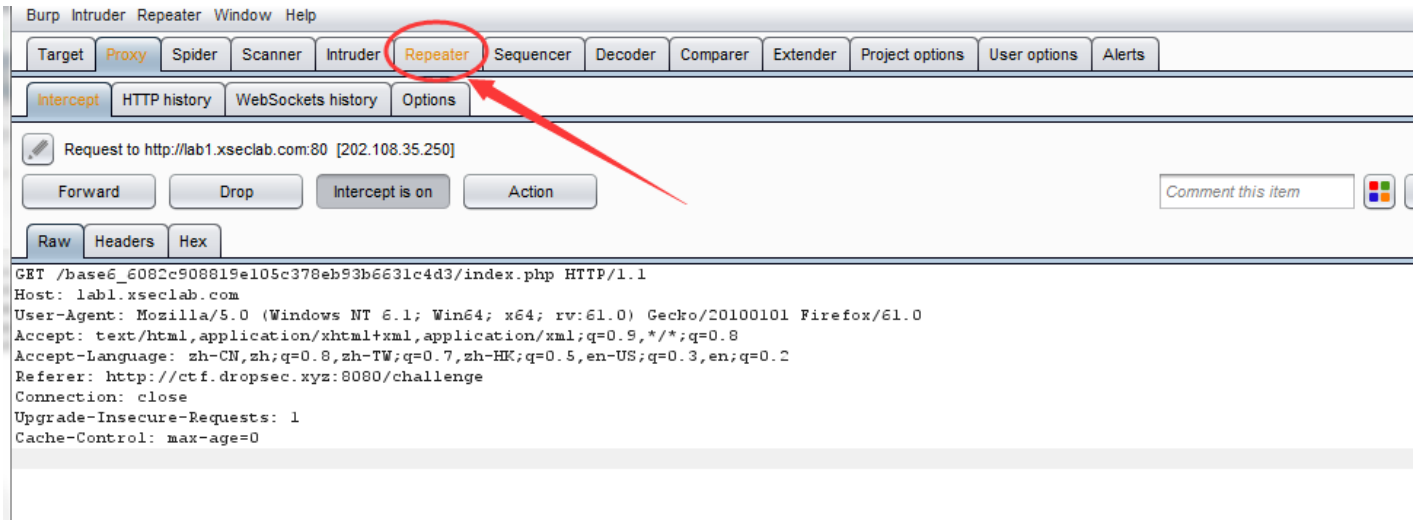
题目链接：http://lab1.xseclab.com/base6_6082c908819e105c378eb93b6631c4d3/index.php

