实验吧-天下武功唯快不破 Writeup

原创

baynk 于 2019-08-17 01:32:28 发布 172 收藏 1

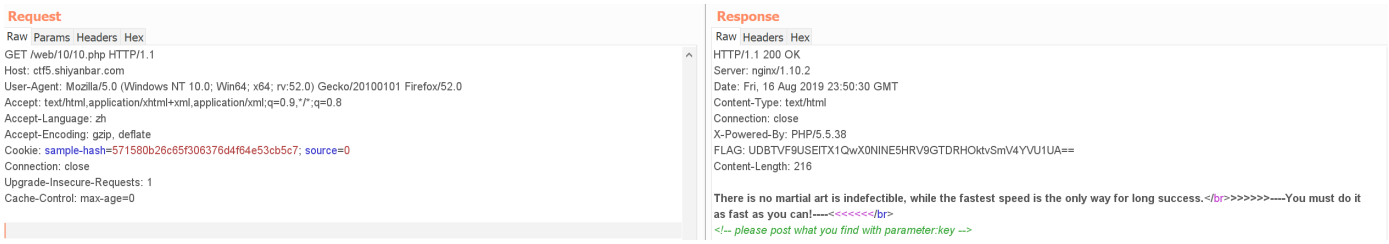
分类专栏： # 实验吧 Writeup 文章标签： 实验吧 CTF

本文链接：https://blog.csdn.net/u014029795/article/details/99687298

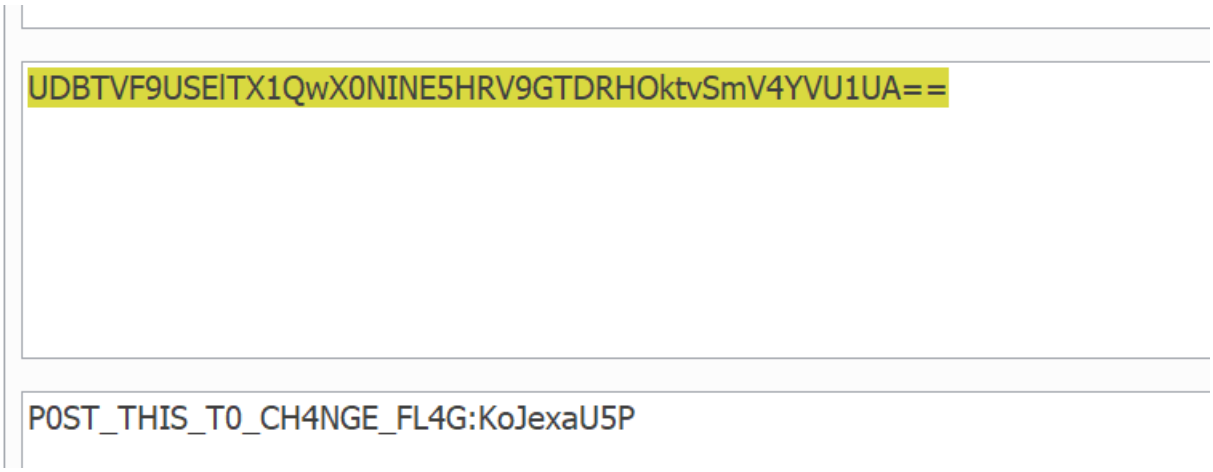
终于遇到一个简单的了。。。

过程

- 链接：http://ctf5.shiyanbar.com/web/10/10.php
- 直接丢到burpsuite中看到源码和返回包。



- 然后在响应头部中看到有flag了，明显是base64的，用burpsuite解出来。



- 发现并不是flag。。。不然也太简单了，然后看了下提示，需要提交key，而key的值就是刚刚解密出来的，然后照着又来了一次。

```
Content-Length: 15

key=KoJexaU5P
```

```
as fast as you can!----<<<<<<</br>
<!-- please post what you find with parameter:key -->
```

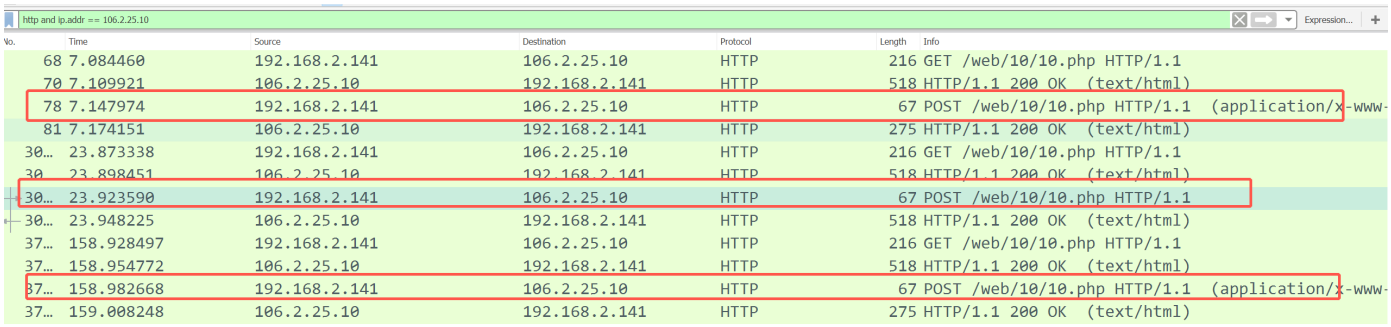
- 然后发现还是这样的，然后继续go了好几把，仍然无止境，这个时候就想到了the fastest speed。。。估计要写脚本跑了，不然再怎么写也没脚本快啊，应该是设计的提交时间的限制。。。接下来去完成py脚本。

---

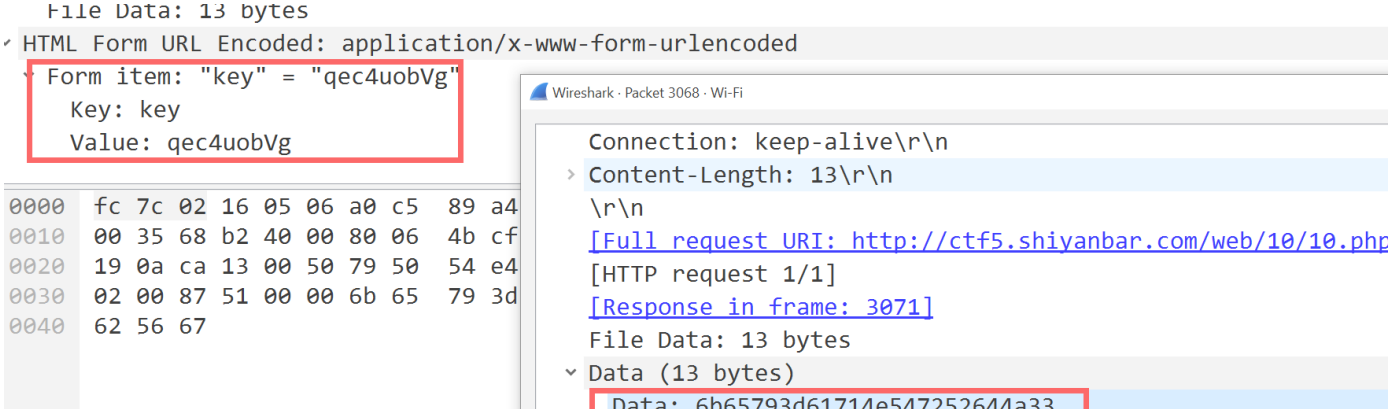
py脚本

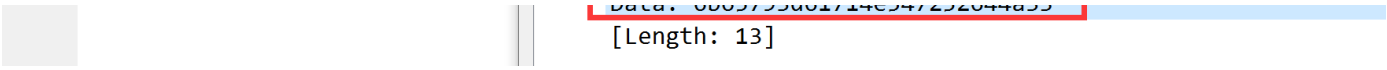
```
import requests
import base64
'''------------------------------------------'''
url = "http://ctf5.shiyanbar.com/web/10/10.php"
key = requests.get(url)
a = key.headers['FLAG']
print(a)
b = base64.b64decode(a).decode().split(':')[1]
print(b)
'''------------------------------------------'''
value={'key':b}
post = requests.post(url,data=value)
#value = "key="+b
#headers = {'Content-Type': 'application/x-www-form-urlencoded'}
#post = requests.post(url,data=value,headers=headers)
print(post.text)
print(post.headers)
```

