Bugku-web题Writeup（持续更新）

原创

秋风瑟瑟... 于 2020-02-18 23:40:26 发布 420 收藏

文章标签： web 安全

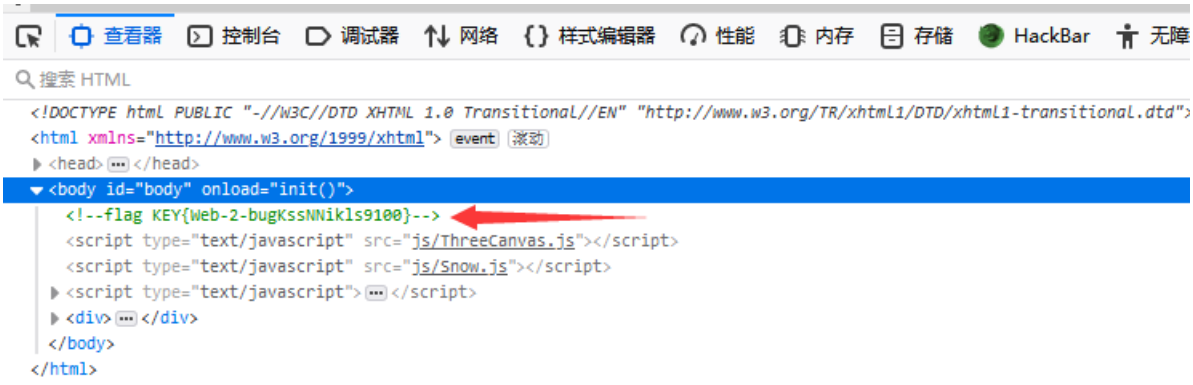
本文链接：https://blog.csdn.net/qq_45628145/article/details/104384586

Bugku-web题Writeup

这里会持续更新**bugku练习平台**上面web题的*writeup*，我也是个新手，如果有什么不对的地方，欢迎大家指出，如果大家觉得写的不错的话，别忘了点个赞哦！

