

信息安全铁人三项赛--资质赛writeup

转载

[weixin_30639719](#) 于 2018-03-17 16:53:00 发布 330 收藏 5

文章标签: [php](#)

原文链接: <http://www.cnblogs.com/blackay03/p/8590877.html>

版权

[博客目录]

- 工具
 - [Burp Suite](#)
 - [stegsolve.jar](#)
 - [十六进制编辑器](#)
- 赛题
 - [第一题](#)
 - [第二题](#)
 - [第三题](#)
 - [第四题](#)
 - [第五题](#)
 - [第六题](#)

1- 工具:

1.1- Burp Suite

一款可以进行再WEB应用程序的集成攻击测试平台。

常用的功能: 抓包、重放、爆破

需求: (建议)Burp Suite + Firefox

介绍: [Burp Suite使用介绍](#)

代理设置+证书导入: [Firefox+Burpsuite抓包配置\(可抓取https\)](#)

使用方法:

- [Burpsuite神器常用功能使用方法总结](#)
- [Burpsuite中爆破功能的使用教程](#)
- [Burpsuite教程与技巧之HTTP brute暴力破解](#)
- [用Burpsuite破解网站密码](#)

1.2- stegsolve.jar

[下载&使用](#)

1.3- 十六进制编辑器

自己上网找吧!

[返回目录](#)

2- 赛题

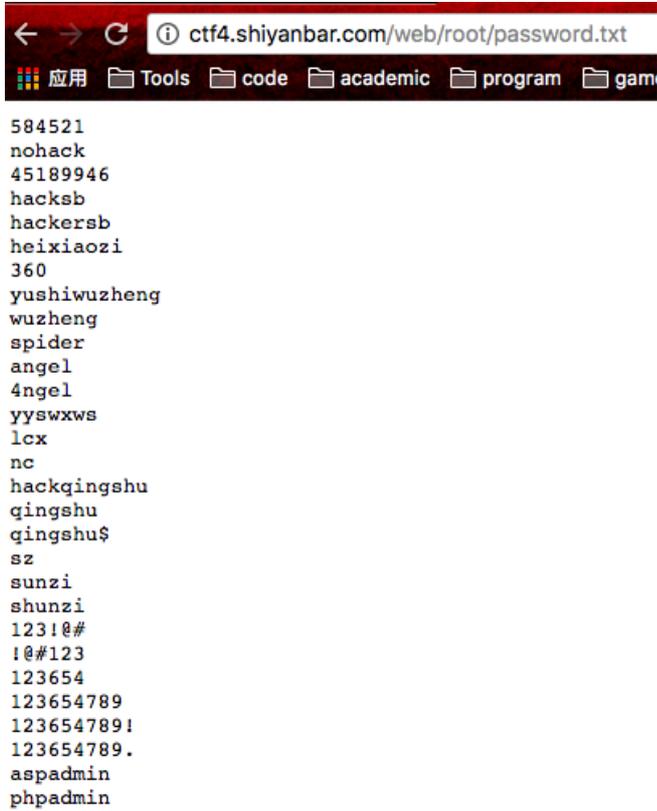
2.1 第一题：你是管理员吗？

题目链接：<http://ctf4.shiyanbar.com/web/root/index.php>

解题步骤：

1. 首先查看源代码，主页面的标题是password.txt，尝试访问password.txt：
<http://ctf4.shiyanbar.com/web/root/password.txt>

出现字典：



```
584521
nohack
45189946
hacksb
hackersb
heixiaozi
360
yushiwuzheng
wuzheng
spider
angel
4ngel
yyswxws
lcx
nc
hackqingshu
qingshu
qingshu$
sz
sunzi
shunzi
123!@#
!@#123
123654
123654789
123654789!
123654789.
aspadmin
phpadmin
```

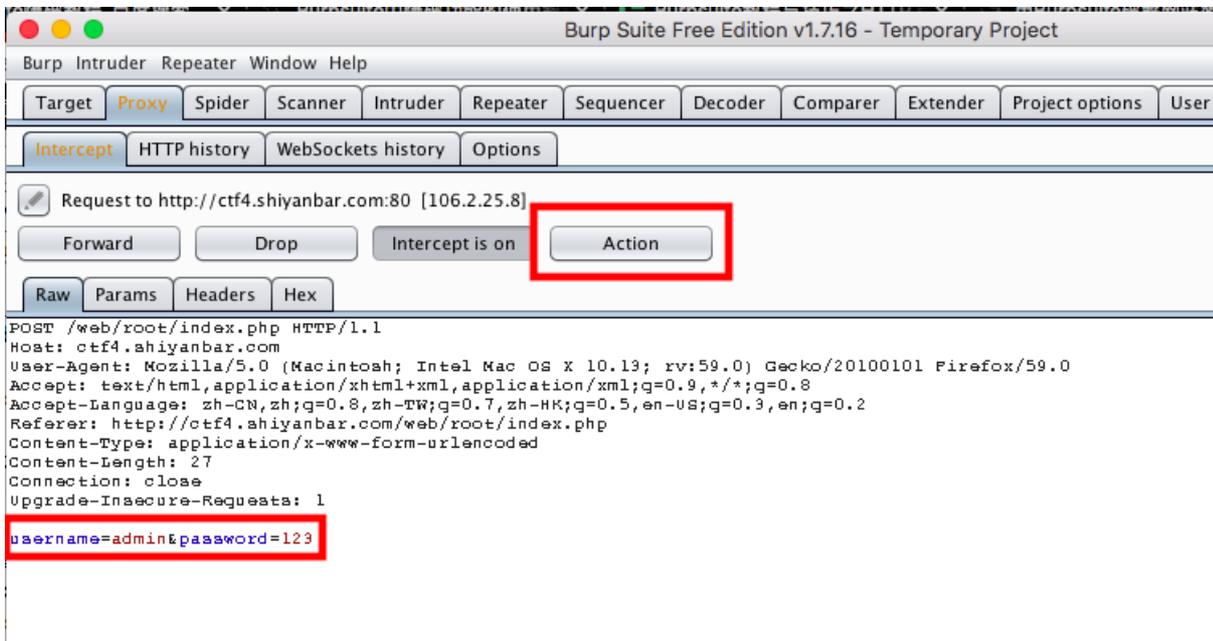
2. 使用Burp Suite爆破：

首先记录字典，随便拿个记事本就行，甚至直接放在剪贴板；

打开Burp Suite，新建项目，点击Proxy-Intercept下面的Intercept is off按钮，让它变成Intercept is on:



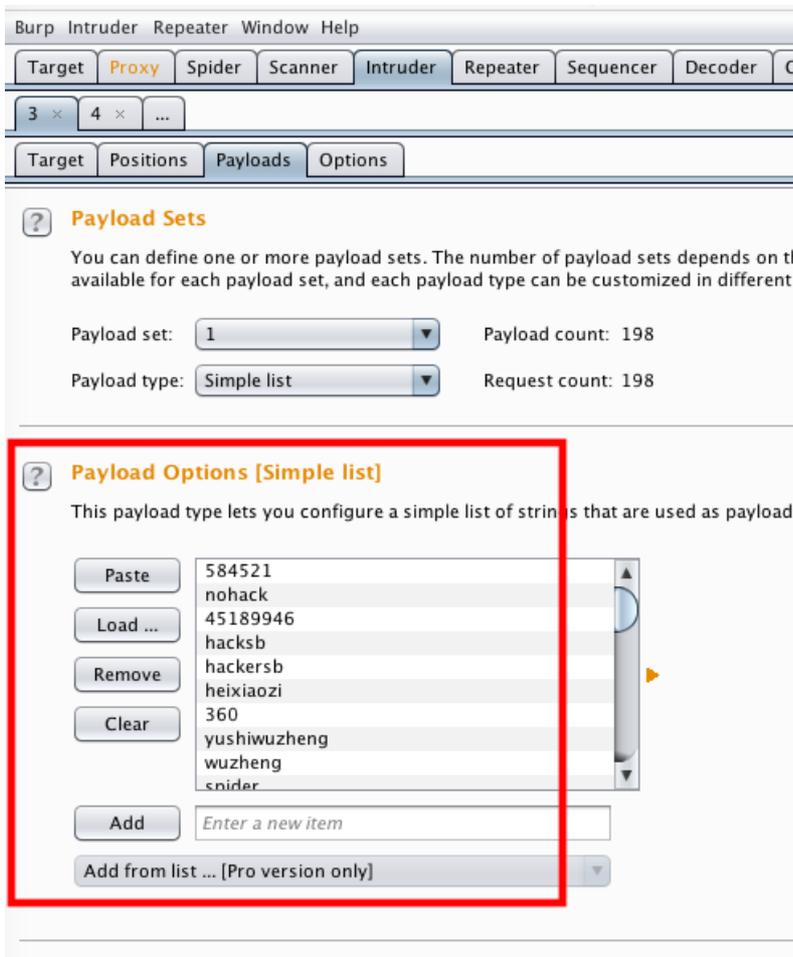
再次访问index.php，页面会一直保持载入，说明已经被Burp Suite抓包，点击forward，让页面加载出来，随便输入几个数，试图登录，页面卡住（被抓包），这时回到Burp Suite，在抓包界面（注意raw里面会出现彩色变量username=admin&password=123）点击action按钮，选择Send to Intruder:



点击最上面菜单栏的Intruder选项(变成橘黄色的), 点击该页面下的position选项, 先点clear清除变量(因为BP默认会选中用户名username和密码password双变量, 双变量爆破会很慢, 因为index中的用户名是固定的admin, 我们只用爆破密码就好了)再选中password的变量(也就是图中的123)点击add, 这时会发现123变成\$123\$, 说明爆破变量已经确定:

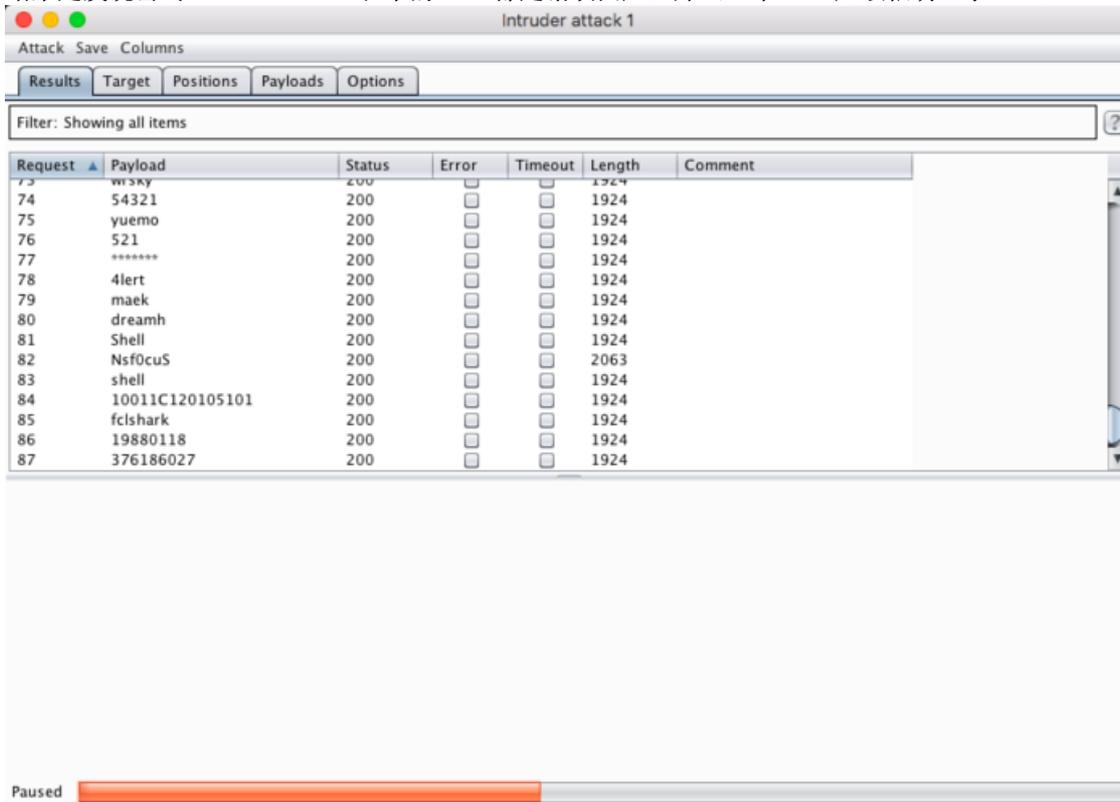


然后点击payload按钮(设置字典), 在payload options这一块中, 将原本的字典复制进剪贴板, 然后点paste, 或者直接导入文件也行:

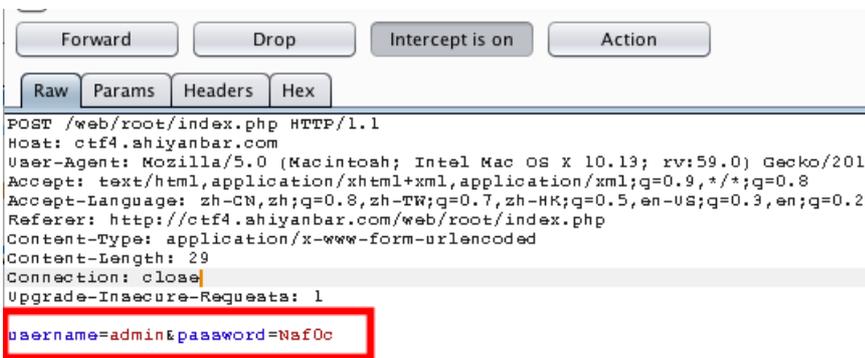


导入后直接点击右上角**start attack**按钮，等待.....

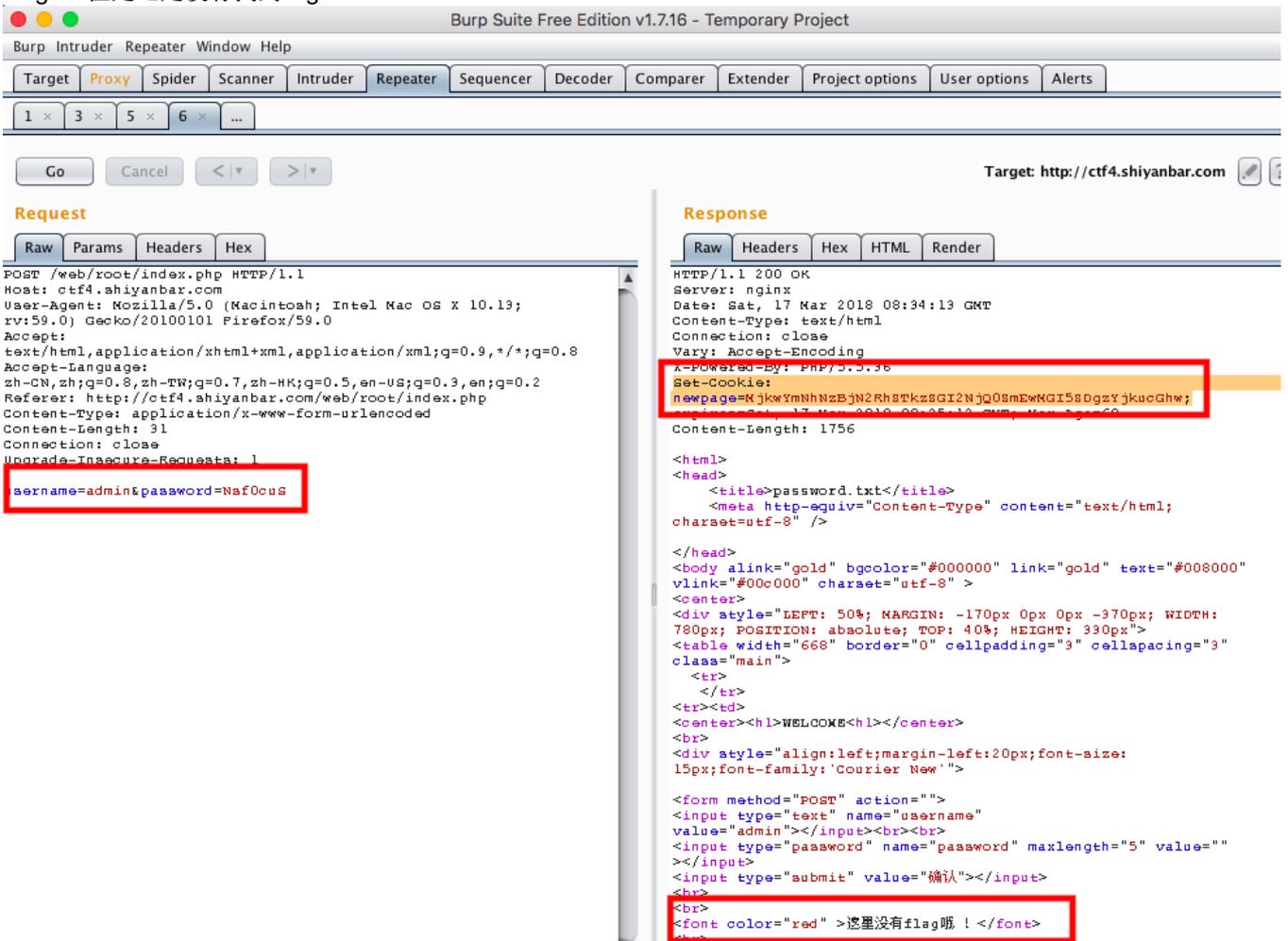
结果是发现密码：Nsf0cuS（一长串的1924都是错误回应，那么一个2063应该很明显了.....）



