实验吧唯快不破writeup

原创

G-Radiation 于 2016-12-09 15:17:41 发布 1387 收藏

分类专栏： CTF 文章标签： writeup ctf

本文链接：https://blog.csdn.net/u012985855/article/details/53539367

原文链接:http://b.zlweb.cc/shiyanbar-wkbp-writeup.html

题目是这个样子的：

点击解题链接显示如下：

下面来分析这道题目，首先从题目和内容可以看出，要想得到key值，必须要快！所以十之八九是考编程题，因为你再快也快不过机器

接着它题目的提示是看看响应头，可以知道我们想要的在响应头里，于是使用brupsuite拦截，查看响应头可以看到如下内容：

其中有个选项是flag，值是一个base64的加密字符串，将其解密得出以下内容：

到这里我就想了，不是应该考编程吗，这也不用很快啊，但在我将后面的JrBYWhEjb提交时，结果证明了我的想法是不正确的，于是就又仔细分析了下解题页面，但源码中发现了如下内容：

看到这里明白了，原来之前的那个是让你在这里提交的，这里的值提交对了才会给出正确的key值，于是编写程序，提交，但是还是不正确，在测试过程中，我发现原来后面的那个值是随机的，而我提交的是我之前解出的值，难怪会出错，于是修改完的程序如下：

```
#-*-coding:utf-8-*-
import requests,base64
url="http://ctf4.shiyanbar.com/web/10.php"
r = requests.get(url)
b64 = r.headers['flag']
decode_flag = base64.b64decode(b64).split(':')[1].strip()
data={'key':decode_flag}
re = requests.post(url,data=data)
print re.text
```

程序运行结果:

将结果提交: