能力验证题目 1-10题答案

（其中第七题没看明白题目（汗））

第一题：



思路：Chrom浏览器输入：view-source:http://120.24.86.145:8002/web2/

结果如下：

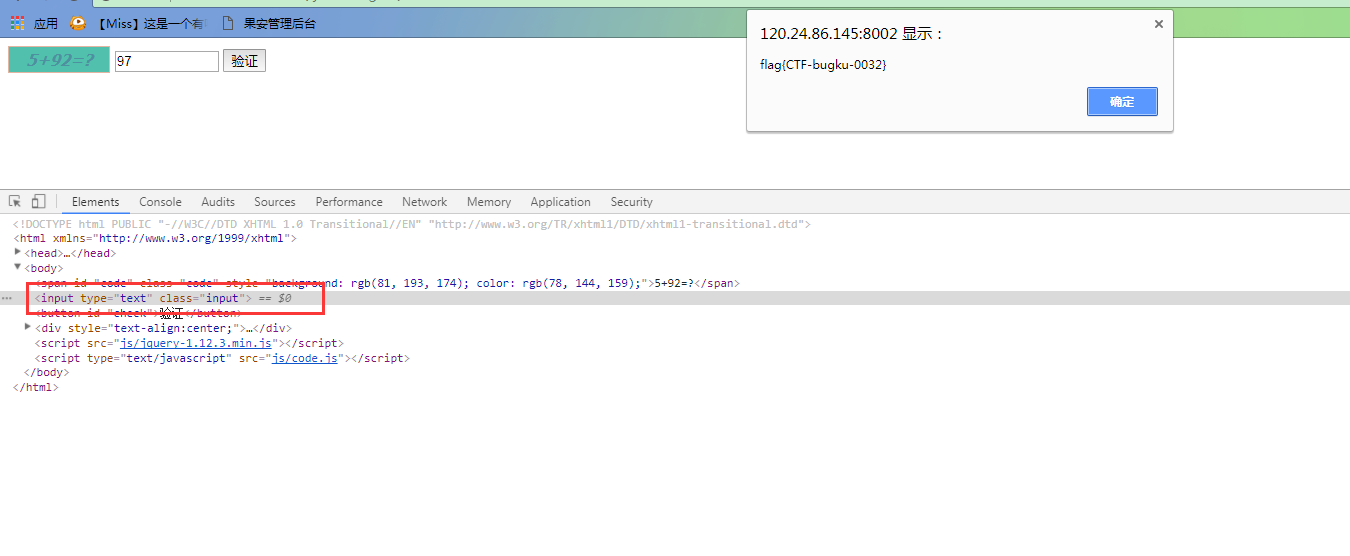


第二题：

思路：

方法1：把input 中的length去掉

结果：

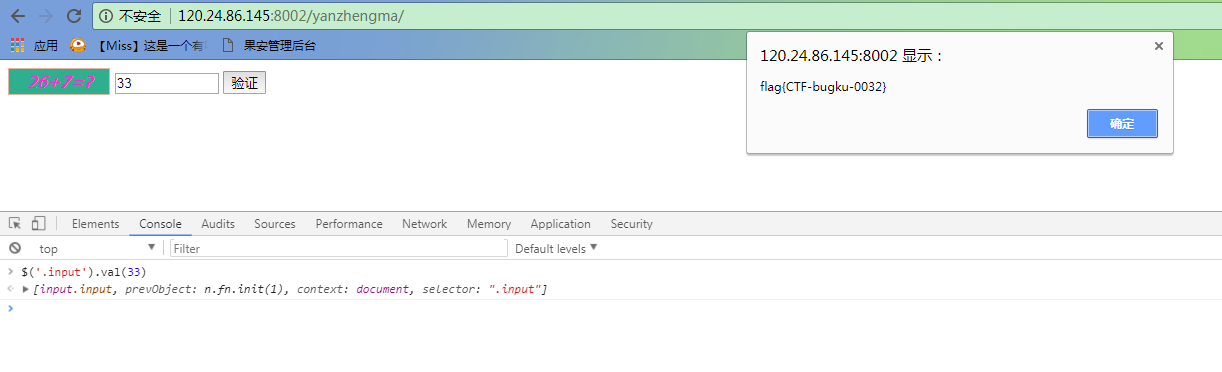


方法2：

控制台写js直接给input赋值

$(‘.input’).value(‘图片的数字和的值’)

