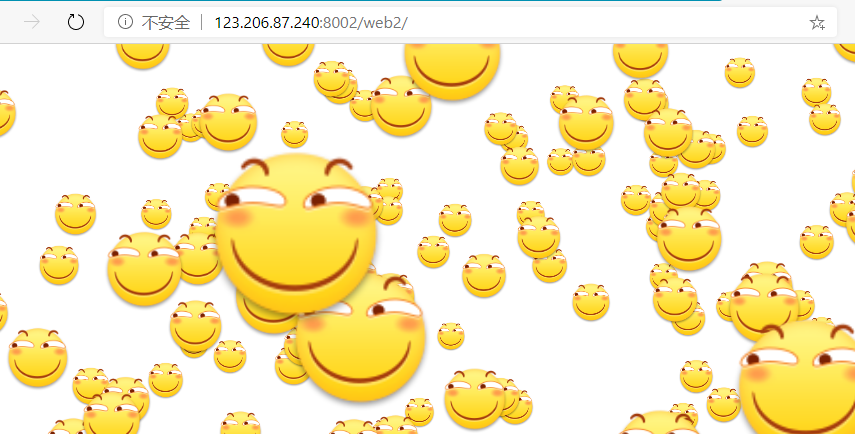
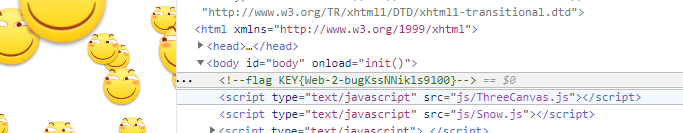
**20200307作业——CTF基础训练**

