实验吧-猫抓老鼠 Writeup

原创

baynk 于 2019-08-31 07:30:51 发布 495 收藏 1

分类专栏： # 实验吧 Writeup 文章标签： CTF 实验吧 猫抓老鼠

本文链接：https://blog.csdn.net/u014029795/article/details/100168552

实验吧 让实验更简单！ 实验吧 Writeup 专栏收录该内容

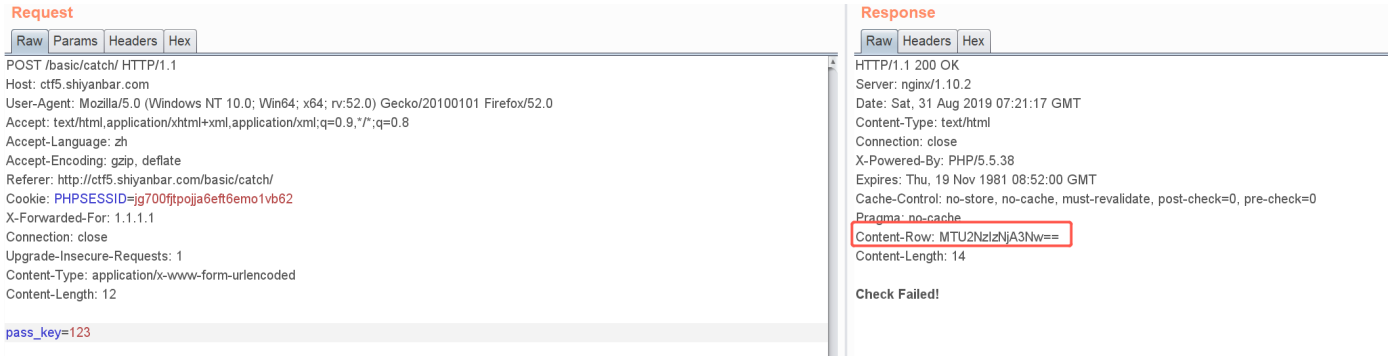
21 篇文章 0 订阅

订阅专栏

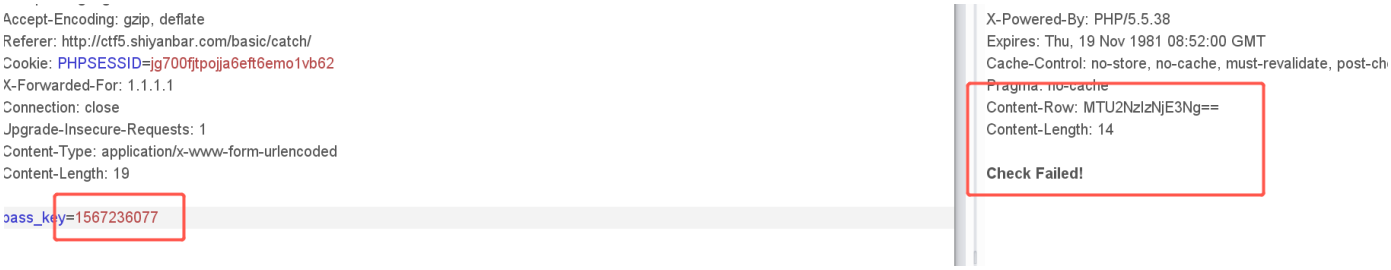
应该是8月最后一篇。。。

过程

- 链接：http://ctf5.shiyanbar.com/basic/catch/
- 这个还是很简单的，而且之前有个题和这个很像，做的很快。
- 进入就是提交一个参数，随便写了些东西，没发现明显注入，丢入burpsuite中看。



- 发现有明显的非常规http头部信息，还是base64加密的，解密后是一串数字，然后提交后仍然数字，感觉像是时间戳。。。



- 还是失败了，可能是手速不够快，毕竟都有时间戳这样明显的提示了，于是用之前写过的脚本，修改着改了下。

```
import requests
import base64
'''-----------------------------------------'''
url = "http://ctf5.shiyanbar.com/basic/catch/"
key = requests.get(url)
a = key.headers['Content-Row']
```

```
a = key.headers['Content-Row']
print(a)
b = base64.b64decode(a).decode()
print(b)
'''-----------------------------------------'''
value = "pass_key="+a
headers = {'Content-Type': 'application/x-www-form-urlencoded'}
post = requests.post(url,data=value,headers=headers)
print(post.text)
```

```
C:\Python37\python3.exe "D:/Programs/Pycharm for python/test/ctf2.py"
MTU2NzIzNjMyNQ==
1567236325
Check Failed!
```

- 还是失败了，然后测试了一会，结果让我有点无语。。原来不需要解密，直接提交读取到的base64值就可以了，修改python，再提交，搞定。

```
C:\Python37\python3.exe "D:/Programs/Pycharm for python/test/ctf2.py"
MTU2NzIzNjQyMg==
1567236422
KEY: #WWWnsf0cus_NET#
```

总结

- 8月结束了，以平均每天一篇blog结束了，9月会更忙，希望可以坚持学习，9月见！！！