1.Web2

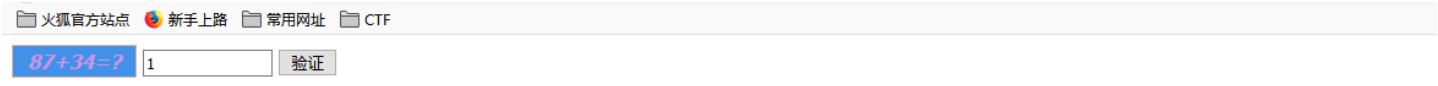
打开之后，一堆滑稽脸在动，按照惯例，f12，发现flag就在源码中。



于是得到flag。

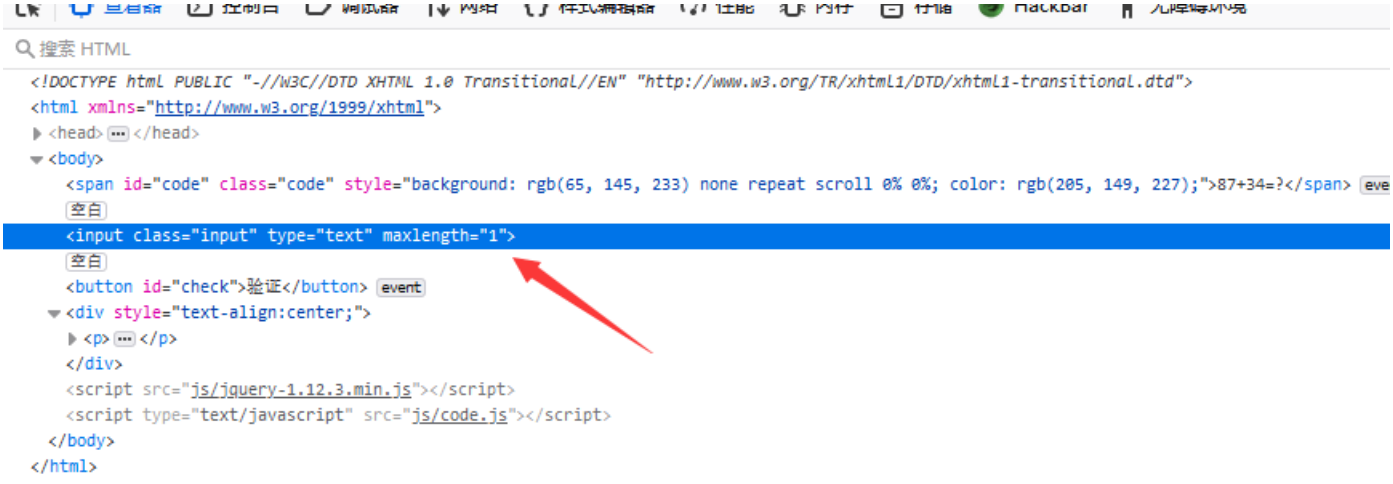
2.计算器

打开之后，发现是一个加法题。

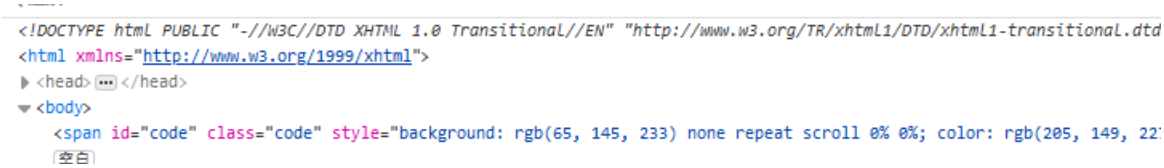


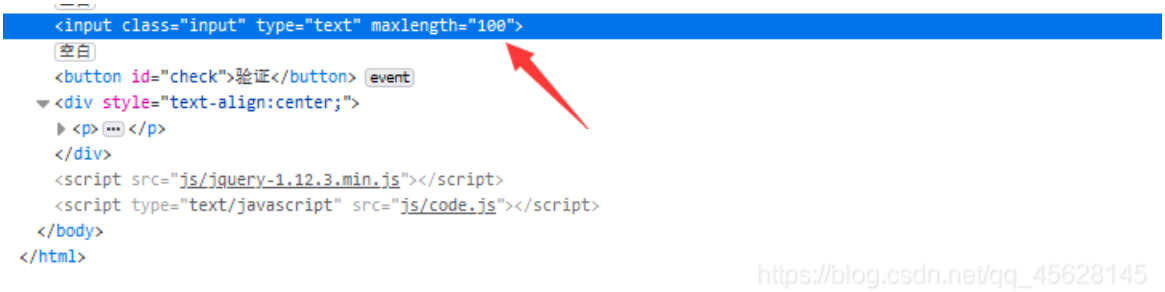
来源:BugKu-ctf

