BugKu ctf web前7题writeup

原创

Tr_0uble 于 2020-10-12 19:43:59 发布 378 收藏

分类专栏： web 学习笔记

本文链接：https://blog.csdn.net/qq_39585393/article/details/109034572

web 同时被 2 个专栏收录

10 篇文章 0 订阅

订阅专栏

学习笔记

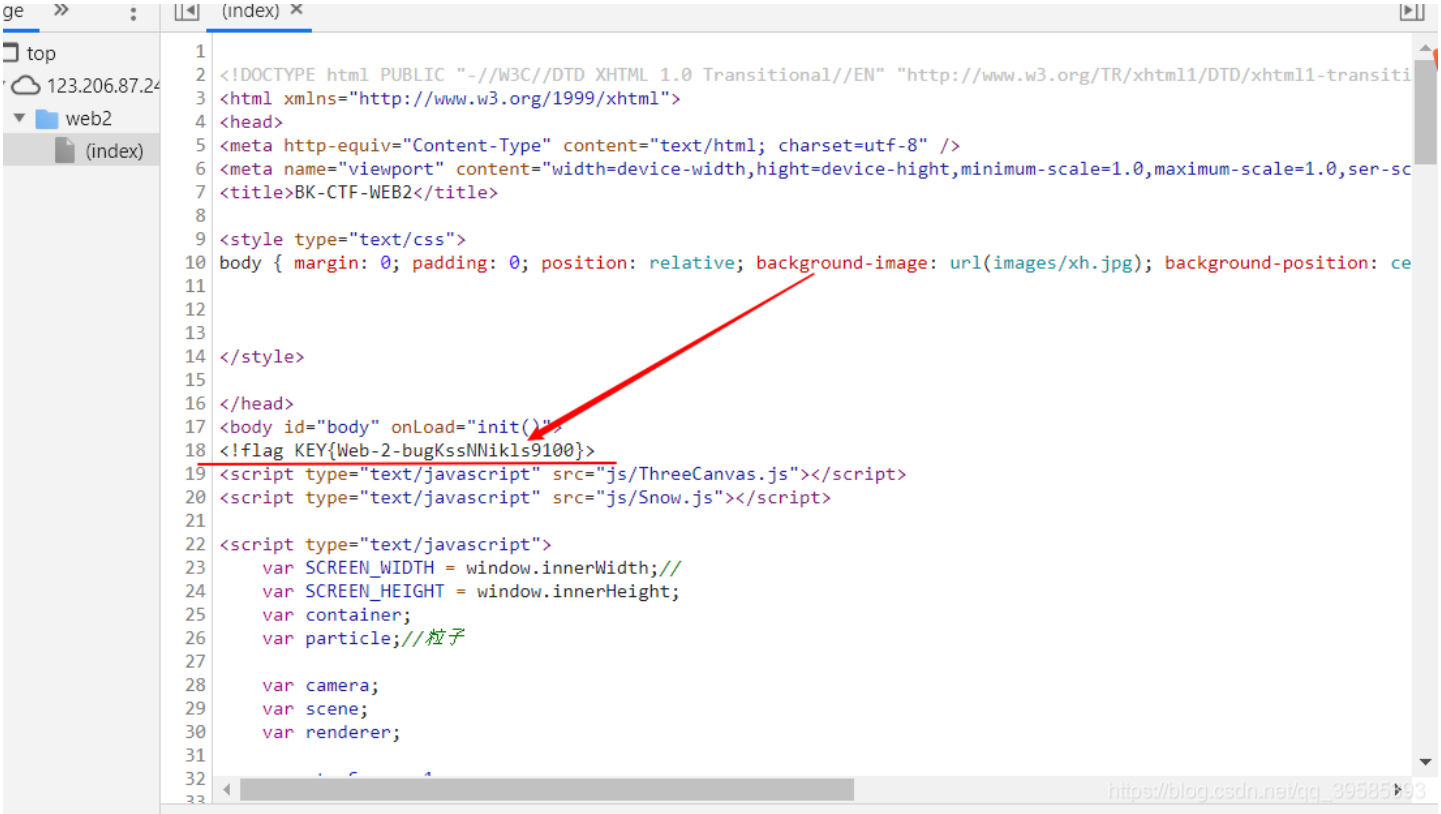
14 篇文章 0 订阅

订阅专栏

前几题都是入门题。。

web2

听说聪明的人都能找到答案。。一堆滑稽不停，直接f12进去看源码，找到flag



KEY{Web-2-bugKssNNikls9100}

计算器题

发现只能输入一位数，按F12, 用选区器选取文本框，在maxlength那个把1改大，然后就能正常输入了

web基础get

直接在URL后面传参 what=flag

web基础post

POST请求没办法写在url里，需要用hackbar或者burp修改，格式就是在最下面Content里写 参数1=值&参数2=值