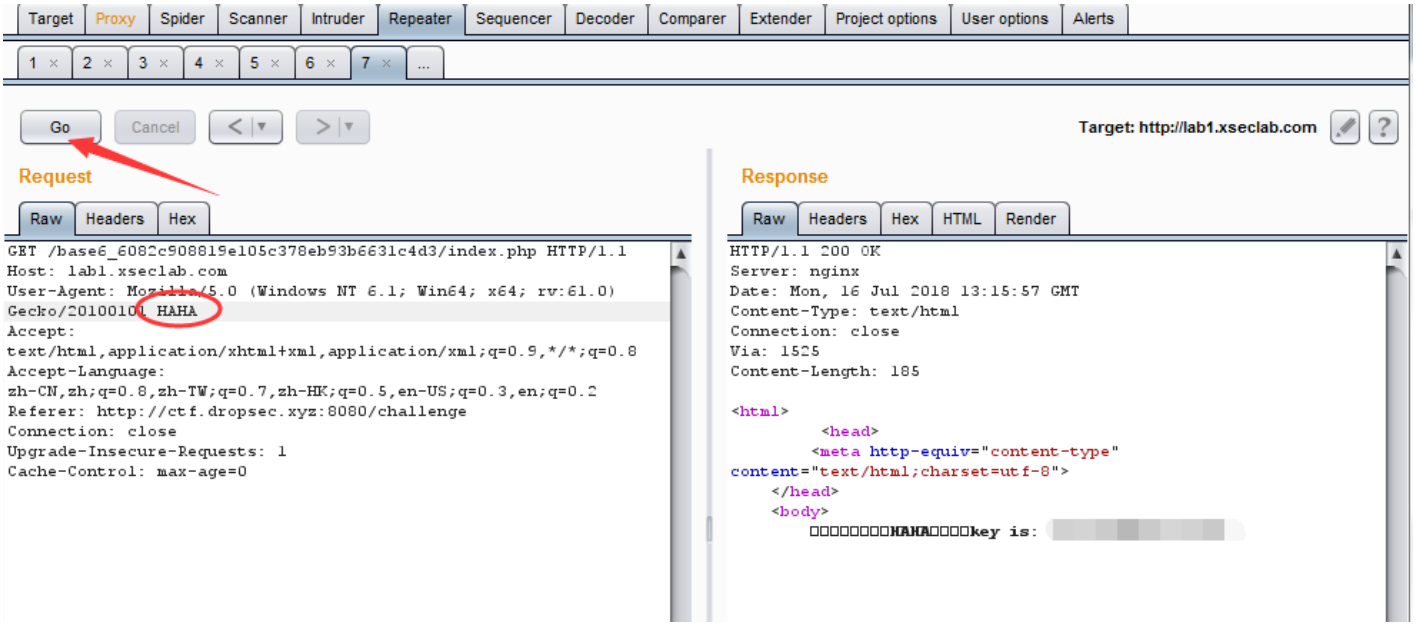


该题也是考察burpsuite工具的使用，修改User-Agent的参数值，根据题目提示，只用修改浏览器名称为HAHA，然后点击go。就可得到答案。

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

Challenge 18 Solves

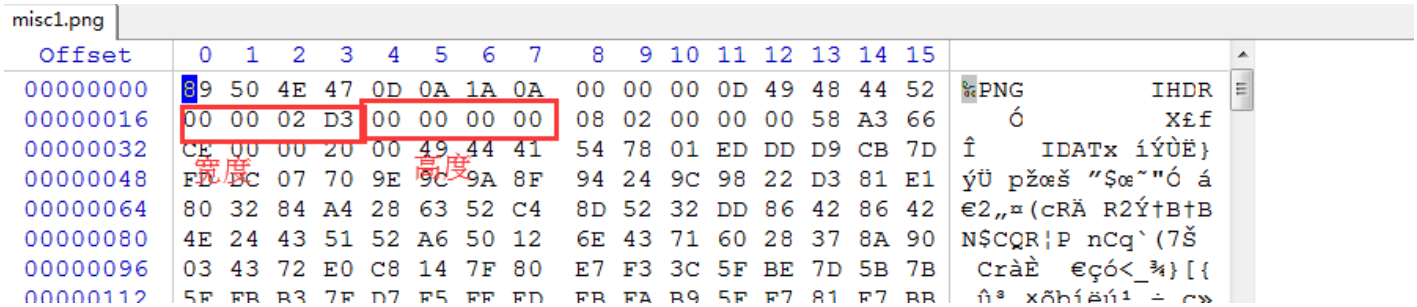
misc1

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。



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

S01ZRENXU1NJVkhGUVZKUkpaRkZNMjNJSTVLVk1XU0xLV1ZYQV1LUO5OTkU0VExLS1pGRkdWQ1dKUkxHV01LWUtVWUhRVENXT1JOR1NVS1dOUkdGS01CVko1SOdXVkpRS1pDWFFUQ1ROU1lFT1VUTE1STFZDTUxFSk5LV1
c2Q0llLWV1EQ1RDWEtWMkZNVjJWTkJKRk1SSO9MQktHWVNTUEtKV0UOV1NUR0ZTRTZWTExNUkRWRO1CUklOTEdXM1pSS01ZR01XQ1dOTllGRVVaUk9CQ0ZPU1NHS1ZJVENVU1BLV1dHWVJTVUdGTEZLVkNGR0ZKVklSUzJJ
UktGSzZDR0tOV1RLVENXR0ZSVEVVS1FOUkdGT1ZUTU1WSVRDVVNFSzVDWE1WMk5OTk5FNFZUSOpKTFZJMjJLSk5KR1dNS1RLTV1EU1RLUk5OMkVRVjJXSlpLRktSTFVKTkxEQVZKUUtaV0UOVktTR0JORk1VU1VMSkxWSV
JMWUpaS1dXVVNYSO1ZRENRM1ZOTldFN1ZDRk1STUUyTUxRS05KVEFNSzJLSV1HWVdDUkdGUOU2VkRNT1JEVkVWU1dNRktXVO9LREtFWUZVVUNWT1JIRVFVW1JMSkZGTVJLT0taS1RDUVNNS1pXRO1TQ1hLWkZGSVZTVk1S
RFZJUksySlJMR1dUO0hLSV1GVVMyVO5OVOZHVkwySkpGRksyM1VJNUpYVVdTRUtJWUhJVDJXT1JKRV1WUOZKWk1GRU1DMktOTEVLV1NXSO5XRU1UM1ZOT1NFT1ZCUkxKS1ZJVkxNSzVKVk1VOUVLWkwgSVZTVk
JGT1JMVTIyW1ZKNUtHVO5LROpaREZVVktURO1JZRVdWQOdMSkZFMjJTSOpSS1dXTktMSO1ZVO1UU1RHRkpFWVZDVO5SQ1ZLTUtTS1JLV1dOS1BKV1ZWTVVTVO5KRkZRVTNNTOJHRkUyM1VLTktFTVZTTEtSV1hRUONYS1JG
RU1VW1FPU1FWTU1DVkdCTEdXNUNXS1JXRVVSM1NLVTRWTVZKUk1SSFZLMjNZSzVLRk1TUO5LWktYQVUyVE5SUOZRVFRMS1pNVkdNRE1MSkpFS1RTUOpWVOZVVDJVT1JTRU9WQ1JLVjVGSVJMWUpOSkRBVkxaS1JLVTRVQ1
RHQk5FV1ZTRk1aSEZHNlNLS1JKVk0zQO1LNUxHSVJDVk5OUOVPVkpRS1pKRk1WU1NKVktHV1NTRktKV1dJVjJWROZTRTRVVExPUk1GTU1CWkpSSkVLNUNHSzVLV1VWU1dLVkhGT1ZETUpKRVZFVlNHS1pMV1lTU05LT1ZW
VVIyVUtaRkVZVkJRT1JRVkdNS1NJUktWTVRTTOtNWVhBVONTR0JXRk1VS1JOQkdGTzIyMkk1S1ZNV1NES5ZLVO1WM1ROUk5FVVZMTE9ONFZHMONLS1ZKRENaQ1ZLVV1HUVRDVEtaVOVPV1NXS1YOVk1NQ1ZKNUxEQVdTSU
taV1hPNktUTk5ZRU9VVExPTjRVMk1LVOpKSEZLNENaS1pMRO1WQ1NLVjJFVVYyVk5CRkZNUkNLTEJLR1lTUOxLSkxHWVYyVkdCTkVXVjNMT1JEVkVWS1JJUkdXVzVDUEtSQ1ZNVENXT1JIR1FVW1FHVk1GRVZKUktWS1RD
V1NQS1JXRTRSU1VHRktYU1ZSUVBCR1ZHTUsySkpMR1c2Q1ZLSV1GVVMyVOdGUOZRVkpRSEZHRk9WVE1LWkhFTVNTVUtaREVFUzJVSVZMRVVWVE1KSkpWSTNDSOpWTEZJU0xaSzVXR1VTMk9LVjJFUVYyVOtKSOZFTURVSj
VLRUtXU1dLW1ZVNFdDVU5NWURBV1NWTVJMRTJNQ1JKVkpXV1ZTSEtOTEZVVEtYS1YyRVdVMO1NUk5GTU1LTOpWS1RBMOMyS1lZR1lWS1ZHRkpFUVVUTE9CREZPV1MySVJMREFOS1RLRV1WVVRDVUtWMkZJVTNNSkpHRk1N
TEVKNUpUQ1FTTEtaVOZVVjJVS1pMRk1WU1FHVkZWRTIyMktKTEZJVFNPS1FZRVVTQ1NOTktYU1RKUktaR0ZJMjNVSVpLRk1XU1VLUkNYSVUyVO5SVUZFVkxMT1JERk9WQ1ZHVk
NGTTIzRU1OS0VLV1NLS1VZVTRXQ1RHRkZGUVVTVOtaS1UyMONPSjVLR1laQ0hLUkxGVVMyVk5NWVZHVTJGTEpHRTIyUO9MSkpYVVZTTUtKV1RDVkNWROEyVV1WMOxPUk1WQ1ZTV1BGTEVLTktUS1VZR1VVU1dJWkpFM1Uz
TU9CSEZNMjNFS1pKRUtNSO5LT1ZYQVJTVEdGSkZJVkpRTOJMVk1NQzJLWkxFSVNTVOtSVOVVVkNTS1VZVktWUOZHRkdWRzIyTOk1SkZJU1RCS1ZWWE1UM1RHQk5FWVZUTFBCUVZHTUtLS1JMVU1SU1dLVV1WRVNDUktSRk
ZNV1JSTEpLRkUyMO1NRkpVS1dTSUpaVOUOVENUT1JGRVdWVExHQjVGQO1ETUpSSEZLNkNJSO5MRVVSQ1dOTTJVNlZKUUtaSUZNMjNRSOpKVENWVEJLS1ZUQTZLTk5SSEVXVjNMT1JFRk9WUO9LUkpHVzVEQktaVOZVVFNX
TkpGRk9VU1FMSktGRVZDU0taTEVLNkNRS1ZWVENSM1VLVV1VR1YzTE9CS1ZHMjJXS1JTRktUUO1LTjVGTVRDVO5STEZPVkpSTVJHRk0yMO1JNUtIVVRTRUtJWUHJFR1VUTUxKRUZJVkxUUEZKV1c0QO5LSV1XRO1TUkdBNFVZVkRLS1pE
Vk1WUO5QRkxEQU5LTOs1TEZVVFNXTk5ZRkVVW1JPQkVGRTJaWVBGR1RDMONLSzVWV1FSU1VLWkhGSVZTVk9SUVZFUktXSVpLWFVTU1dLTkxGVVRLUOtaTEZPV1NGROZGVkcyM1FLNUpWSVRTRUtNWUhBVjJVSVZORVVWS1
FQQ1FWRzZTVOxCSkdZV1NVS1ZWVFNUQ1dOSkZFTVZLVOxKS1ZLVkxFSzVKREFXUOdLUktWRVVTVUtWTkVXVVNWT1JNRktNTEVKUkxXWVdTWkTOTEZVVENWRO1TRUdVVExMSkxGTVZTTOxCSOZNU1NOS1pWVTRUU1NJVkxF
V1ZUTE9CTUZNTUxFS1JKREEOQ1hLW1ZWTVZTVO5OSEZLVVJRSkpORkUyMOVLWkdUQU1LTOtWV1RDUjJUS1JFWFVWU1ZPQkxWRzNDU01KR1RBVExaS01ZV11XU1NHR1dGT1VaUkxKRUZFMjNRSVpLVk1WU1ZLUkNUU1EyUO
lWTkZBV1RNS1Y0VkdWU0tKVkpFS1JTUEtNWVZFVENTS1pXRk9WU1dLSkNGTVZMVUs1R1dXV1NLS1pLRTRUU1ROTllFUVVUTEdGSEZJUktXSk5IRksOQ1ZLRV1VTVZDVU1WMkdDVlJRTEpMRk0yUO1LWkpUQzRDTktKV1dZ
VjJWT1JERVFWVExMSkxWRVZDS1BGR1dXNUNMS1JDV1VTU1dJWkhGQVVaUklaTkZFV1NXS1JJVENUU1BLU1ZYSVdLVkdGSkVXVkxMT1JRVkVNQzJKSkdXVVRTVO0TEhBVENTTk1ZV1FWS1JLWkdGSzIyTOxGS1ZNVkxaS1
lZREtVM1dLVk5FTVZUTFBCR1ZJTUtLSk5MR1daQO9LUkRFTVMyTOtWWUVPVkNXTOJDRk9STFVKWkxWTVdTVOtaS1UOVjJVT1JGRUtVVExIRkxWQO1LMkpCSkdXVFNIS1JLRVM2U1NLV1dFN1VaUUtaROZPMjJPTEpKV1k0
QO1LWktGRVYyVkdGSkVRVUxNTVJEVk1WU1dLUkxEQTVEQktNWVZLNktOROJIRkFVMOtLWkdGRU1MTU1GSVRBMkNNS1ZWWFFSMldLWkdYU1ZUTEdWSFUyMjNFSVJMRk1TU1RLUkNYQVJTUOtSRVhTVkpRSEZHVkcyM1FMRk

