CTF-2017第二届广东省强网杯线上赛:broken

原创

Flutter&Python&Test 于 2018-07-26 09:44:47 发布 63 收藏
文章标签： java python 软件测试 js web

本文链接：https://blog.csdn.net/MidSummer411/article/details/111957398

> 分值：50分 类型：Web题目名称：broken
> 题目内容：http://106.75.72.168:1111/ you got a file, but ...

解题过程

1. 点击url,页面显示" Hi, a CTFer. You got a file, but it looks like being broken."
2. 点击"file"链接,页面显示jsfuck码
3. 查看各步骤报文,无异常,也没有隐藏跳转
4. 分析jsfuck代码,删除最后的（），最前面多了个[,也删掉
5. 复制jsfuck代码到浏览器console里运行,弹出flag内容.

知识点

- jsfuck
  jsfuck的起源:在渗透测试时,js代码可能被关键词检测，于是作者考虑躲避关键词检测的想法，例如 eval等关键词.

1. 用各种方法来规避这个检测。
2. 把方法写成通用的程序。
3. 把包含的字符做到极致，最后只剩下 ()+[]! 这六个字符。