准备输入答案121的时候，发现只可以按1个数字，于是f12，发现有长度的限制，只能输入一个数字。



于是修改限制。





重新输入答案，进行验证，得到flag。

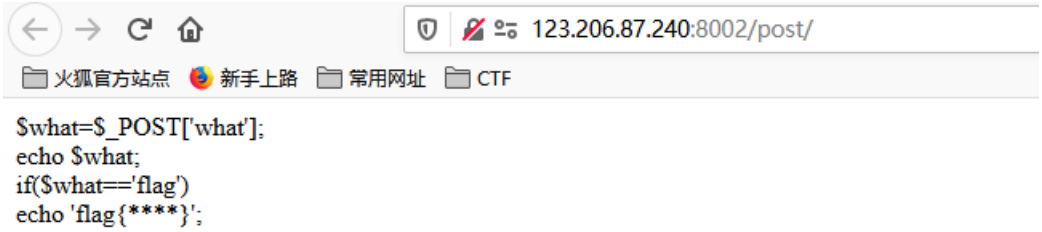
3.web基础$_GET

打开之后，发现一段php代码。

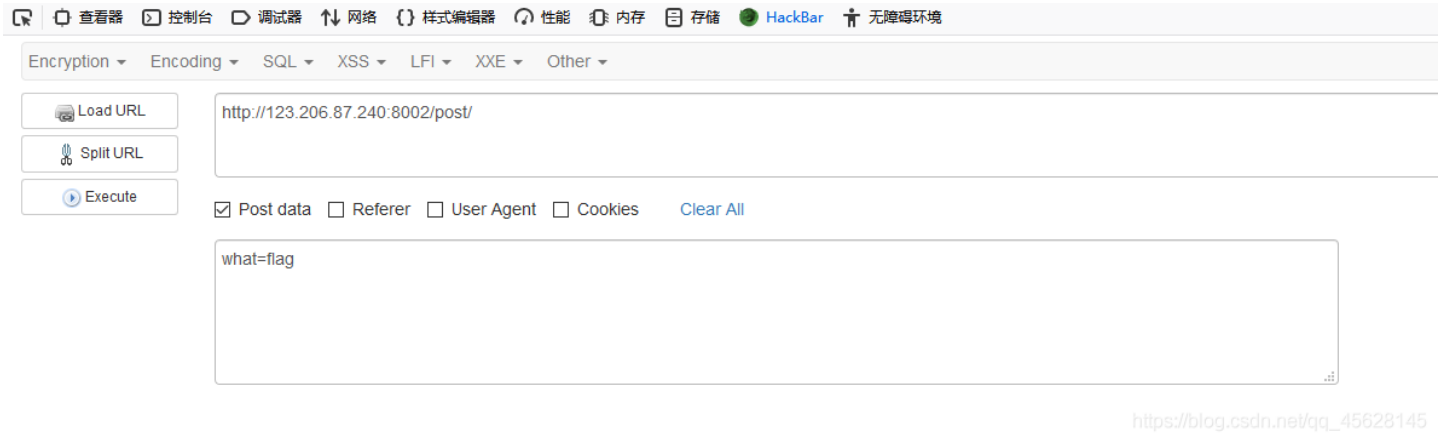
让我们用GET方法获取what的值，当what=flag时，输出flag，于是直接构造?what=flag，得到flag。