看到一堆乱码，做过这种类题的，知道这是一串base64编码。

推荐一个base64，base32，base16在线编码解码工具：http://www.qqxiuzi.cn/bianma/base64.htm

先进行base64解码，再把解码后的代码进行base32解码，就这样一直循环，知道最后得到flag。

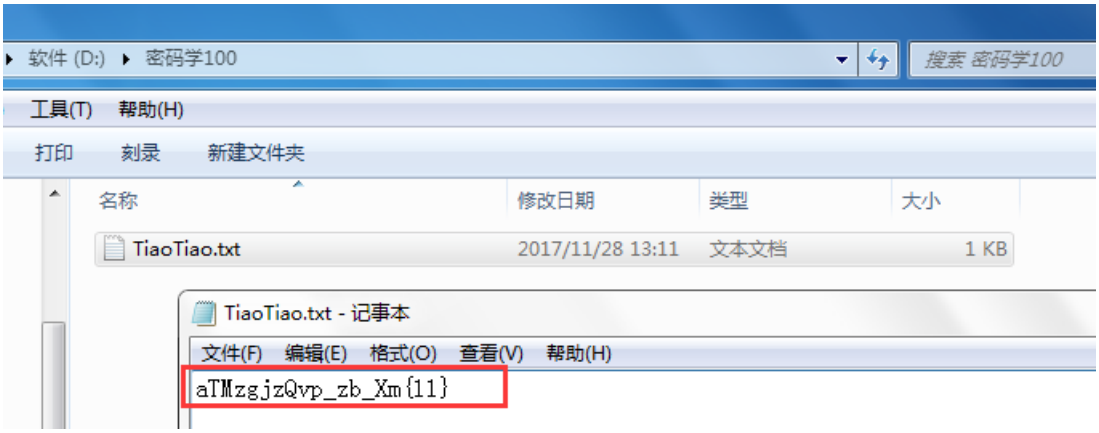
8、密码学100

题目链接：https://pan.baidu.com/s/1pLQK1Ov

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

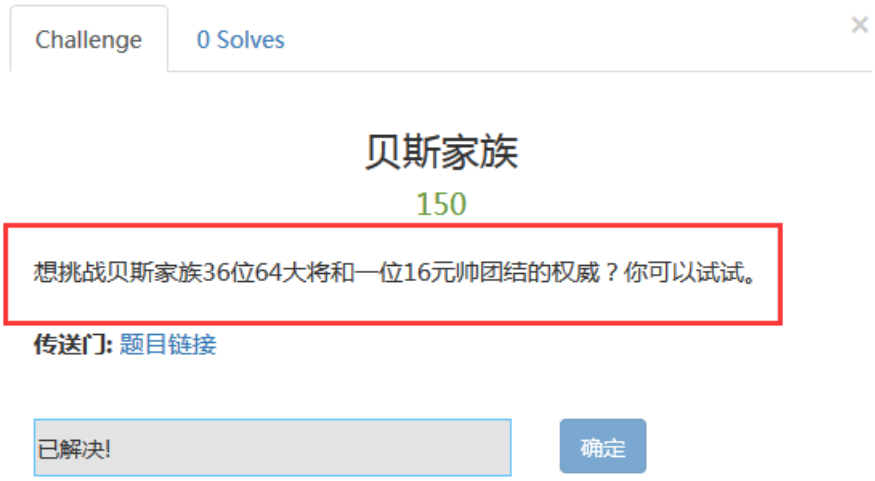


将txt文件中的代码复制到下图的密文框中，选择凯撒密码，因为不知道位移数，所以可以点击列出所有组合，经过以往做题经验，再经过仔细观察发现，位移-5或21位后的密文，同时存在“flag”这四个单词。说明即为经过栅栏加密过的结果。

