Tamevic's Ctf-Web writeup@实验吧‘天下武功唯快不破’

原创

TameVic 于 2019-03-05 19:58:25 发布 782 收藏

分类专栏： web 文章标签： web ctf

本文链接：https://blog.csdn.net/qq_43264421/article/details/88200185

Tamevic’s Ctf-Web writeup@实验吧‘天下武功唯快不破’

> 第一篇wp，希望自己有个好的开始，养成一个好的习惯

url： http://www.shiyanbar.com/ctf/1854

分析

看到题目提示我们看看响应头。先点击进入url，调出控制台查看响应头

能看到其中含有

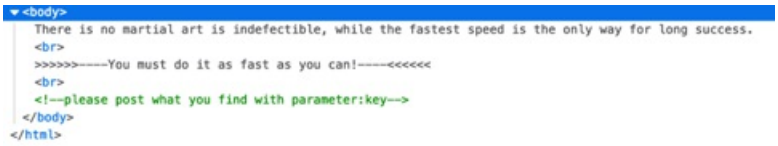
```
key：UDBTVF9USElTX1QwX0NINE5HRV9GTDRHOkFOM0xkUmdPNg==
```

将其base64解密后可得明文：

```
P0ST_THIS_T0_CH4NGE_FL4G:AN3LdRgO6
```

前文页面提示，包括html代码中都藏有提示：让我们将key以post方式发送

There is no martial art is indefectible, while the fastest speed is the only way for long success.
>>>>>>-----You must do it as fast as you can!-----<<<<<<



因此我们使用postman发送key试试，发现无果。再结合题目说的“唯快不破”，编写脚本进行发送：

```
import requests
import base64
r = requests.post('http://ctf5.shiyanbar.com/web/10/10.php')
key = r.headers['FLAG']
flag = base64.b64decode(key).decode().split(':')[1]
para = {'key':flag}
result = requests.post('http://ctf5.shiyanbar.com/web/10/10.php',data = para)
print(result.text)
```

这里可以学习下post（）函数的用法：

post（url，data）

结果

post发送后即可得到flag：

```
CTF{Y0U_4R3_1NCR3D1BL3_F4ST!}
```

End

你确实很快？？？我才不快好吗！