- 找到密码后，我们关掉抓包：Intercept is off或者直接点Forward，我们将结果输入password.txt页面，发现只能输入五位数！？看来不行，我们得用Burp Suite来登录了，再次开始抓包 Intercept is on(如果之前点forward就不用了，Intercept会一直保持)，我们随便输入一些数进去，然后登录，页面再次加载，我们抓到包后看到raw中的可修改的彩色部分：



我们再次点击action按钮，选择Send to Repeater按钮（重放功能），在Request栏中将password改为Nsf0cuS，点击go按钮，Response中出现信息，发现Set-Cookie: newpage=MjkwYmNhNzBjN2RhZTkzZGI2NjQ0ZmEwMGI5ZDgzYjkucGhw; bingo! 但是还是没有找到flag!



- 我们对MjkwYmNhNzBjN2RhZTkzZGI2NjQ0ZmEwMGI5ZDgzYjkucGhw; 进行base64解码，结果为: 290bca70c7dae93db6644fa00b9d83b9.php
关掉抓包: Intercept is off
赶紧访问试试: <http://ctf4.shiyanbar.com/web/root/290bca70c7dae93db6644fa00b9d83b9.php>
发现又是一个新界面，还没结束！打开抓包，随便输入点东西:

小黑留言板

你还没有登录，不能留言！

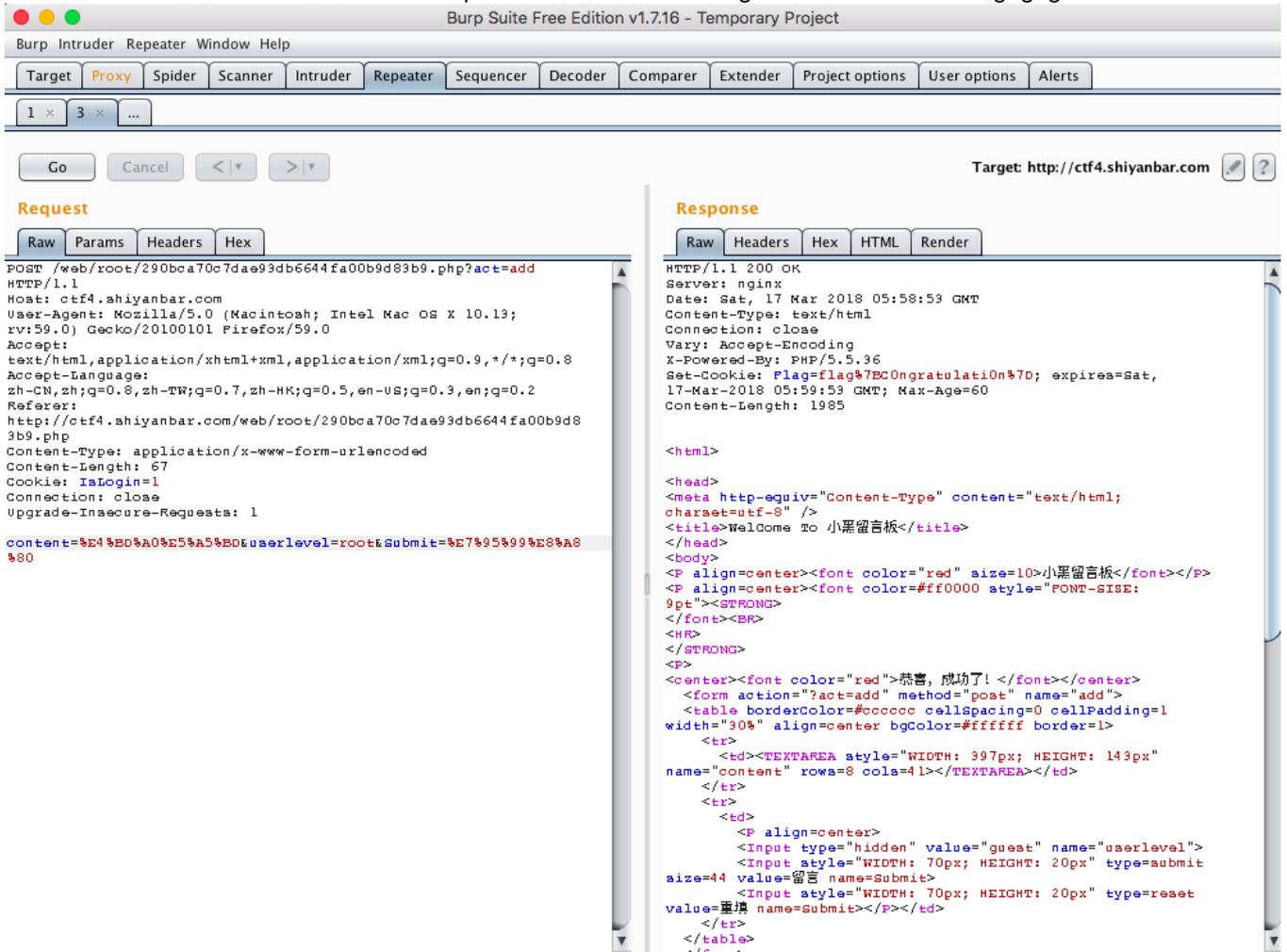
难过啊！

小黑最近刚学会php就写了个留言板让大家使用,可是这个留言板有漏洞,导致大黑们可以通过某些手段以小黑的身份留言

大黑们,你们准备好了吗?