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。

9、贝斯家族

题目链接：https://pan.baidu.com/s/1hsamci4



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。

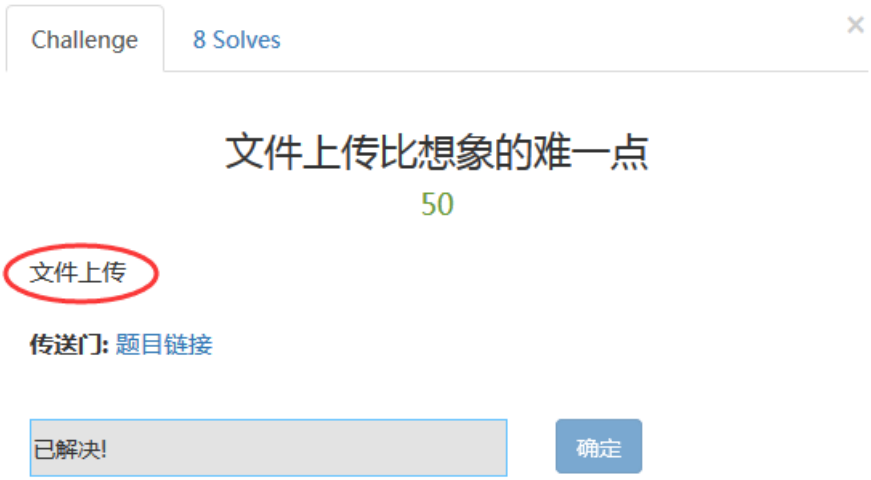
在这里推荐一个在线十六进制转文本字符串的网站：http://www.5ixuexiwang.com/str/from-hex.php

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

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。

10、文件上传比想象的难一点

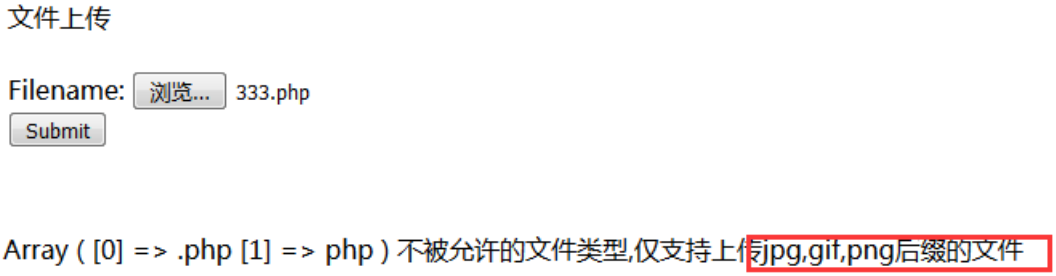
题目链接：http://teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/index.html



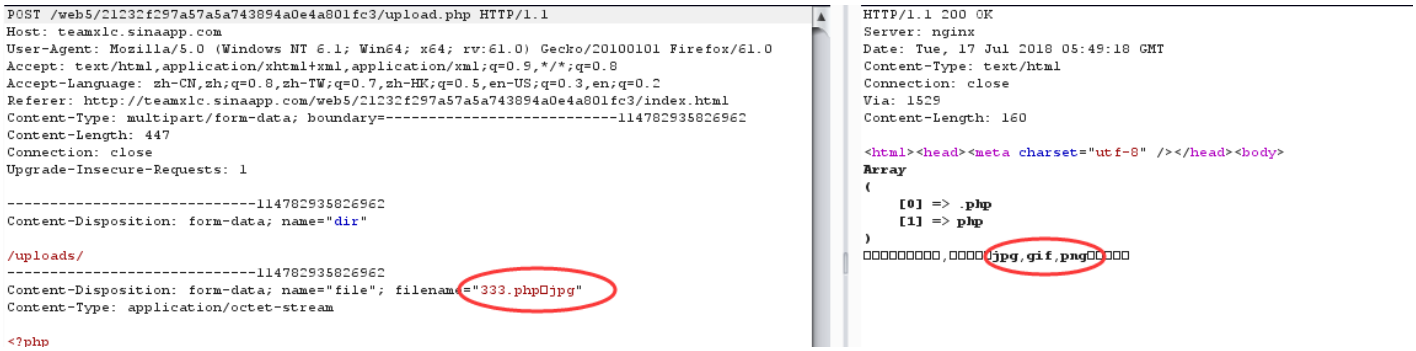
解题思路：00截断、路径构造

解题方式：

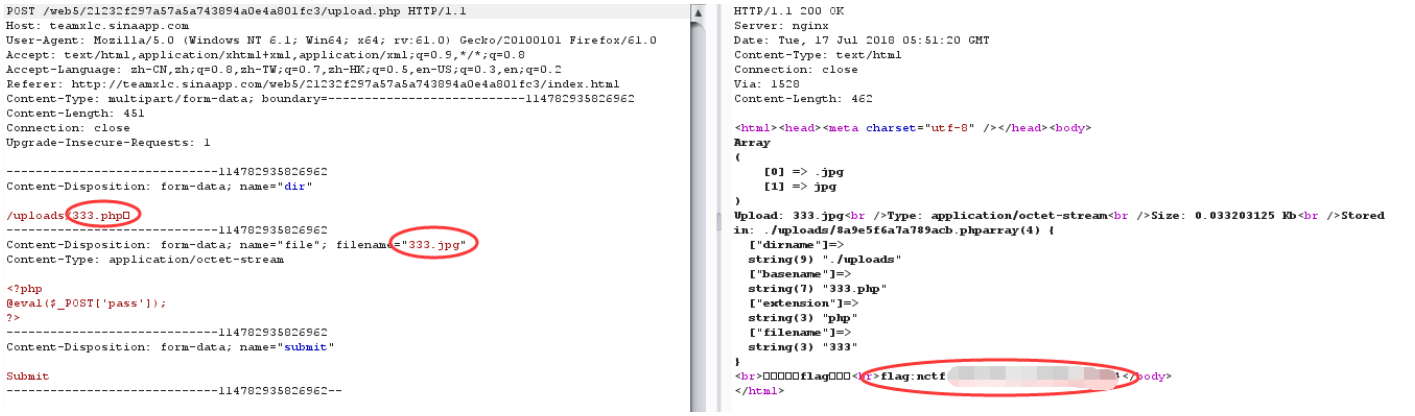
1、上传任意php文件，使用burpsuite抓包，发送至Repeater后直接GO，页面提示需要上传图片文件；