4.web基础$_POST

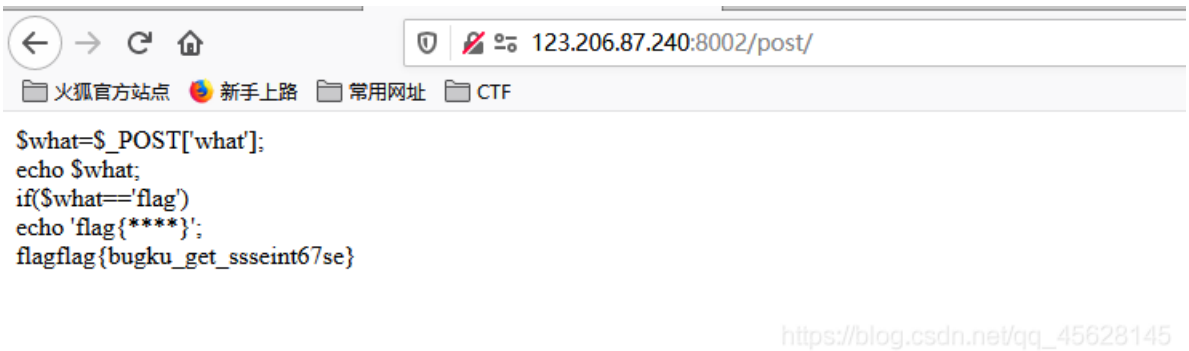
打开之后，发现一段php代码。



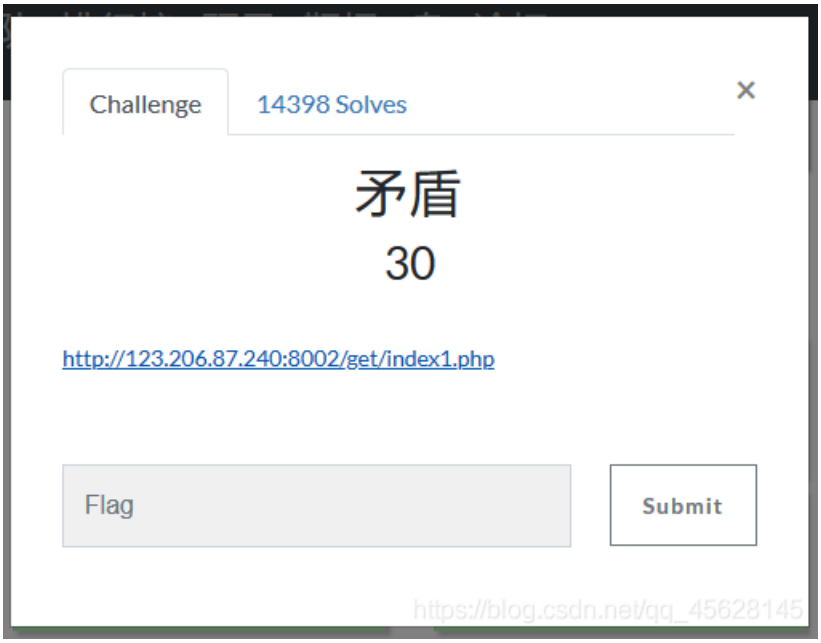
让我们用POST方法获取what的值，当what=flag时，输出flag。
于是打开Hackbar（火狐自带），进行构造。



执行之后，得到flag。

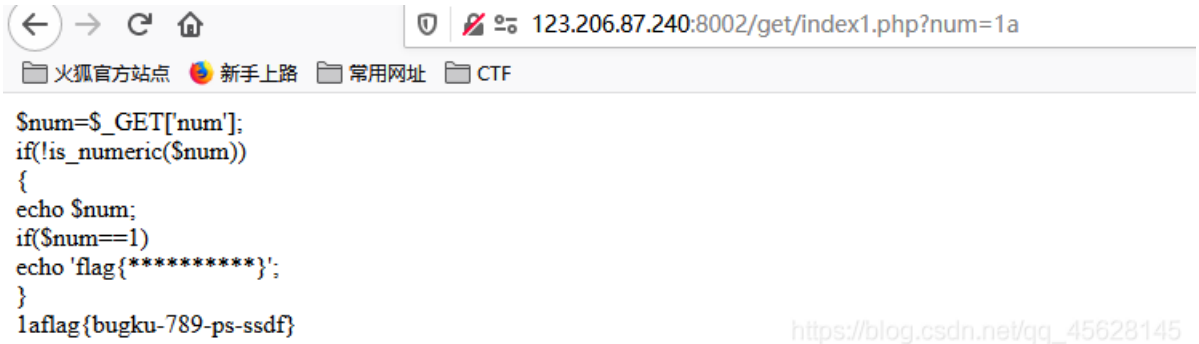


5.矛盾

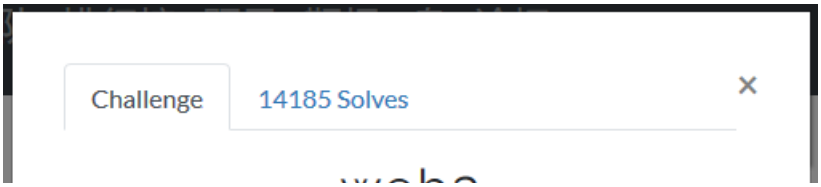


进入之后，发现一段php代码。

通过GET方法获取num的值，如果num=1是数字或者数字字符串的话，输出num，下一步又是如果num=1，输出flag，这不就自相矛盾了吗。但是在这里由于是php，php判断字符串以1开头即可判断等值。于是构造num=1a，得到flag。