留言者	留言内容

抓到包发现了可修改部分！赶紧Send to Repeater，修改Cookie: IsLogin=1和userlevel=root，gogogo~



5. flag终于出现！但是！注意这个格式！千万不要以为直接输入上面的数就可以了！错！

【答案格式】：flag{}

flag{flag%7BC0ngratulati0n%7D}

因为%7B和%7D是{和}，所以答案应该再进行url解码！

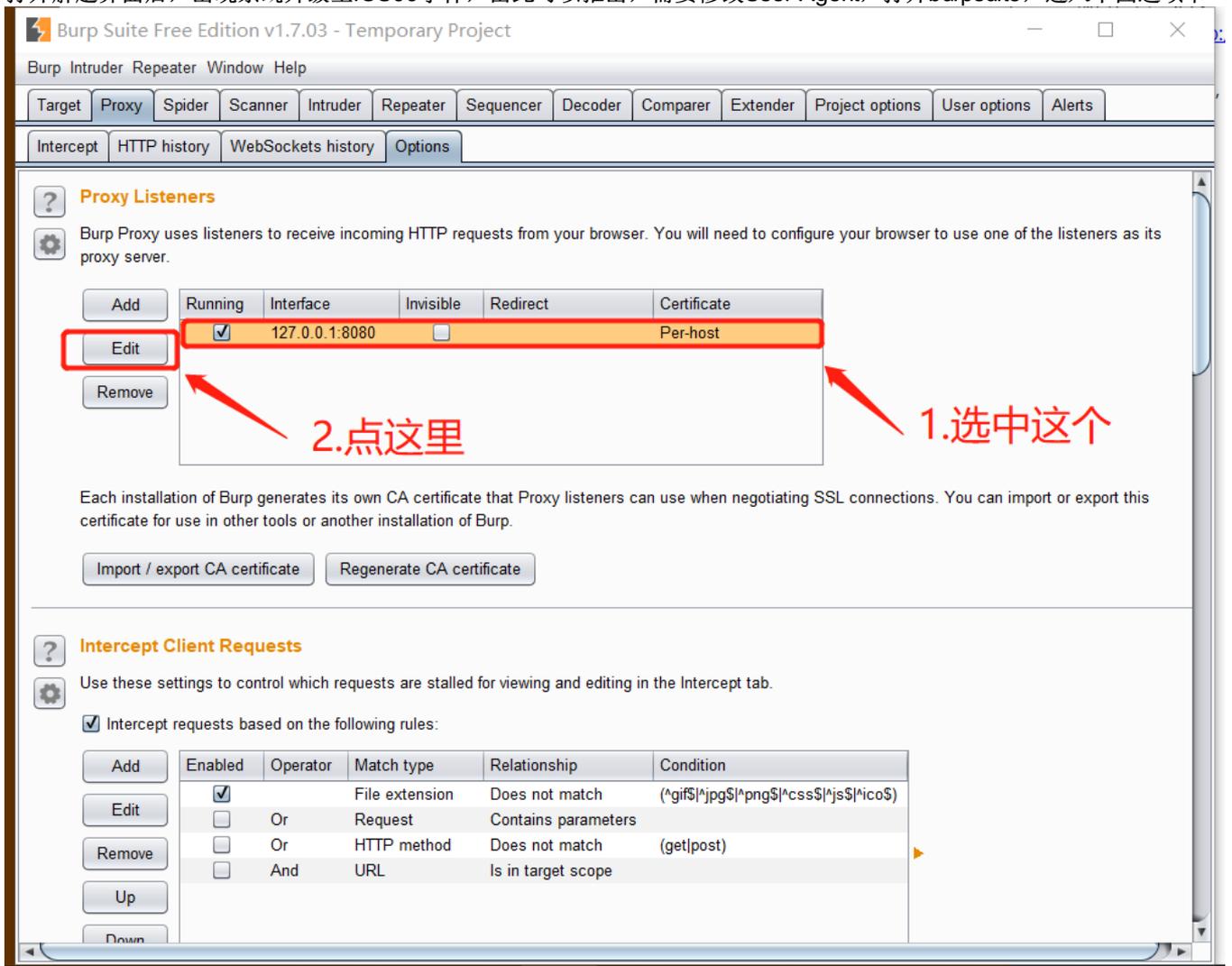


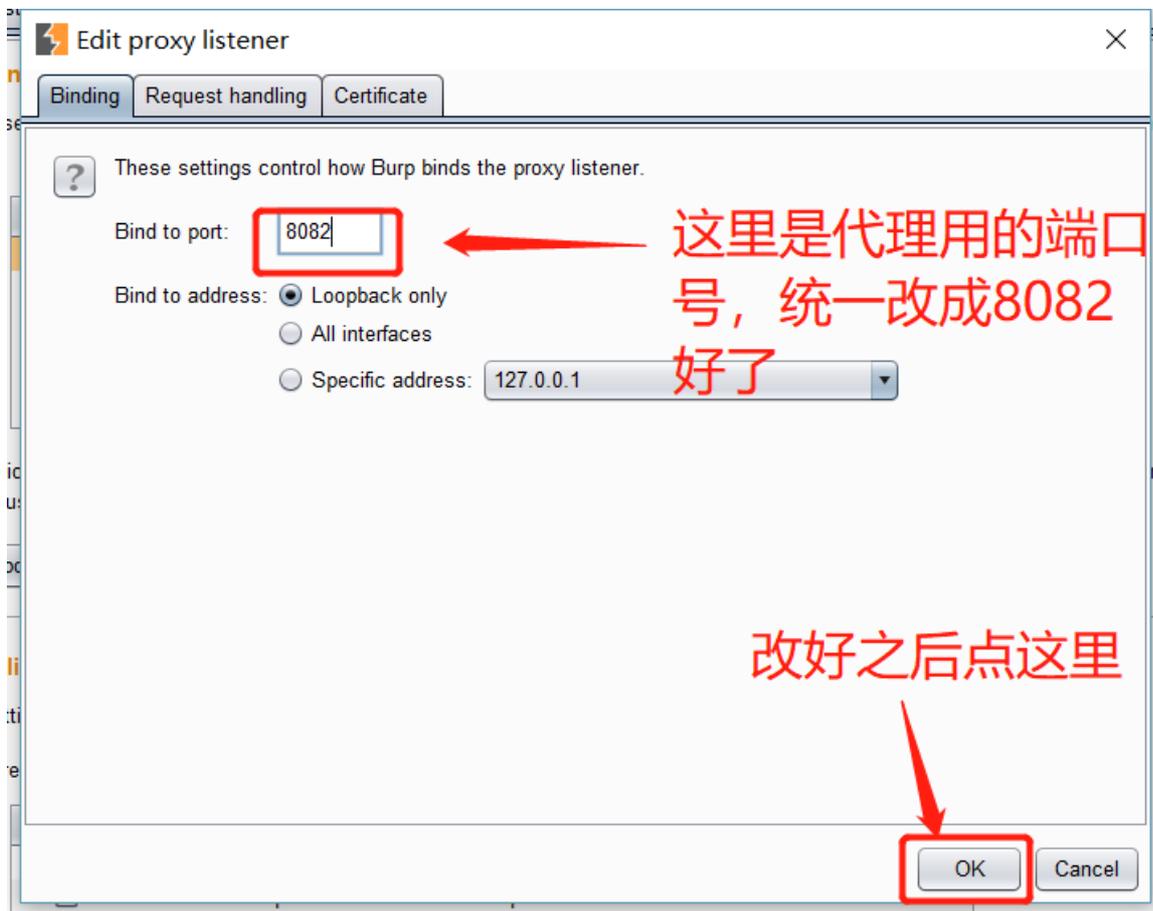
[返回目录](#)

2.2 第二题：iOS

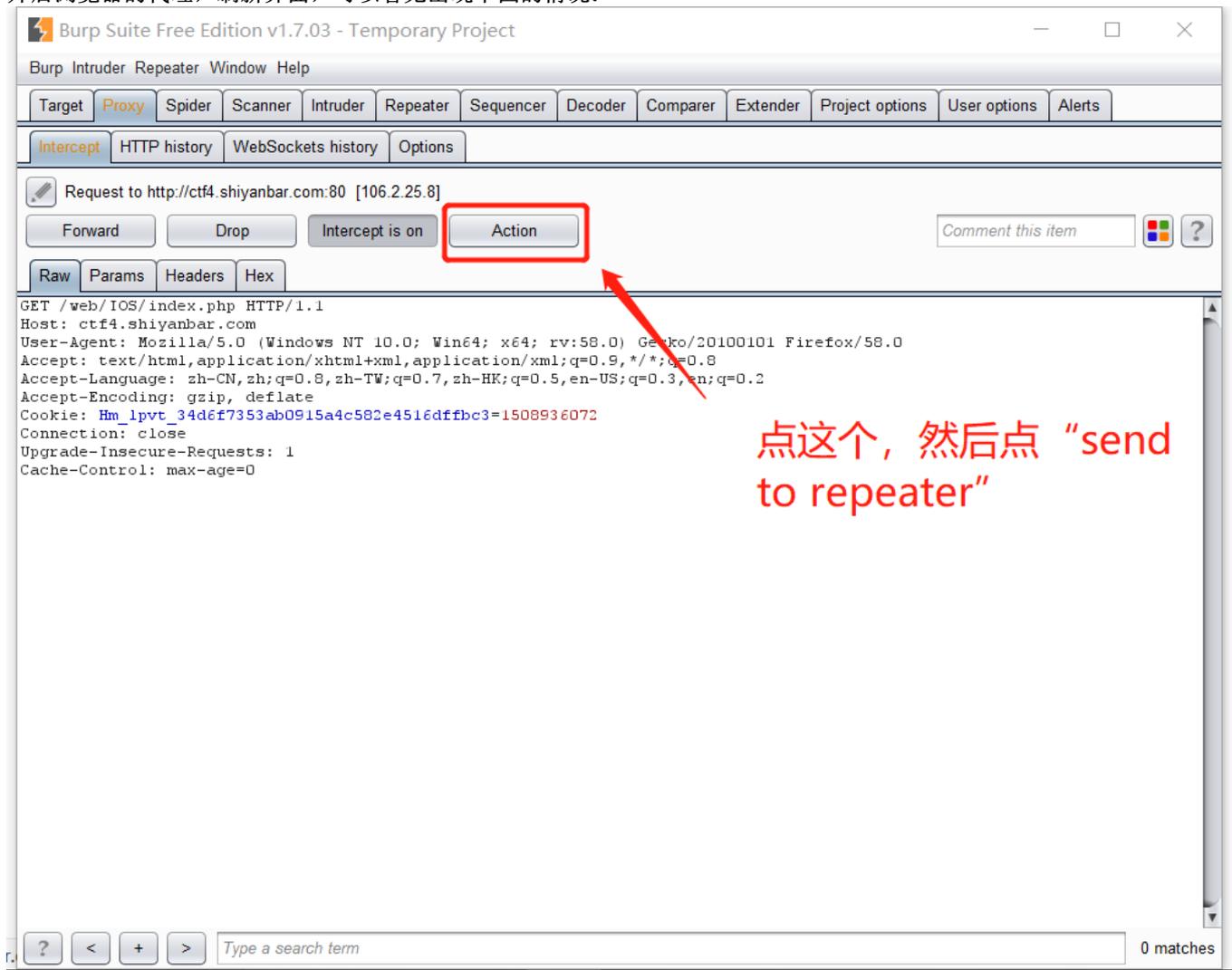
解题链接：<http://ctf4.shiyanbar.com/web/IOS/index.php>