结果：

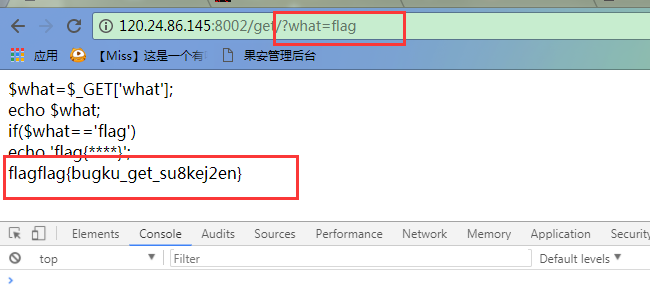


第三题：



思路：网址后面输入?what=flag

结果：



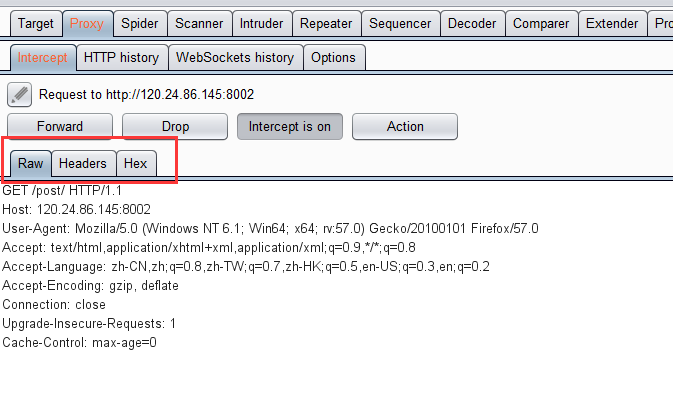
第四题：



思路：通过火狐的RESTer 修改提交方式为post，添加body参数 what=flag。

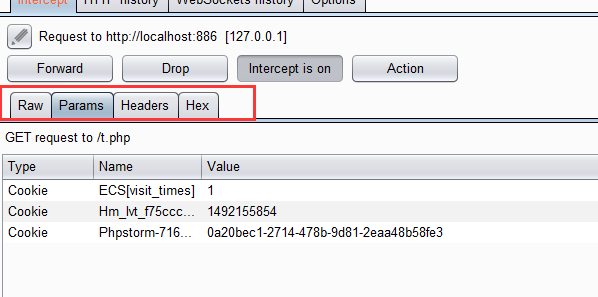
碰到问题：有时候提交不会显示 flagflag{bugku\_get\_ssseint67se}， 具体原因不详。

还有使用 BurpSuite抓包改post提交，居然没有找到Parma选项，（主要针对这个http://120.24.86.145:8002 这个ip，而我本地的localhost是有params选项的）如图：



（图4.1 <http://120.24.86.145:8002> 没有params选项）

抓其它包时候是有params选项的，如下图



（图4.2、本地localhost有params选项，请求百度网址也是有params参数）

最终使用RESTer结果如下：

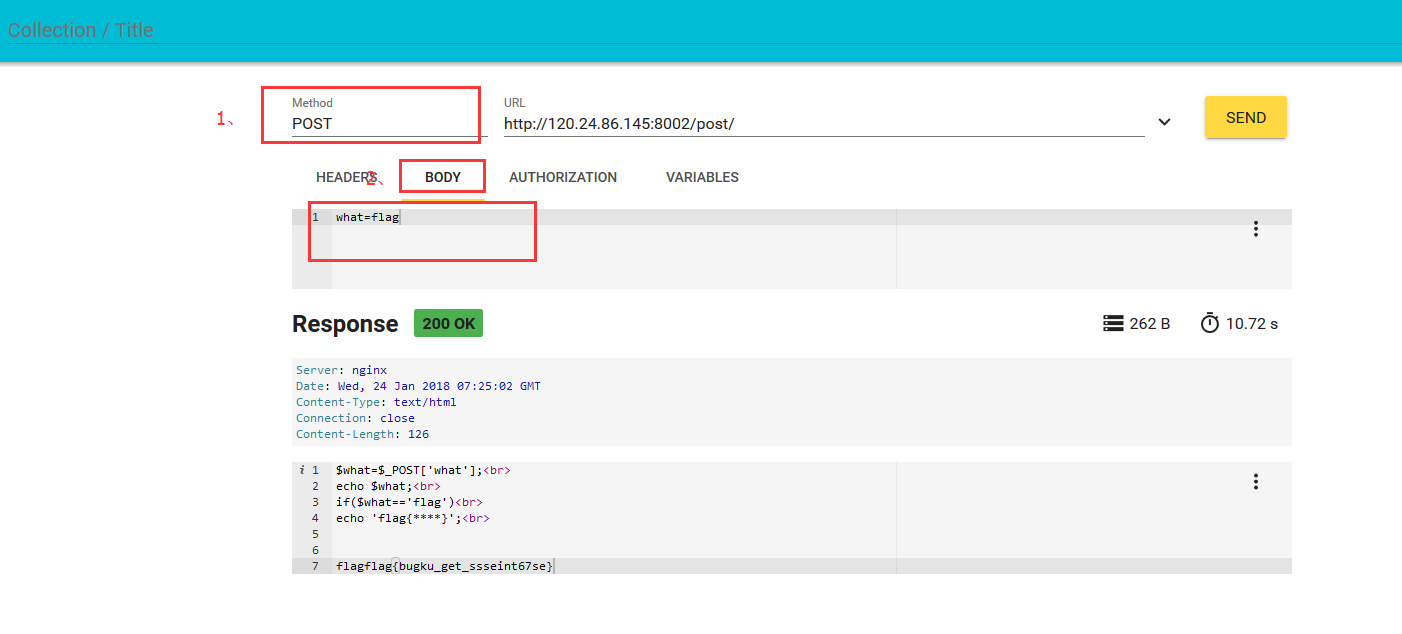


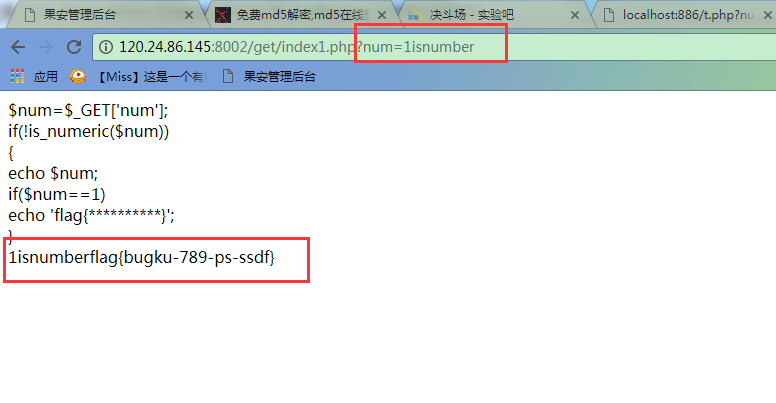
图4.3

第五题：



思路：网址后面输入 ?num=1xxxxx (第一个为数字，后面加字符串)即可

结果如下：

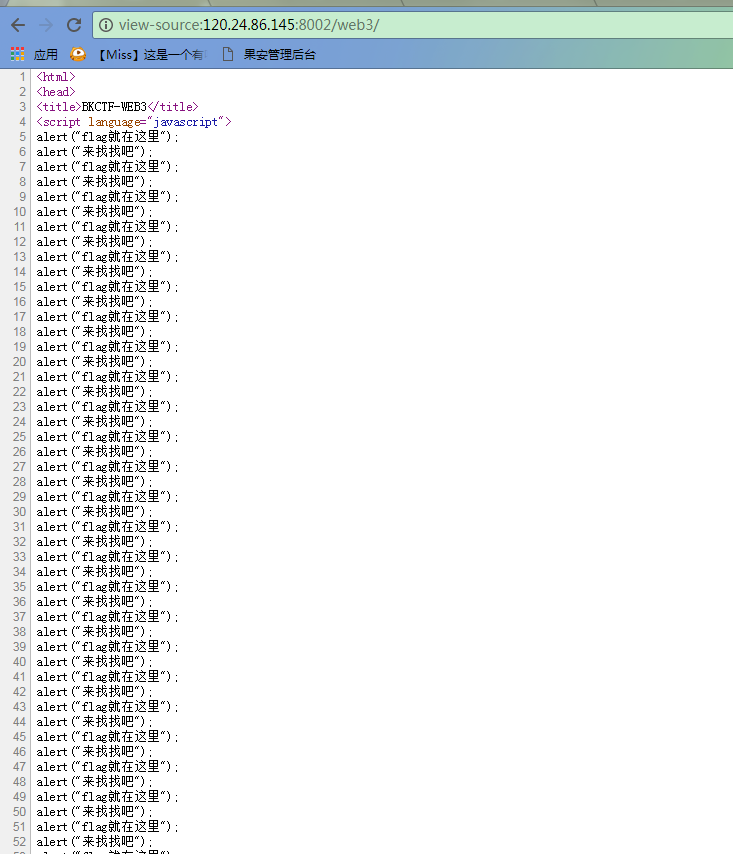


第六题：



思路：使用chrom浏览器在网址前面输入 view-source:http://120.24.86.145:8002/web3/ （view-source:url网址）即可查看源码