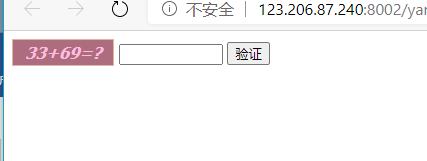
**Bugku—web篇**

1滑稽 第一题链接：http://123.206.87.240:8002/web2/

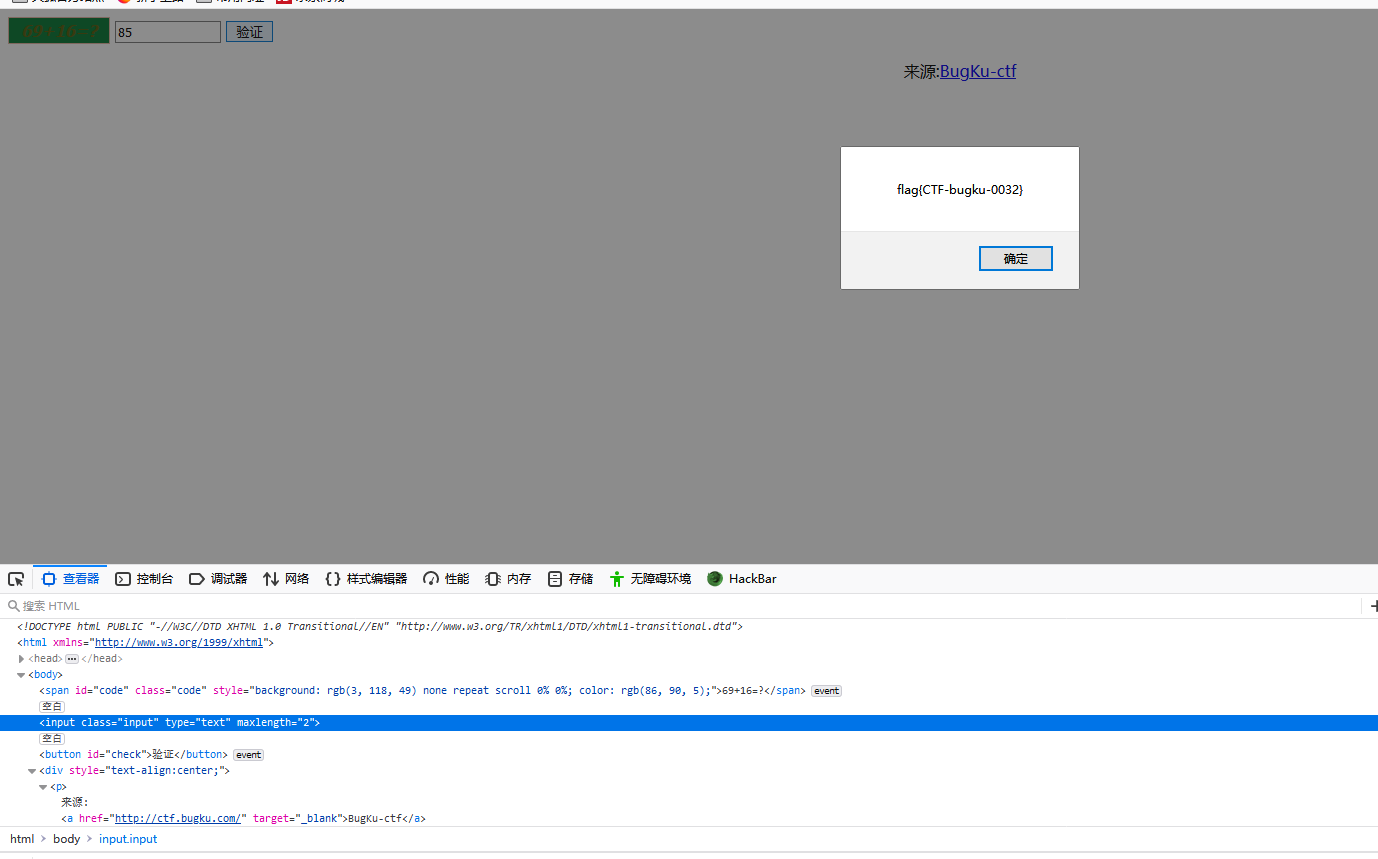
点击进去发现是一个满屏滑稽的页面一个参数都没有

这个时候就可以利用鼠标右键查看网页的源码了里面可能会有一些意想不到的东西,源码里面就展示网页的flag

2、计算器 地址：<http://123.206.87.240:8002/yanzhengma/>

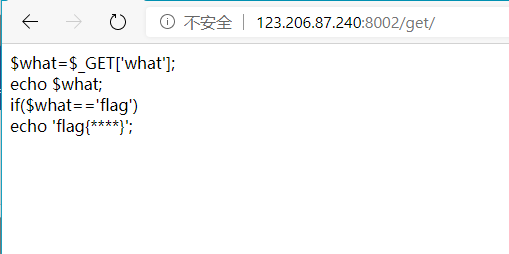


点开网页发现是一个简单的计算源码前面是xx+xx后面是要你输入的值，经过计算将值输入发现该输入框只能输入一个数字，打开开发工具，找到管理输入框位数的函数将后面的1改为2再次输入正确值得到flag

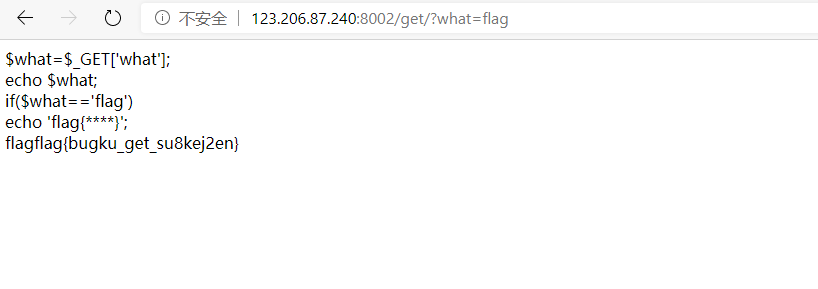


3get请求 http://123.206.87.240:8002/get/

打开网页发现已经给你展示了源码，源码是一个get请求包的形式，

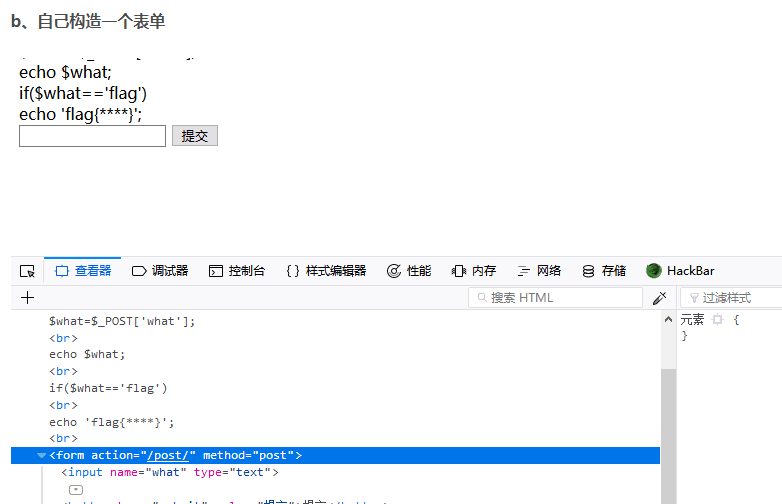


通过判断发现其中一段是$what=flag这一句就是一个判断当what=flag的时候即输出flag，因为其是一个get请求包形式，所以在搜索框自己给what赋值就好了，即？what=flag，所以到这个时候该网页的flag已经显示出来了



