i春秋Web-broken(2017第二届广东省强网杯线上赛)

原创

大千SS 于 2019-05-15 18:59:33 发布 641 收藏
分类专栏： i春秋 文章标签： i春秋Web jsfuck编码

本文链接：https://blog.csdn.net/zz_Caleb/article/details/90242594

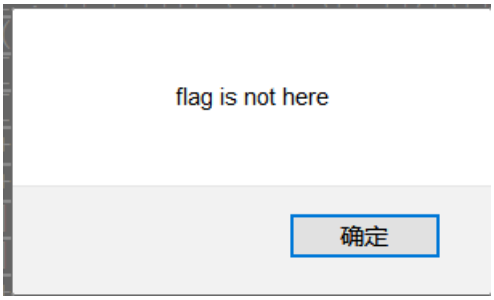

i春秋 专栏收录该内容
13 篇文章 0 订阅
订阅专栏

进站源码没什么东西，有个链接进去看到jsfuck编码，拿到控制台里去执行确无法执行，可能是编码出问题了。

jsfuck编码原理参考：https://github.com/aemkei/jsfuck/blob/master/jsfuck.js

网站上有编码源码，给出了各个字符的jsfuck编码形式，最后的一对括号是没有的，应该是多余的，去掉之后仍然不能成功。

最前面的应该是[]，我们在第二个字符的地方补上一个]，回车弹出：



alert("flag is not here")进行jsfuck编码之后有5903个字符，然而网页中的这一串却又40000个字符之多，应该是还有一部分编码，而flag可能就在没有显示出来的字符里，下面就是这一串编码的修复了。

根据原理，编码中没有单纯一对括号的情况，所以去掉最后的()，开头的第一个[也可能是多余的，删除之后回车得到：
Array ["var flag=\"flag{f_f_l_u_a_c_g_k}\";alert('flag is not here');"]

拿到flag。