- 没想到还是把自己给坑了，原来都喜欢把post数据以字符串进行提交，然后会加上contet-Type的头部的，这次看抓包过程中没有，就没加了，一直出不了效果，然后换成了字典的形式马上就好了，也不需要头部，服了。。。又踩坑了。
- 开wireshark抓包，分别做了三次测试，用字典提交数据为第一次，第二次就是字符串，第三次是字符串加表单方式，结果为第一次和第三次相同，如果字符串没有头部去定义提交表单方式则结果不同

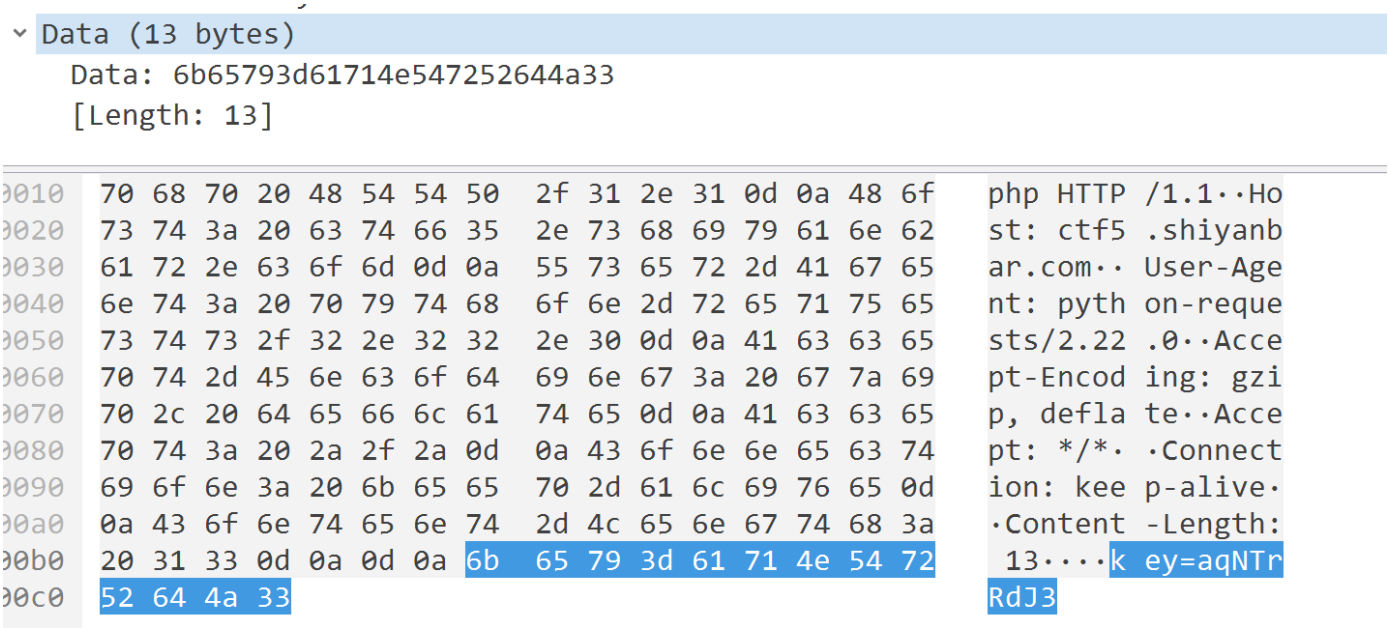


- 对比报文的详细内容。





- 将报文进行url解密后发现，格式是正确的。。。



- 经过测试后，发现如果不定义头部中的提交表单方式默认会以类似“multipart/form-data ”这种方式进行提交表单，这种一般是在上传文件时才会用到，我感觉问题在于获取表单数据的函数上，可能获取不到form-data这种方式提交的数据表，有机会再去证实了。

总结

- 这问题碰到过，但是解决了就解决了，这次又踩了同一个坑，不过这次理解得更透彻了一些，还没完全理解，差一次证实，需要去写一个php尝试一下。
- 好好的web题变成了python题，又从python题到了web题。。。无语~~