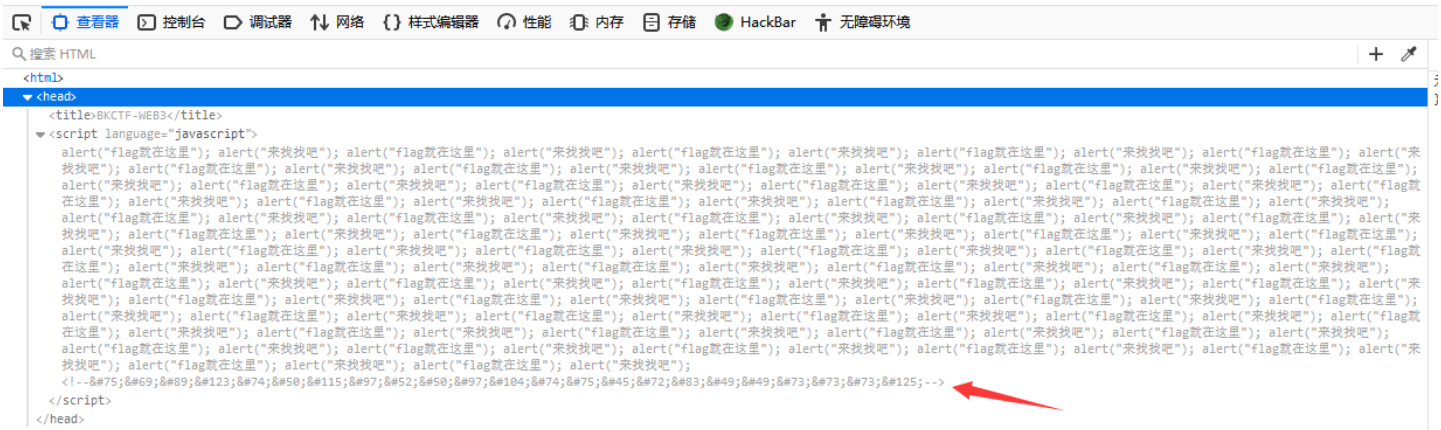
6.web3



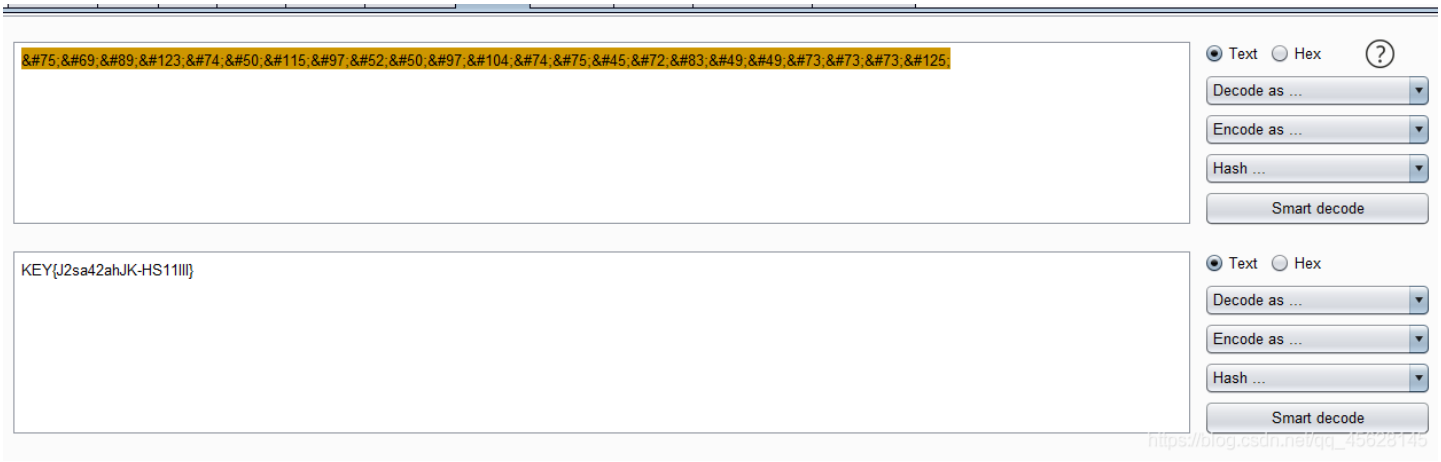
进入之后，发现这个。

点击确定，又继续弹出，点击确定，任然继续弹出。

于是勾选“阻止此页面创建更多对话框”，点击确定，继续查看源码。发现源码里面有一串HTML编码的字符串。



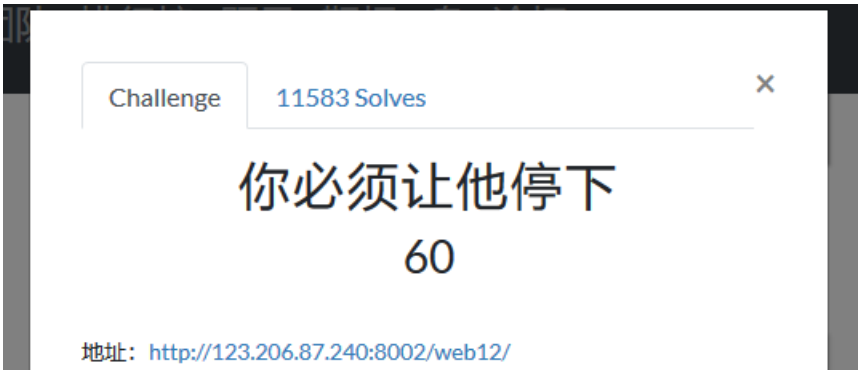
对其进行解码，得到flag。

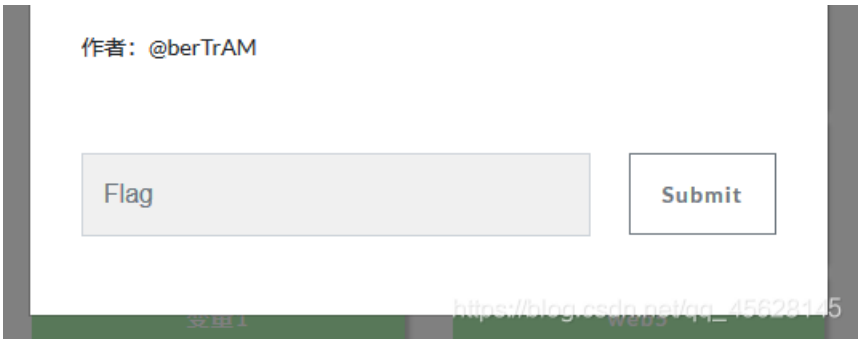