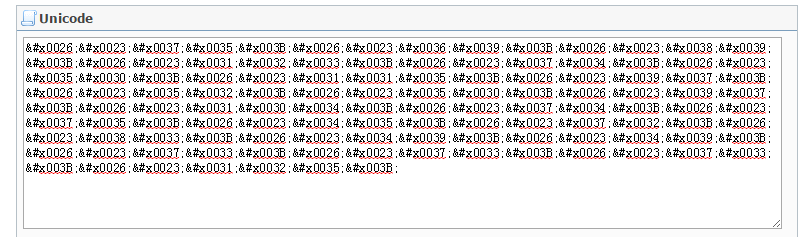
结果：



找到



然后进行Unicode编码结果如下：（此处不懂是啥）



第七题：

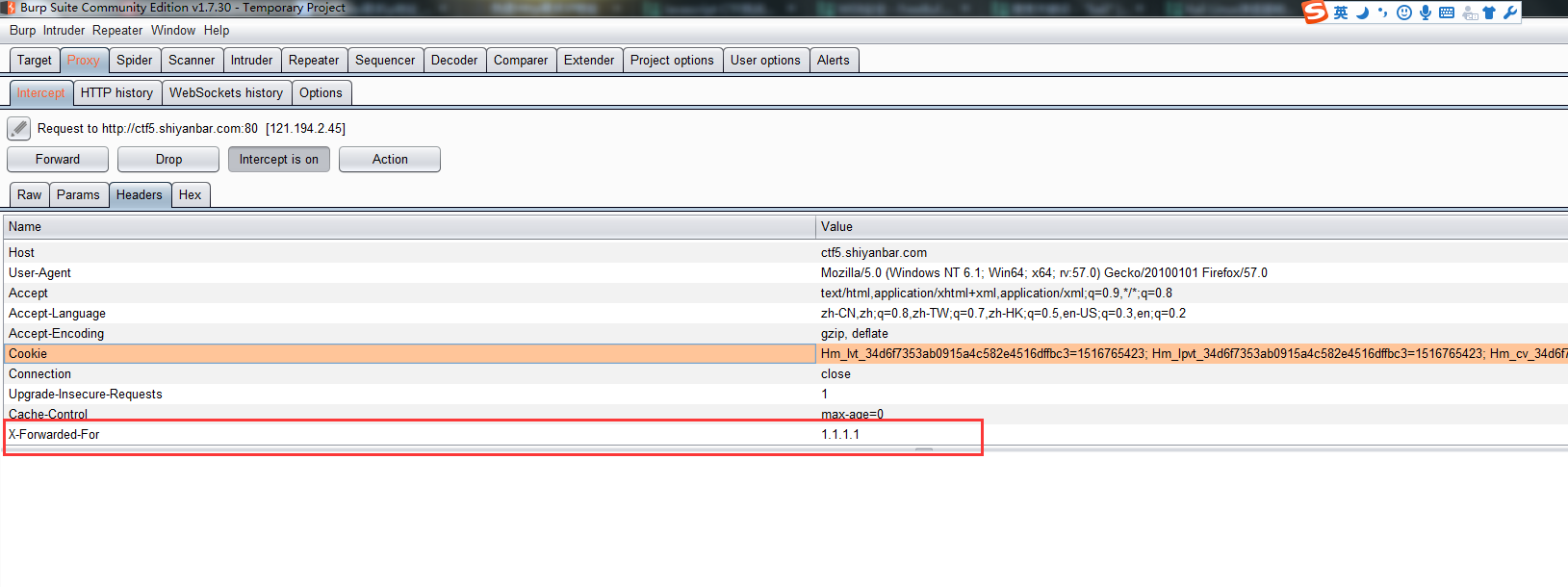


题目没看明白（汗）？？