4post请求 <http://123.206.87.240:8002/post/>

这一题和上一题大致相似，但是不同的就是上一题是用get的显示明文的在搜索框窗，传输的这一题是一个post的请求包，由于post包与get唯一的区别就是从带有 POST 方法的表单发送的信息，对任何人都是不可见的（不会显示在浏览器的地址栏），并且对发送信息的量也没有限制。所以我们在网页代码中加入自己构造的表单代码，输入flag，提交即可得到flag的值。



表单格式：

<form action="/post/" method="post">

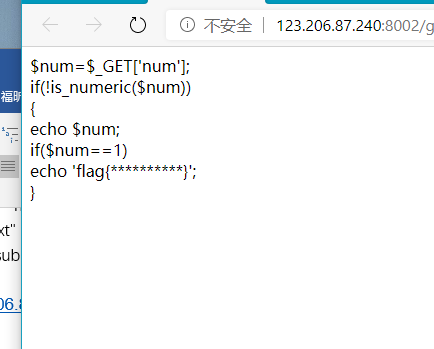
<input type="text" name="what">

<button type="submit" value="提交">提交</button>

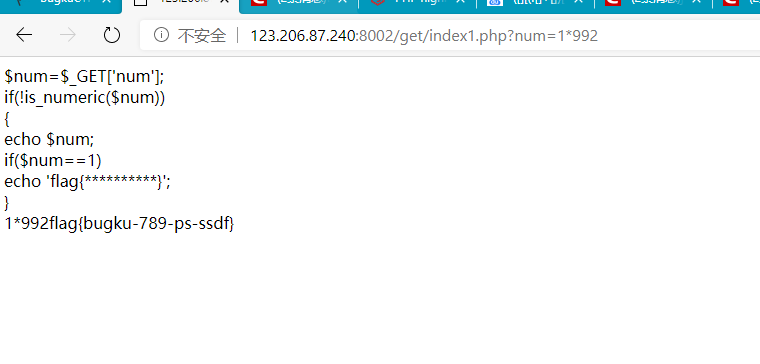
</form>

5、矛盾<http://123.206.87.240:8002/get/index1.php>

分析源码发现

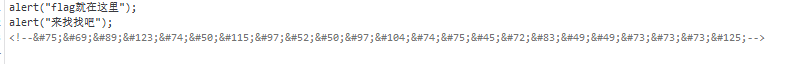


这是利用get传参的即当num==1变量num==1时输出一个flag但是前面还有一个判断条件即num不等于数字，这个时候想到的就是num做一个运算最后的结果为1当然就可以输出了我们就给num=1\*233，这样就输出一个flag了



6、flag就在这里快来找找吧 <http://123.206.87.240:8002/web3/>

打开后发现是一个无线循环的2个对话框，点击打开源码发现源码最末端有一个这样的



字符串，百度了一下发现是一种加密方式利用HtmlEncode解码，即可得到flag的值。



7、听说把 flag.baidu.com 解析到123.206.87.240 就能拿到flag

由题意可知，只要把123.206.87.240解析成为flag.baidu.com就能拿到flag所以这一关改win10下的host文件就可以了，改完访问域名得到了flag

8、你必须让他停下地址：<http://123.206.87.240:8002/web12/>

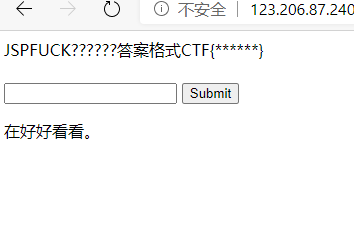
打开网页发现是一个不断刷新的网页这个时候你肯定不能看到他的网页源码，打开bp进行抓包发现其中有一条是



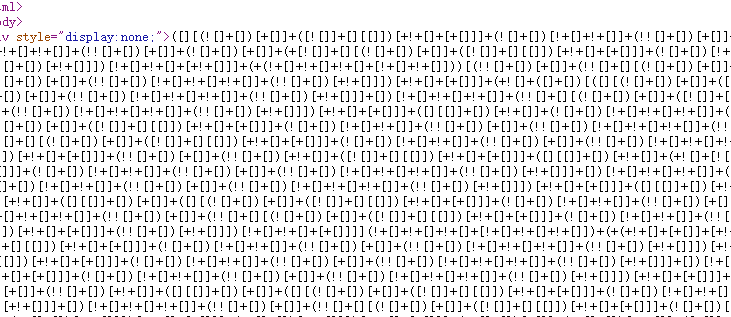
所以flag就在这里

9、JSPFUCK??????答案格式CTF{\*\*} <http://123.206.87.240:8002/web5/>

打开网页发现是一个搜索框输入123反馈



打开其源码发现一长串



猜想是一种编码方式，打开百度搜索其中一段得出是一种单浮点数，只需丢入控制台，输出便得到了flag