7.域名解析

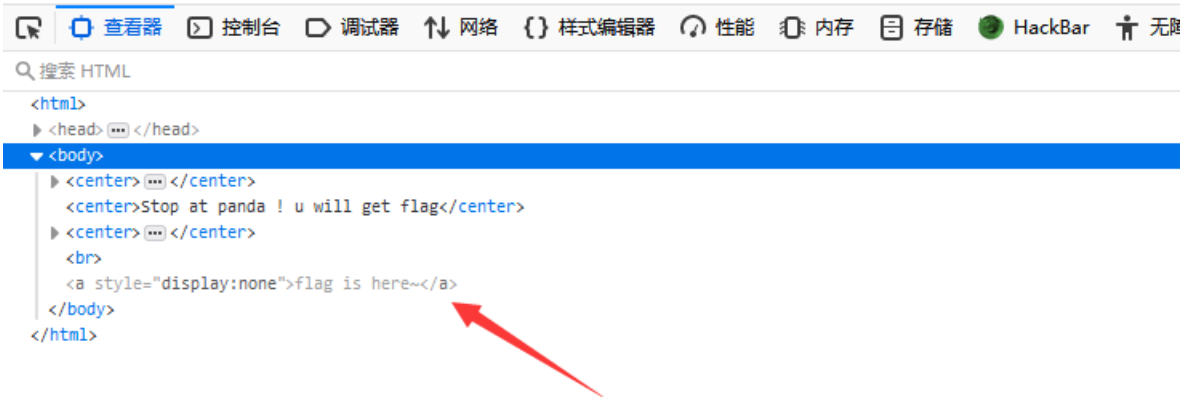
题目说把flag.baidu.com解析到123.206.87.240就能拿到flag，于是直接修改本地hosts（不知道方法的可以百度），再次进入flag.baidu.com，得到flag。

8.你必须让他停下来





进入之后，发现屏幕一直在跳，停不下来，于是去浏览器禁用js，再次进入页面，停下来了，查看源码，发现有一个a标签里面这样显示的。



flag is here。于是我们继续刷新，并且查看源码，然后刷新到了这样的一张图片，发现flag就在里面，得到flag。