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；



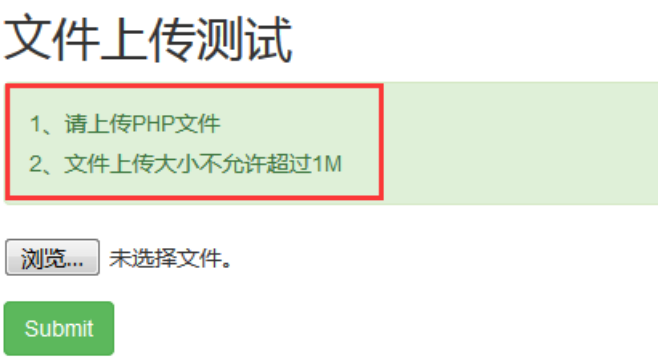
3、将333.php设置到/uploads/后，使用00截断，如下：



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/



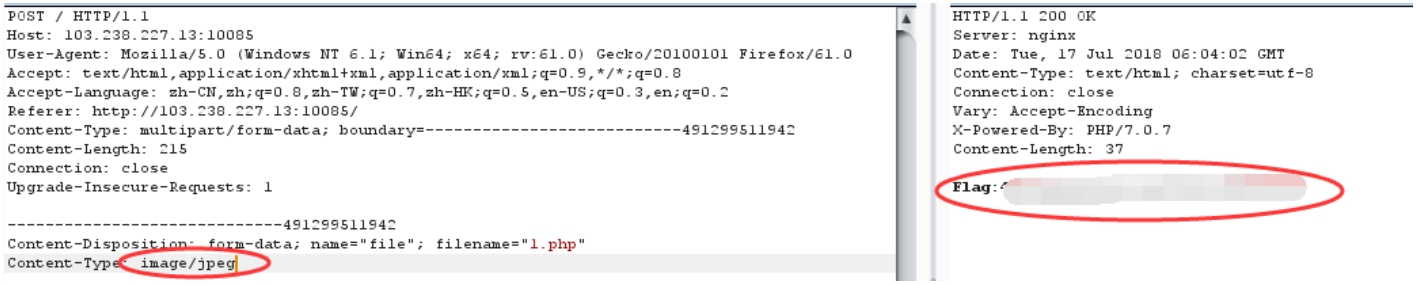
1、根据题目要求先上传任意php文件，文件大小不超过1M，如下图。

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。

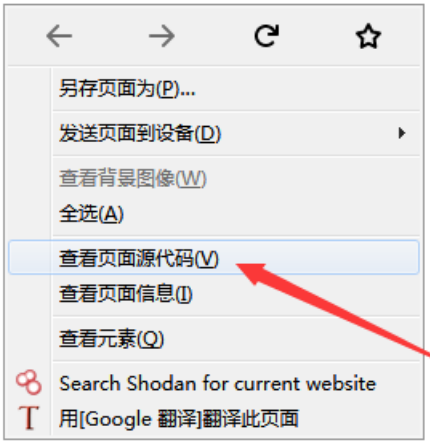
直接将其类型改为image/jpeg,再点击go即可得到flag。



12、签到题

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

key在哪里？

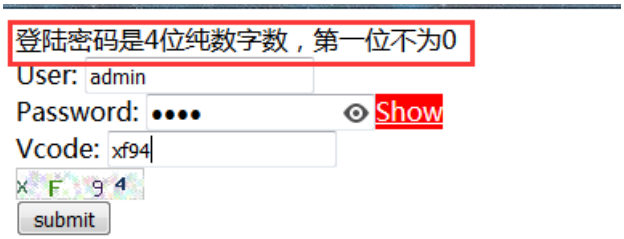


```
<html>
    <title>key在哪里？</title>
    <head>
        <meta http-equiv="content-type" content="text/html;charset=utf-8">
        <a style="display:none">nctf{                    }</a>
    </head>
    <body>
    key在哪里？
    </body>
</html>
```

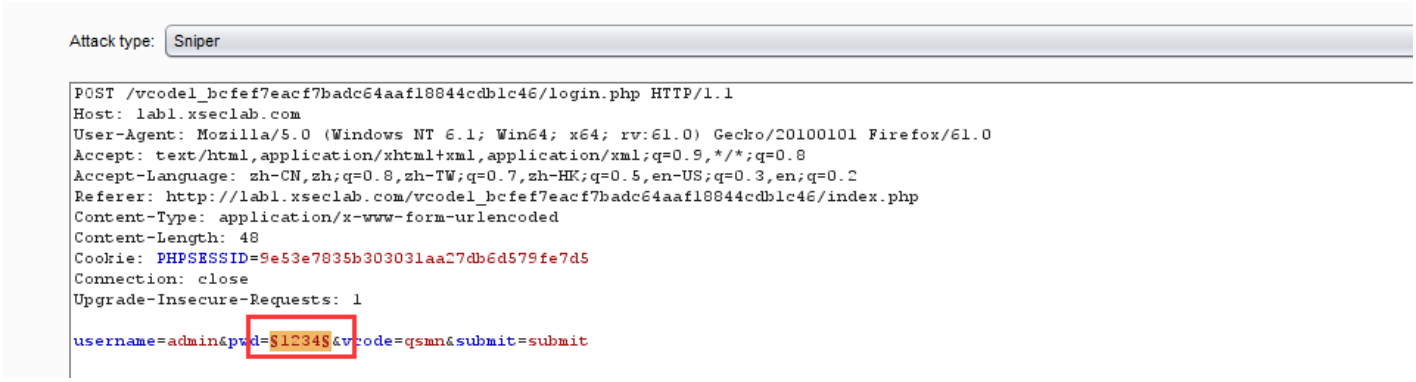
签到题就是简单，主要是考察查看源代码。直接点击题目链接，空白处右键点击查看页面源代码，即可得到flag。