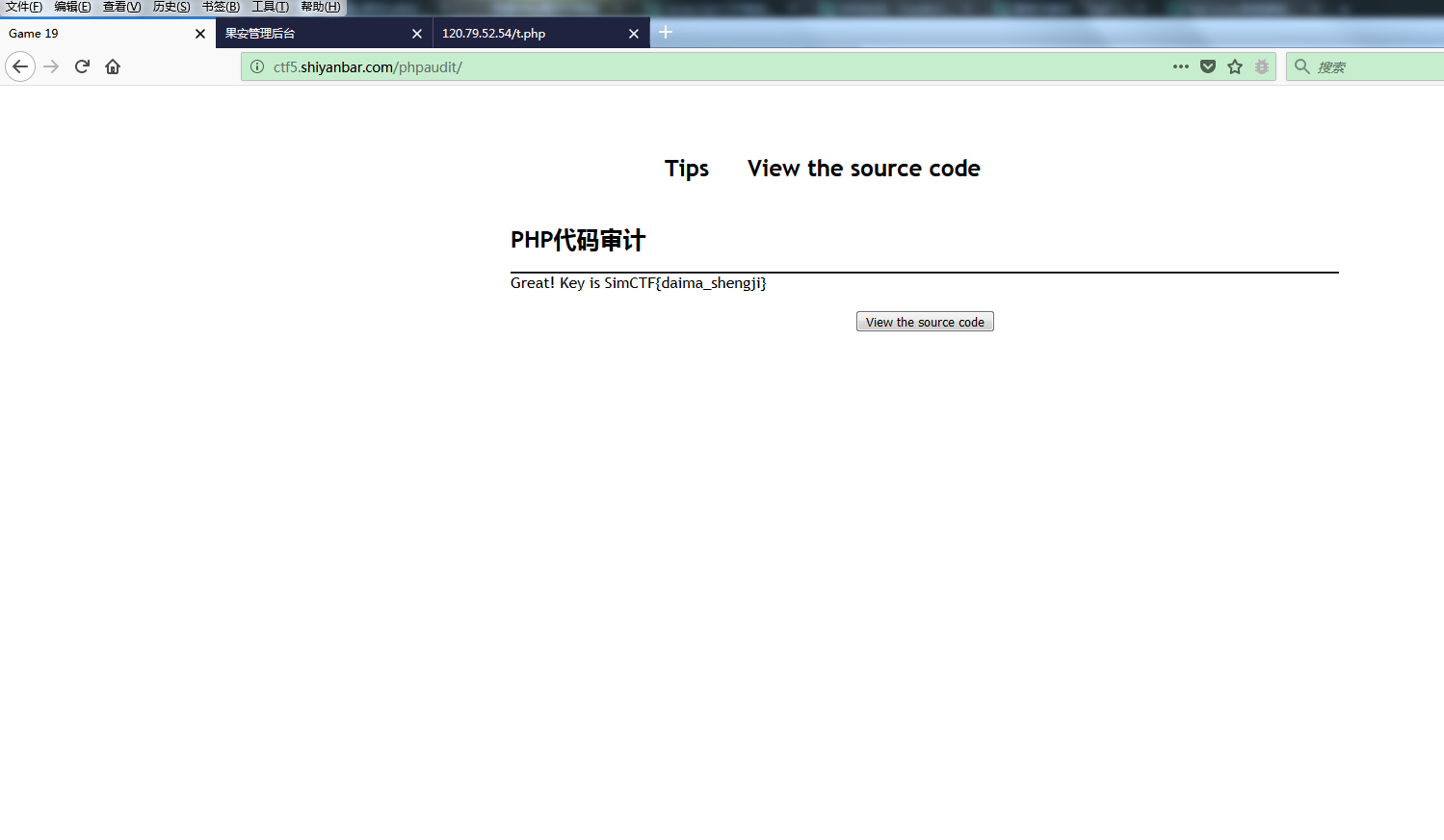
第八题：



思路：使用BurpSuiteCommunity添加 X-Forwarded-For 修改 ip为 1.1.1.1 请求头



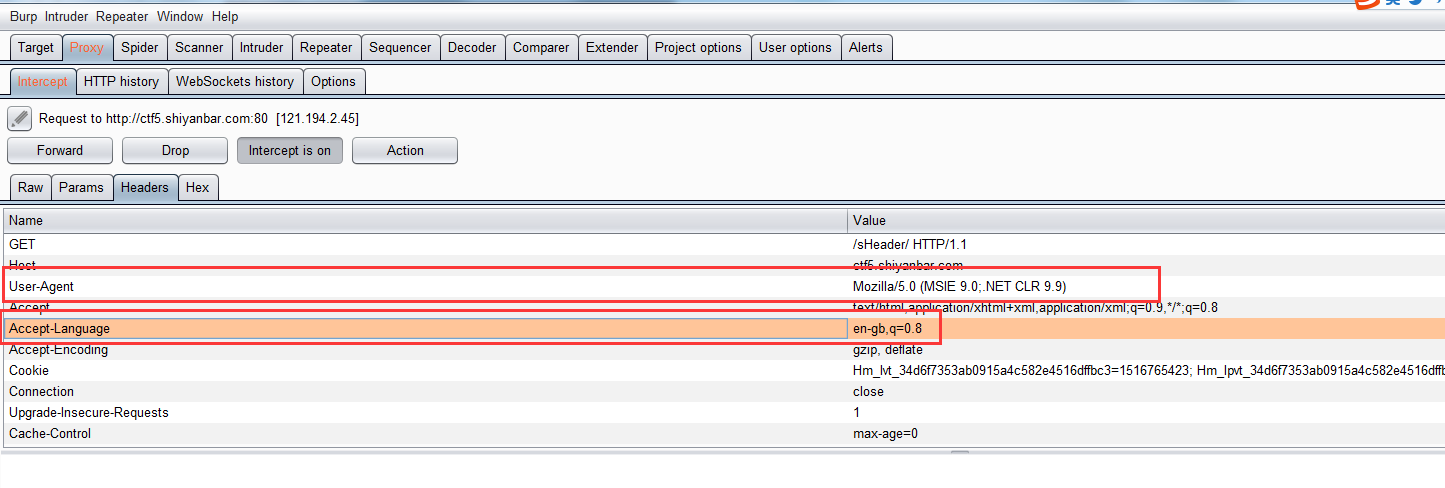