1. 打开解题界面后，出现系统升级至iOS99字样，由此可以推出，需要修改User-Agent，打开burpsuite，进入下图选项卡

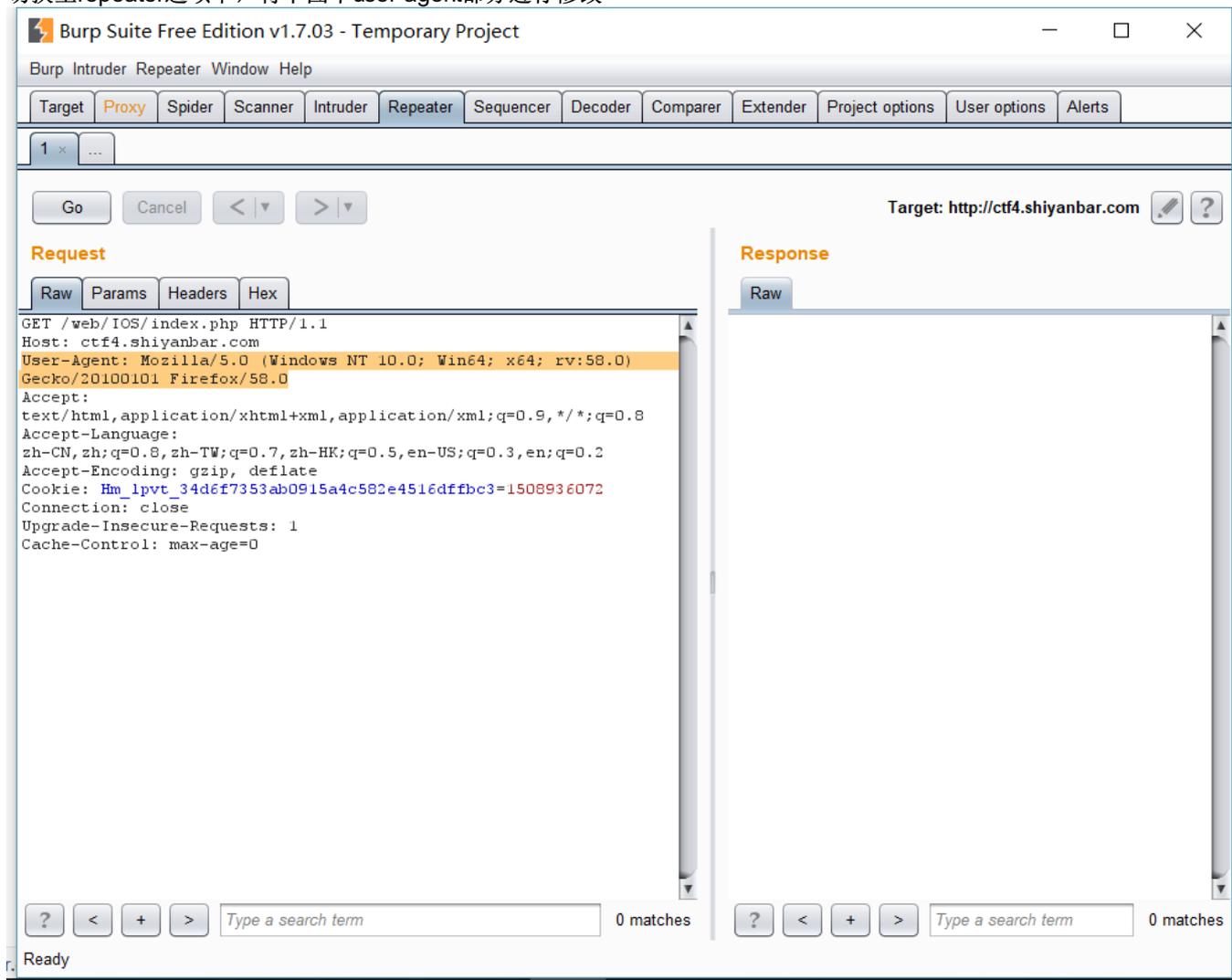




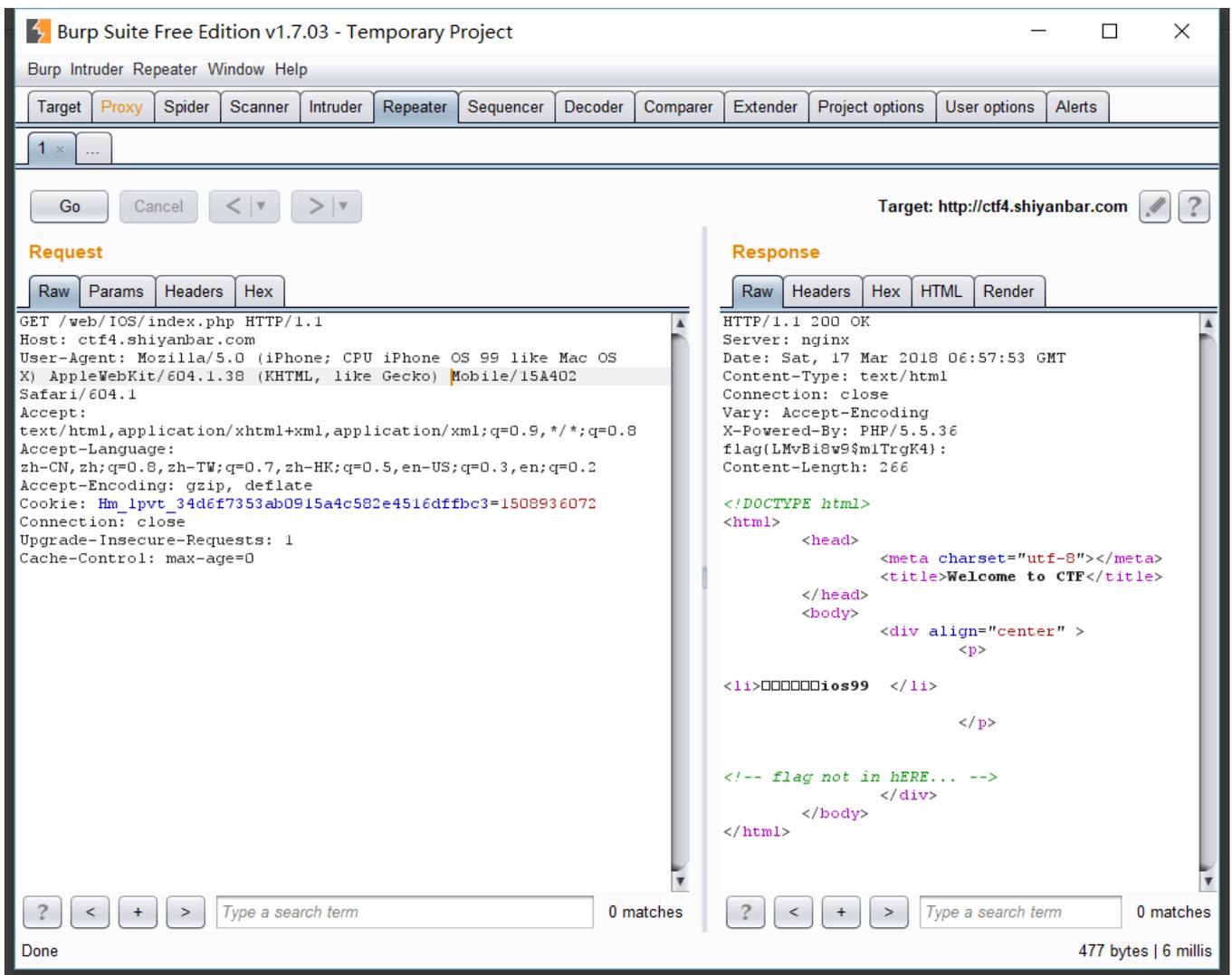
2. 然后是修改浏览器的代理设置，将ip地址和端口号设置成和上图一样的即可。
3. 开启浏览器的代理，刷新界面，可以看见出现下图的情况：