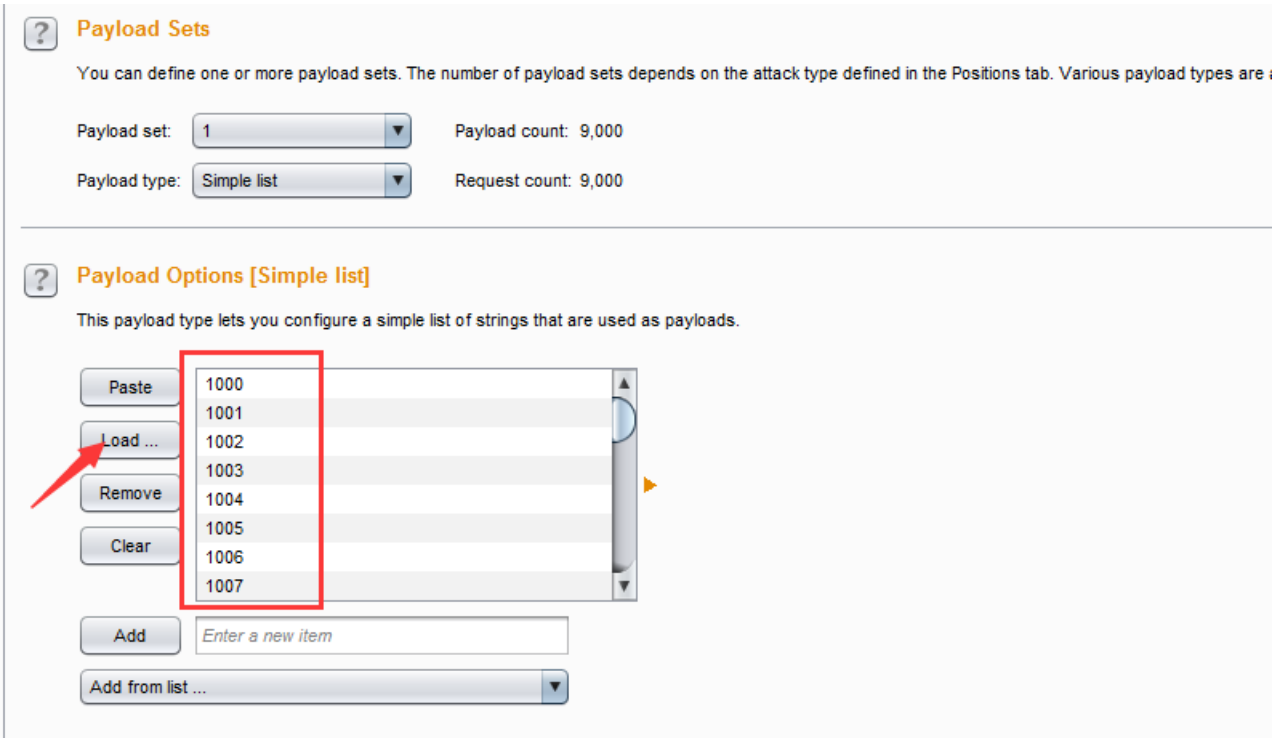
13、没有人的密码会这么简单

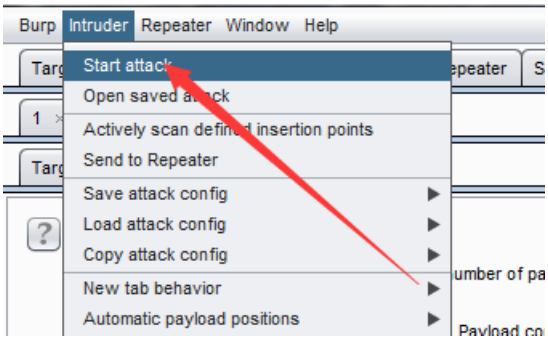
题目链接：http://lab1.xseclab.com/vcode1_bcfef7eacf7badc64aaf18844cdb1c46/index.php

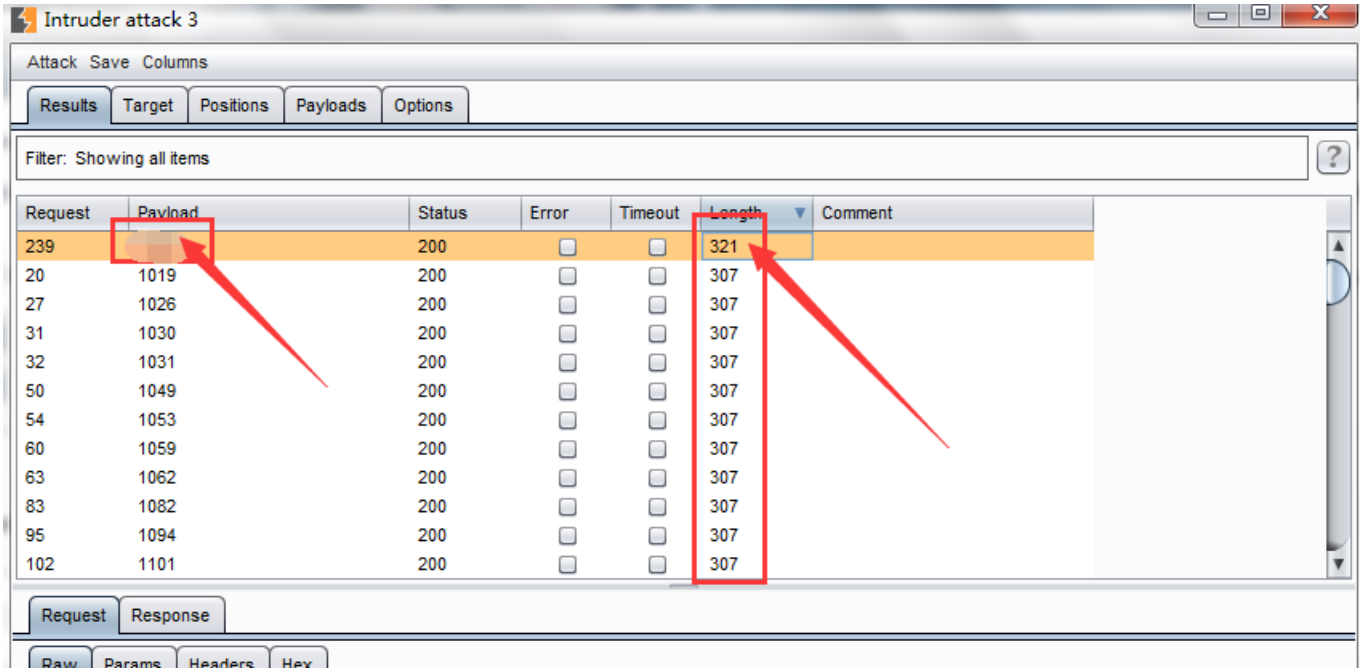


根据提示，用木头超级字典生成器生成符合题目条件的字典，然后用burpsuite抓包，右键点击send to Intruder。设置payloads，将字典加载上去，点击start stack







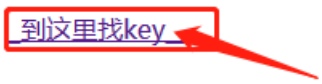


可以看到length和其他的不一样的就是密码。输入密码后即可得到key。

key is !

14、我说的是真的

题目链接：http://chinalover.sinaapp.com/web8/



点击链接“_到这里找key_”

这里真的没有KEY，土土哥哥说的，土土哥哥从来不坑人，PS土土是闰土，不是谭神

按照出题人的套路，肯定不是这样的，所以先不要点击“_到这里找key_”，首先右键点击空白处，选择查看页面源代码。

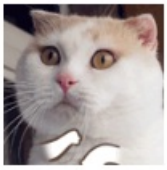
```
<html>
    <head>
        <meta http-equiv="content-type" content="text/html;charset=utf-8">
    </head>
    <body>
        <a href="./search_key.php">_到这里找key__</a>
    </body>
</html>
```

发现一个链接，点击它，即可得到key。

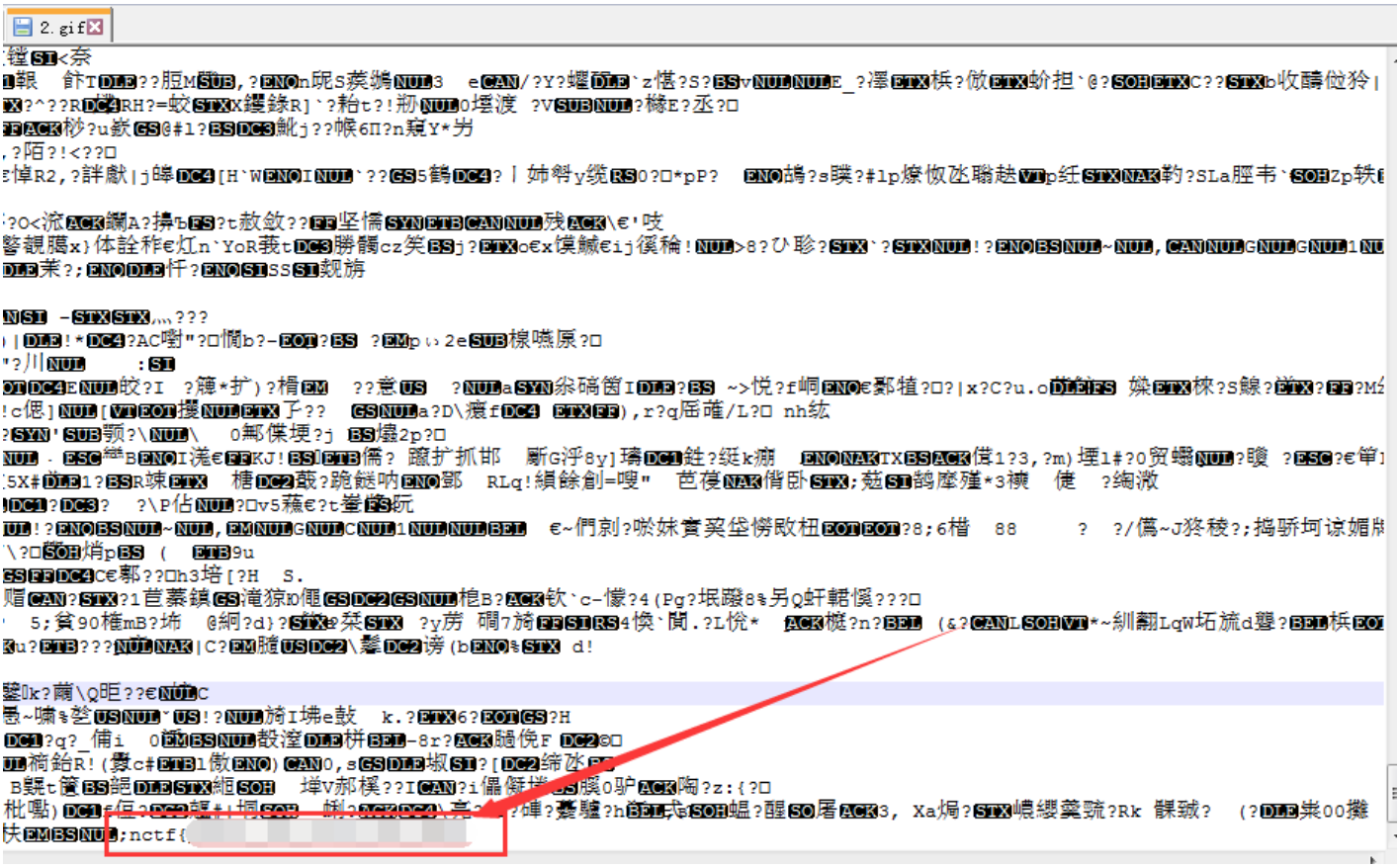
```
<script>window.location="./no_key_is_here_forever.php"; </script>
key is : 
```

15、你会改后缀吗

题目链接：http://chinalover.sinaapp.com/web2/index.html

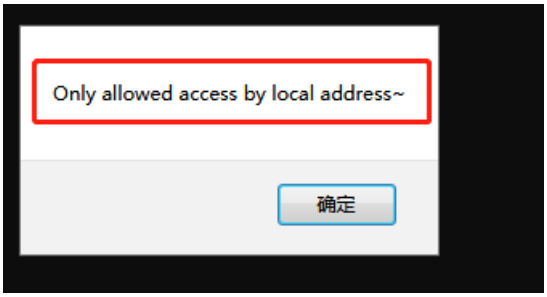
答案又是啥。。 

看到一个gif图片，查看源代码，没有什么发现。把gif图片下载下来，用notepad++打开，可以再文件末尾找到flag。

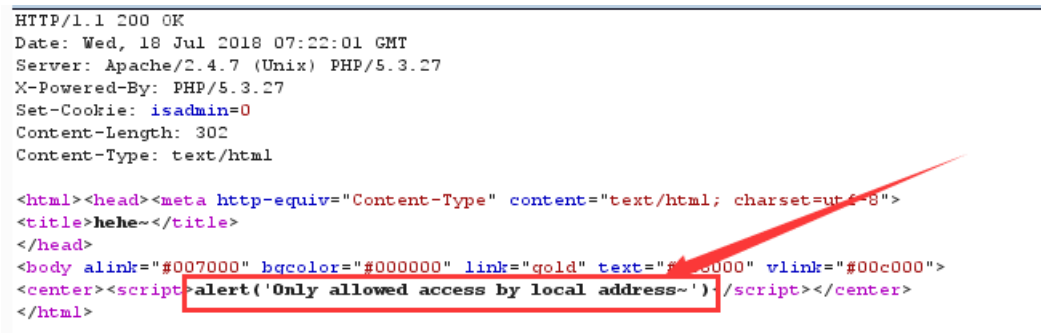


16、本机登录

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



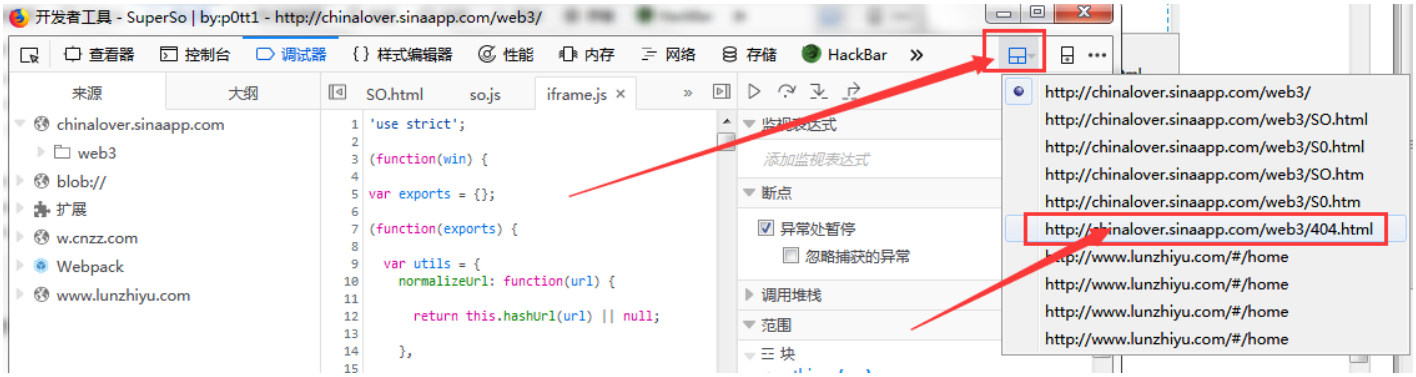
根据题目提示，用burpsuite抓包，send to Repeater,直接点击go，发现只有本地地址才能允许通过。