结果如下：



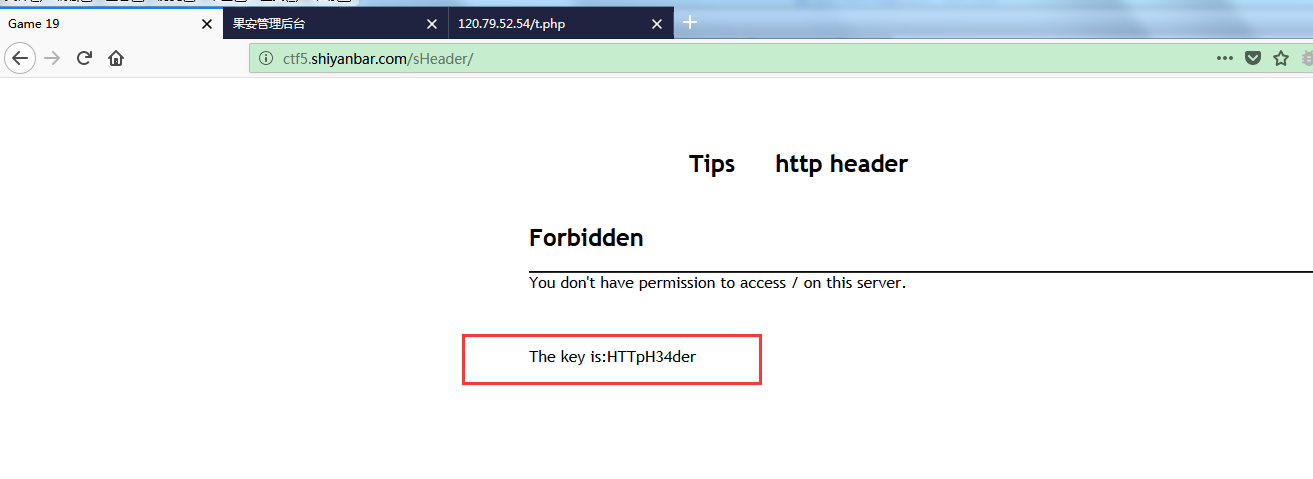
第九题：



思路：修改两处请求头，user-agent,accept-language如下图



结果：



第十题：



结果：在console中粘贴代码，有弹窗信息