4. 切换至repeater选项卡，将下图中user-agent部分进行修改



5. 修改成下图对应位置的样子之后，点go，右半部分反馈得到flag:

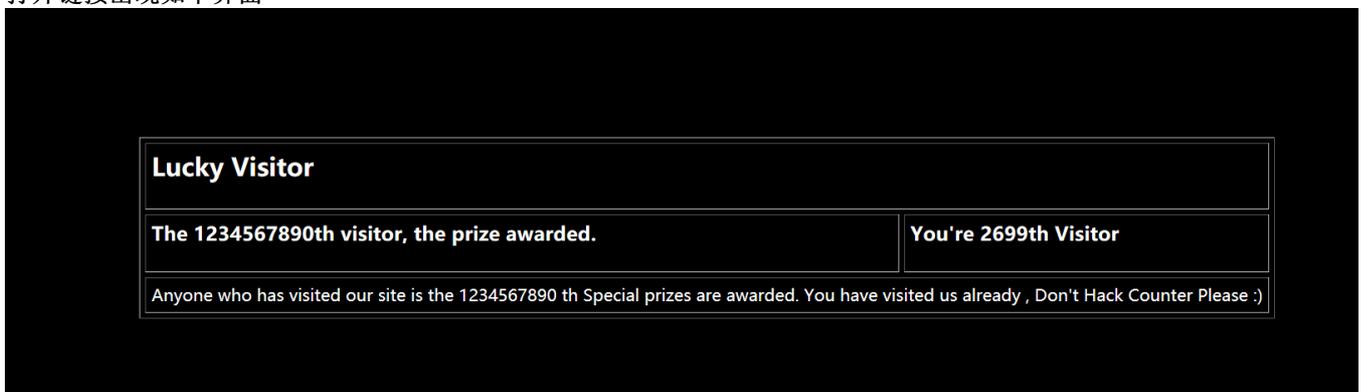


[返回目录](#)

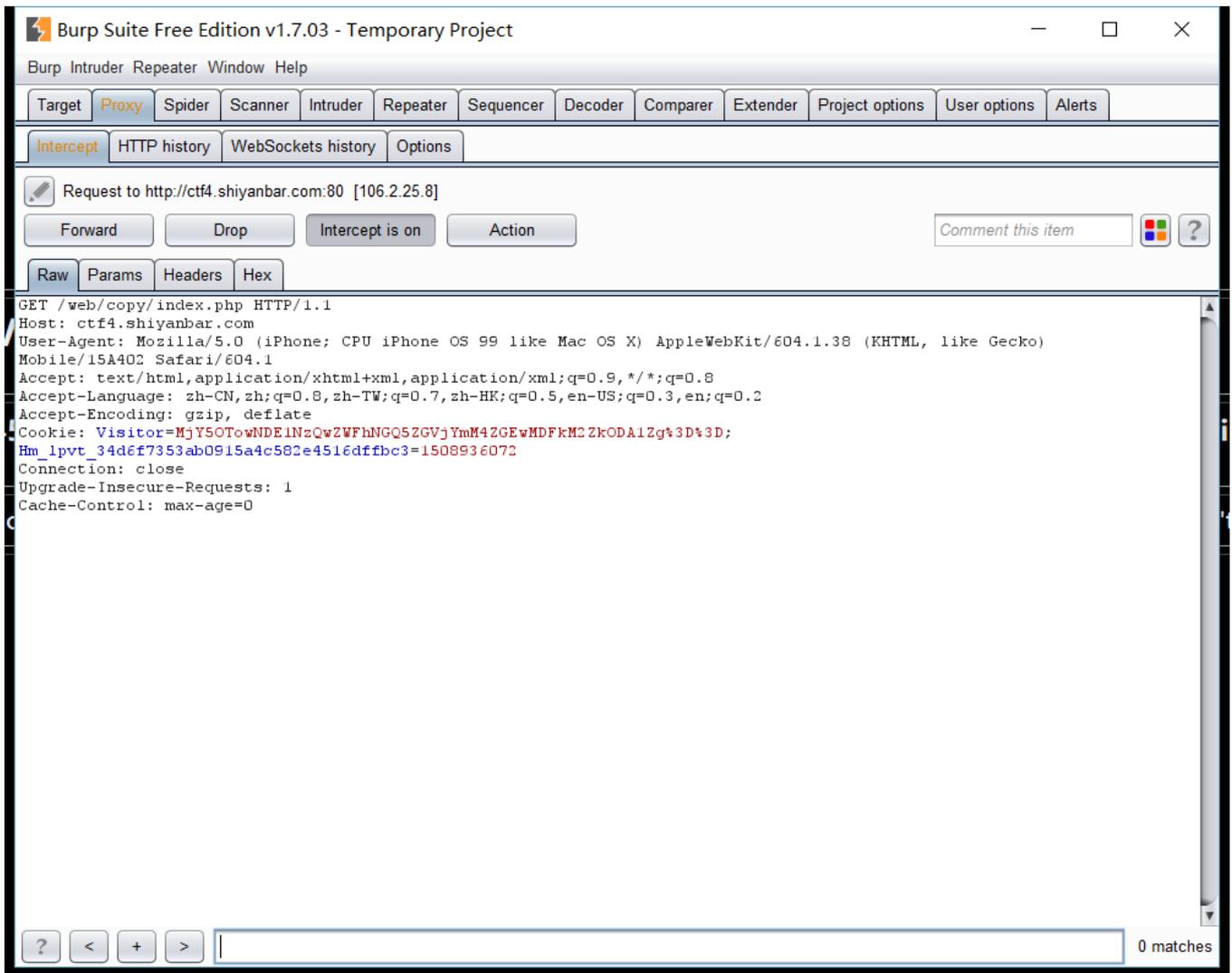
2.3 第三题：照猫画虎

解题链接：<http://ctf4.shiyandar.com/web/copy/index.php>

1. 打开链接出现如下界面



2. 根据最下面一排的提示，可以得知，要为第1234567890位用户才可以访问，尝试用burpsuite抓包



3. 可以发现在Cookie那一栏出现:

Visitor=MjY5OTowNDE1NzQwZWFhNGQ5ZGVjYmM4ZGEwMDFkM2ZkODAlZg%3D%3D;

因为%3D%3D转换之后是==, 则可以猜测Visitor=后面所跟的是经过base64加密的字符串, 对字符串进行解码, 得到2699:0415740eaa4d9dec8da001d3fd805f

其长度为32, 刚好是2699的32位小写md5编码:



4. 根据页面中出现的You're 2699th Visitor可得cookie中Visitor后的字符串格式为“base64(人数:md5(人数))”, 将1234567890进行32位小写的md5加密, 得到:

e807f1fcf82d132f9bb018ca6738a19f

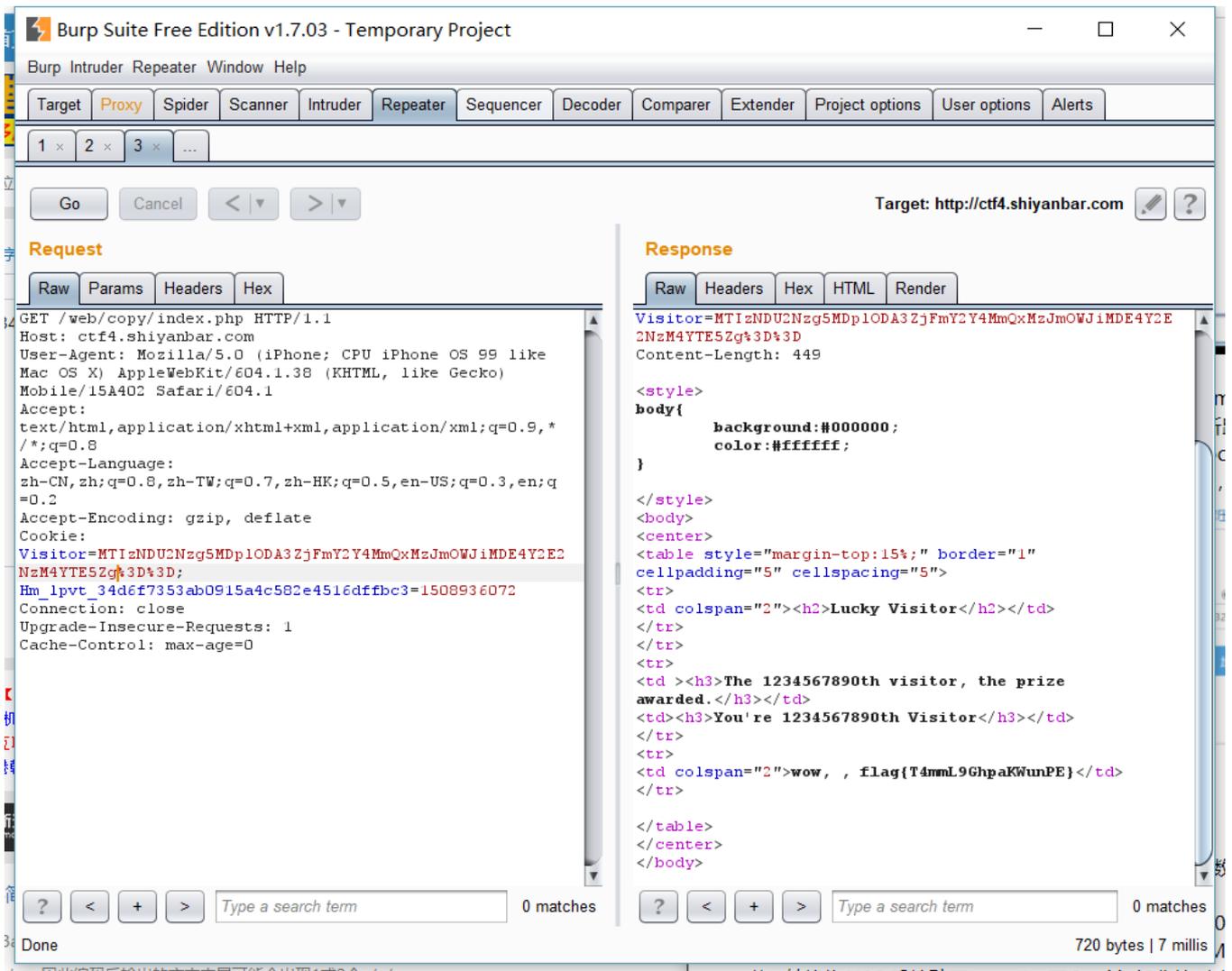
在该字符串前面加上1234567890: 构成

1234567890: e807f1fcf82d132f9bb018ca6738a19f

进行base64编码, 得到:

MTIzNDU2Nzg5MDplODAzZjFmY2Y4MmQxMzJmOWJiMDE0Y2E2NzQ5YTE5Zg==

将=转换为%3D后粘贴至repeater下Cookie部分的对应位置。点go, 得到flag:



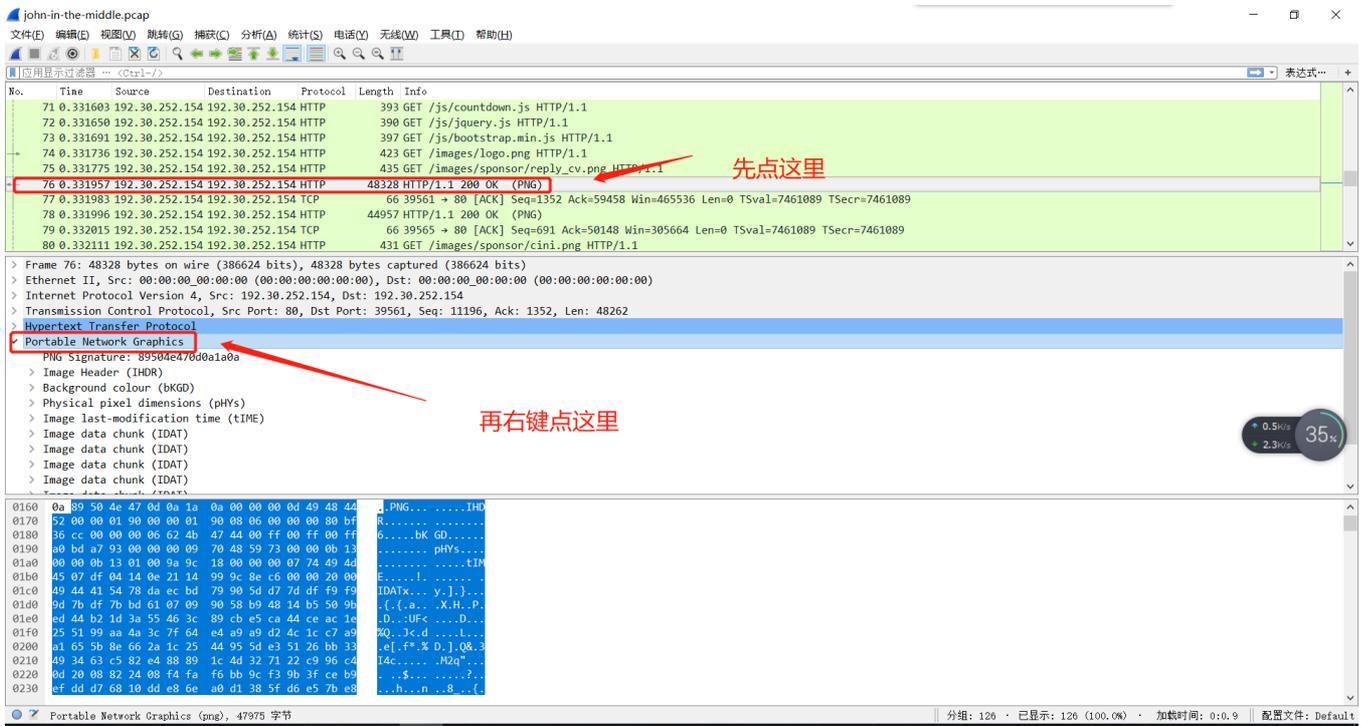
[返回目录](#)

2.4 第四题：问题就在这

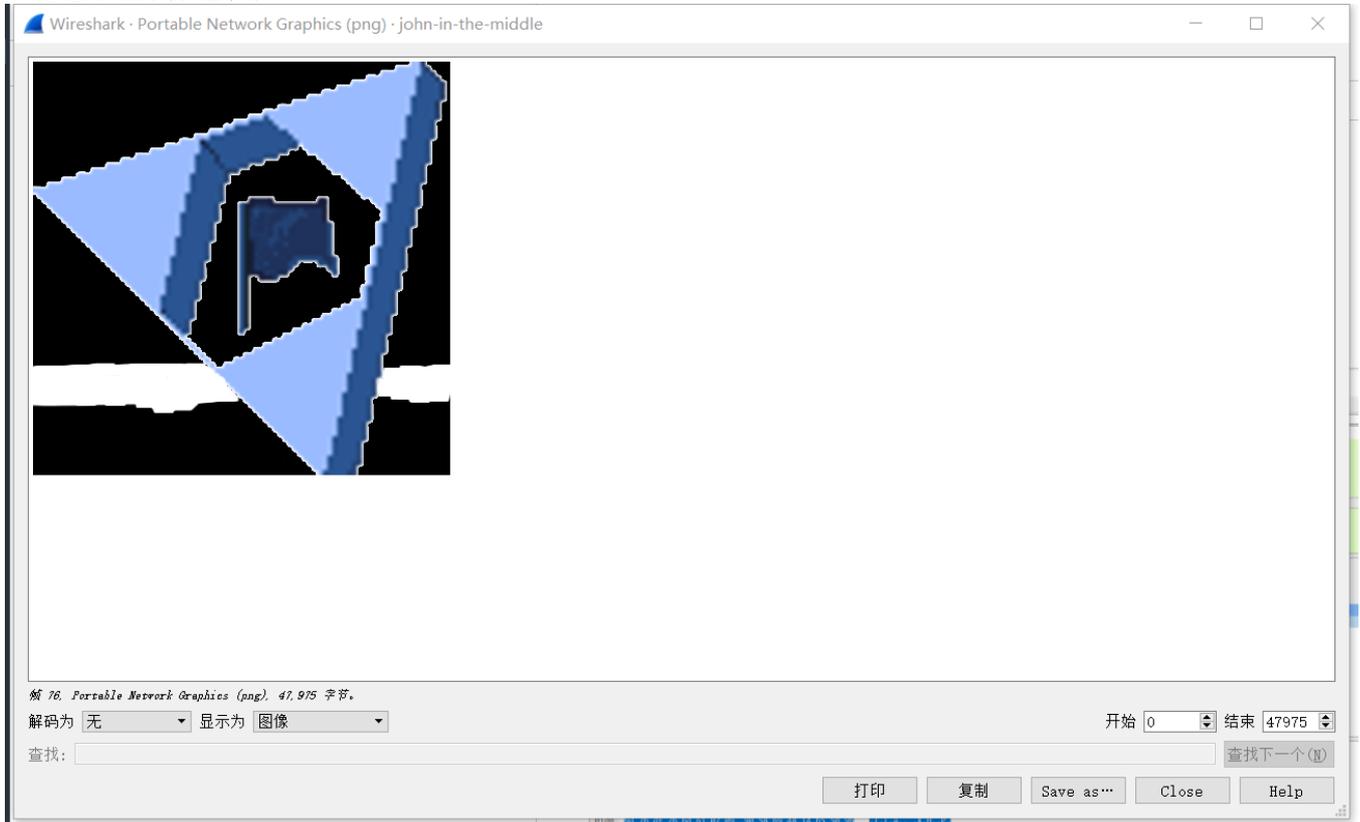
题目描述：找答案 GPG key: GhairfAvvewvukDetolicDer-OcNayd#