那么就在Request里加上一个条件X-Forwraded-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。

```
  A:visited { color: maroon }
</STYLE>
</HEAD><BODY>
<center>
<TABLE width=500 border=0 cellspacing=10><TR><TD>
<!-- Placed at the end of the document so the pages load faster -->
<!--
<script src="./js/jquery-n.7.2.min.js"></script>
<script src="./js/jquery-c.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-{.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-h.7.2.min.js"></script>
<script src="./js/jquery-i.7.2.min.js"></script>
<script src="./js/jquery-s.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-i.7.2.min.js"></script>
<script src="./js/jquery-s.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-a.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-l.7.2.min.js"></script>
<script src="./js/jquery-4.7.2.min.js"></script>
<script src="./js/jquery-g.7.2.min.js"></script>
<script src="./js/jquery-}.7.2.min.js"></script>
-->
```

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？

Submit

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。

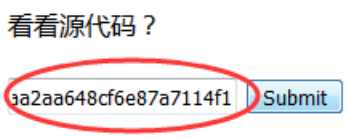
```
<html>
<title>BKCTF-WEB4</title>
<body>
<div style="display:none;"></div>
<form action="index.php" method="post" >
看看源代码？<br>
<br>
<script>
var p1 = %66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%76%61%72%20%61%3d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%
var p2 = %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%72%6f%72%22%
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("67d709b2b

p2=aa648cf6e87a7114f1"==a.value)return!0;alert("Error");a.focus();return!1}}document.getElementById("levelC

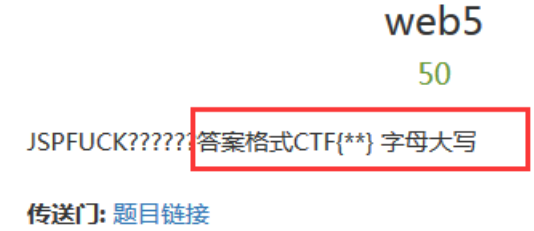
%35%34%61%61%32经过编码后的结果为54aa2，再根据eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));这条与语句，可以知道最后需要提交的数据为p1+54aa2+p2

即67d709b2b54aa2aa648cf6e87a7114f1，把其输入到输入框中，点击submit即可得到flag。



20、web5

题目链接：http://120.24.86.145:8002/web5/



```
<html>
<body>
<div style="display:none;">([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+
<form action="index.php" method="post" >
JSPFUCK??????答案格式CTF{******}<br>
<br>
<input type="input" name="flag" id="flag" />
<input type="submit" name="submit" value="Submit" />
</form>
</body>
</html>
```

查看源码可以发现一长串括号，百度一下，得知是jother编码，用在线jother解码也行，或者F12打开控制台直接将代码复制到输入框中，点击回车，即可得到flag。

注意flag格式，全部改成大写。

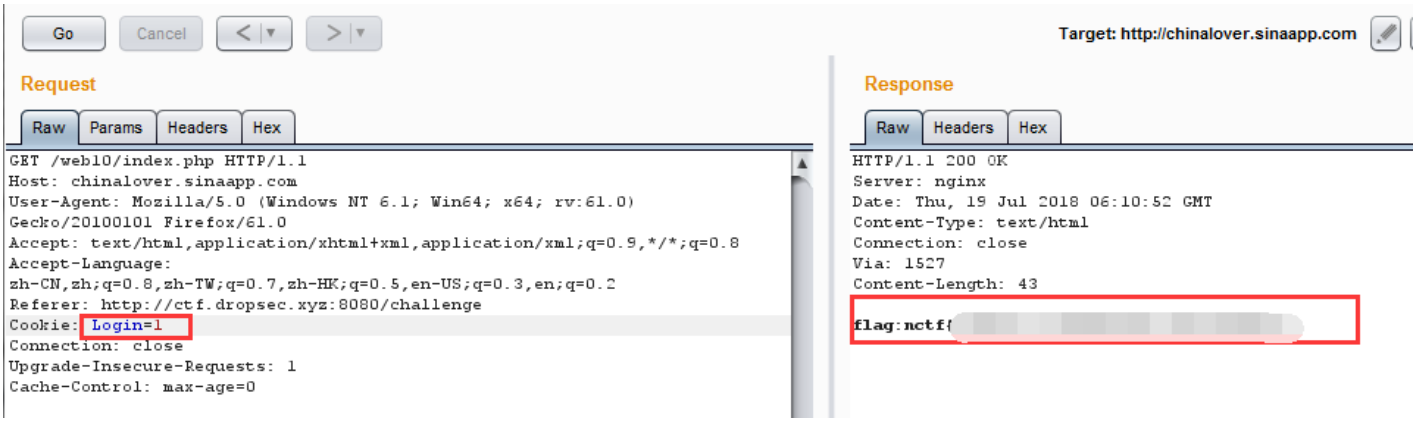
21、cookie

题目链接：http://chinalover.sinaapp.com/web10/index.php

点击题目链接，发现什么也没有。根据提示cookie，想到用burpsuite抓包。

```
GET /web10/index.php HTTP/1.1
Host: chinalover.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://ctf.dropsec.xyz:8080/challenge
Cookie: Login=0
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

send to Repeater后可以看到cookie是Login=0，把0改为1，然后点击go。即可在Response中看到flag。



22、矛盾

题目链接：http://120.24.86.145:8002/get/index1.php

```
$num=$_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.shiyanbar.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。

```
GET /sHeader/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (IE 9.0;.NET CLR 9.9 Win64; x64;
rv:61.0) Gecko/20100101
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-gb q=0.3,en;q=0.2
Referer: http://ctf.dropsec.xyz:8080/challenge
Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1531831966;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*%E6%B8%B8%E5%A
E%A2
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
    <div id="templatemo_menu">
        <ul>
            <li><a href="#" class="current">Tips</a></li>
            <li><b>http header</b></li>
        </ul>
    </div>

    <div id="templatemo_content_wrapper">

        <div id="templatemo_content">

            <div class="content_title_01">Forbidden</div>
                        <div
class="horizontal_divider_01"> </div>
                        <div class="cleaner"> </div>

                        <p>You don't have permission to access
/ on this server.</p>
                        <p><br><br>The key is
          <div class="cleaner"> </div>
        </div>
```

转载于:https://www.cnblogs.com/wendy9593/p/9320576.html