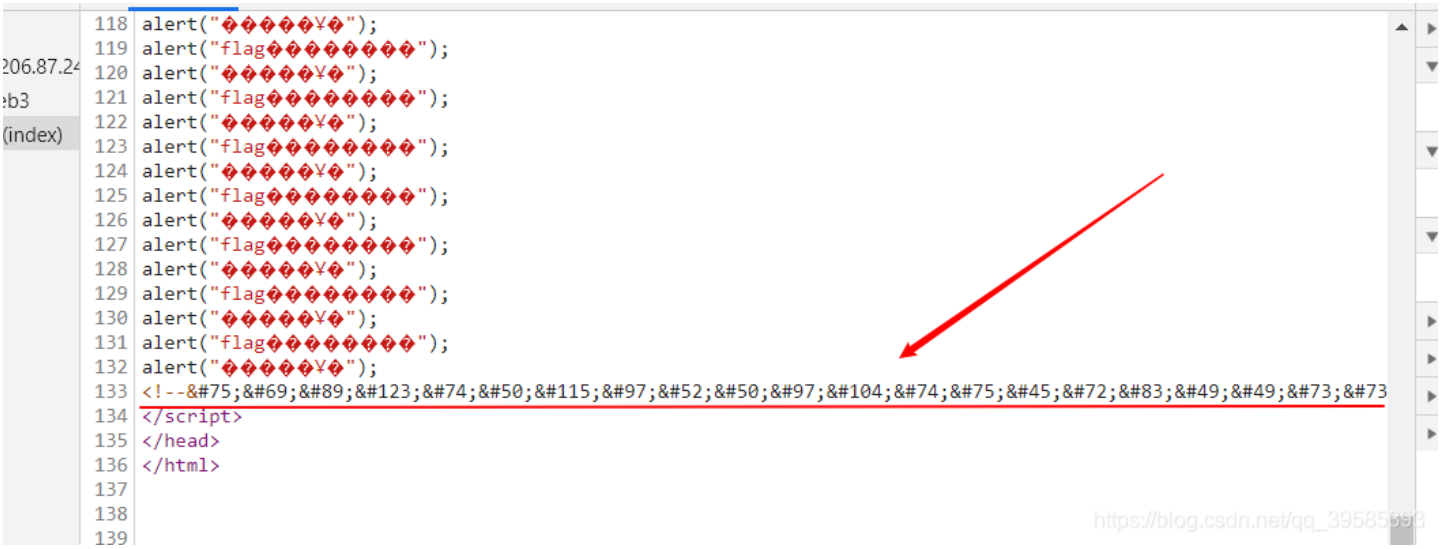
如果用hackbar就没这么麻烦了，直接在框里填就行。
what=flag

矛盾

这个要求不是数字且为1，其实有绕过的办法。下面num1的判定是两个等号，这是弱类型比较（PHP弱类型，可自行百度），如果等号两边类型不同，会转换成相同类型再比较。与之对应的是强类型比较，用的是三个等号=，如果类型不同就直接不相等了。在弱类型比较下，当一个字符串与数字比较时，会把字符串转换成数字，具体是保留字母前的数字。例如123ab7c会转成123，ab7c会转成0.（字母前没数字就是0）
URL:
http://123.206.87.240:8002/get/index1.php?num=1a

web3

一直弹窗不停，F12打开查看发现



注意这个，很像是编码，猜测flag就在里面，用html解码就可以了，解码得到果然是flag

域名解析

域名解析要把域名重定位到要求的ip，使用burpsuit拦截，然后修改host即可，其中burpsuit需要启用代理才能进行拦截抓包，直接贴个连接想看的去看

安装

简单抓包教程

因为我拿https测试的，https需要进行证书的设置才能进行拦截大家可以自行百度