解题链接：<http://ctf4.shiyanbar.com/ste/gpg/john.tar.gz.gpg>

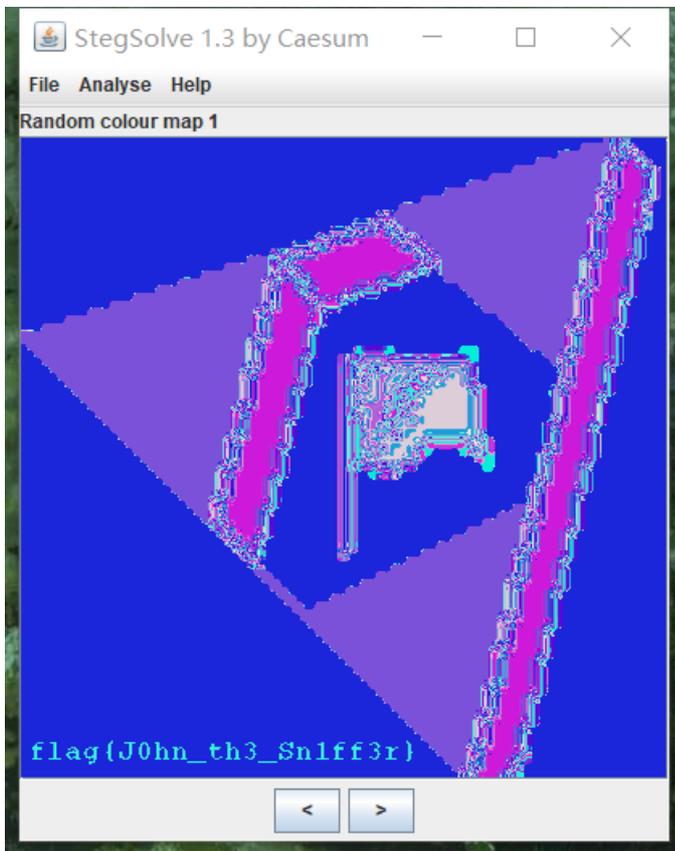
1. 点击链接后会下载一个文件，文件后缀名是gpg，使用工具<https://gpg4win.org/download.html>直接输入key解密出文件，解压后发现是一个后缀名为pcap的数据包文件。
2. 利用 wireshark打开后，



右键选择“显示分组字节”



3. 保存为png图片，用stegsolve打开，一个一个试就能得到flag了：



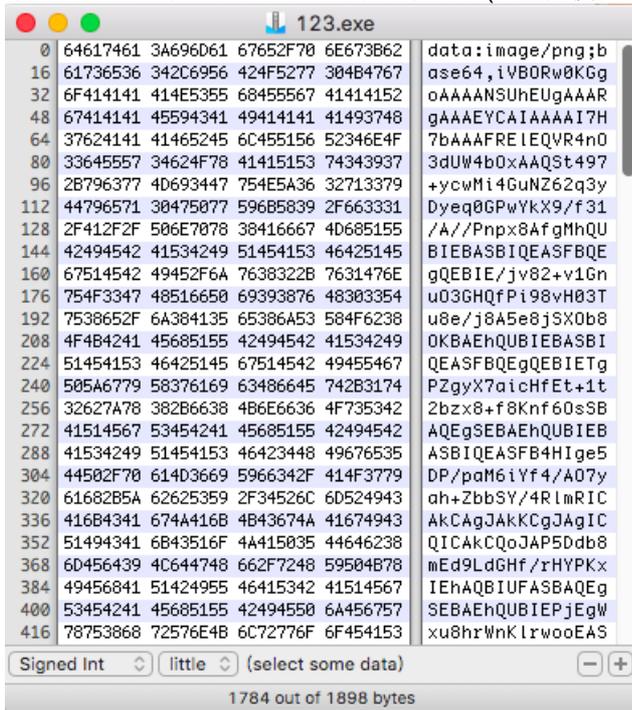
[返回目录](#)

2.5 第五题：你最美~

题目链接: <http://ctf4.shiyanbar.com/web/root/index.php>

解题步骤:

1. 点击之后是一个123.exe用16进制的编辑器(网上随便找一个)打开:



2. 药~是个base64的图片, 上base64图片解码

以下是您的 Base64 代码所解码出来的图片，右键另存为保存图片。



返回

3. 药~打开手机微信扫一扫一下：
you're beautiful~

[返回目录](#)

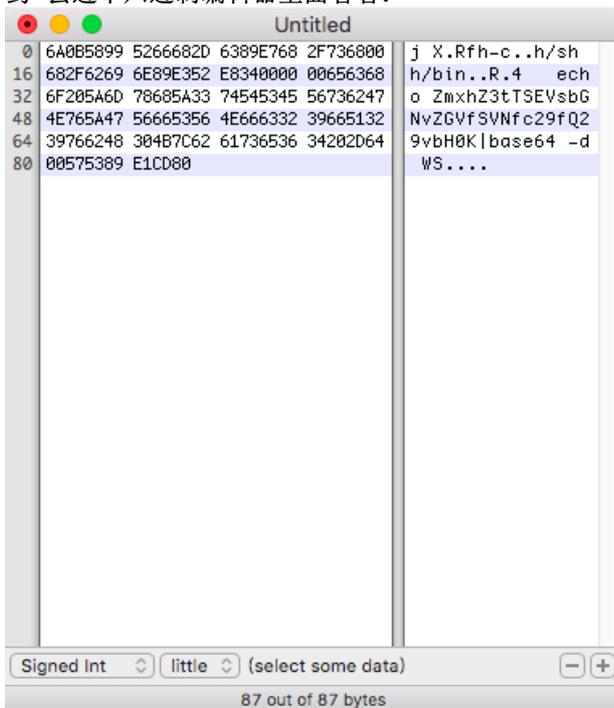
2.6 第六题：shellcode

解题链接：<http://ctf4.shiyanbar.com/re/shellcode/shellcode.txt>

1. 新弹出的界面只包含以下信息,熟悉注入的同学一看就很像shellcode:

```
\x6a\x0b\x58\x99\x52\x66\x68\x2d\x63\x89\xe7\x68\x2f\x73\x68\x00\x68\x2f\x62\x69\x6e\x89\xe3\x52\xe8\x34\x0
```

1. 药~丢进十六进制编辑器里面看看:



嗯，提取出内容：

ZmxhZ3tTSEVsbGNvZGVfSVNfc29fQ29vbH0K
真熟悉~

2. 药~base64解码:

将代码以BASE64方式加密、解密

[Base64在线编码解码GB2312](#)

[Base64在线编码解码UTF-8](#)

[PHP加密/解密](#)

请输入要进行编码或解码的字符：

```
ZmxhZ3tTSElcode_IS_so_Cool}
```

解码结果以16进制显示

Base64编码或解码结果：

```
flag{SHEllcode_IS_so_Cool}
```

3. so~cool !

[返回目录](#)

转载于：<https://www.cnblogs.com/blackay03/p/8590877.html>