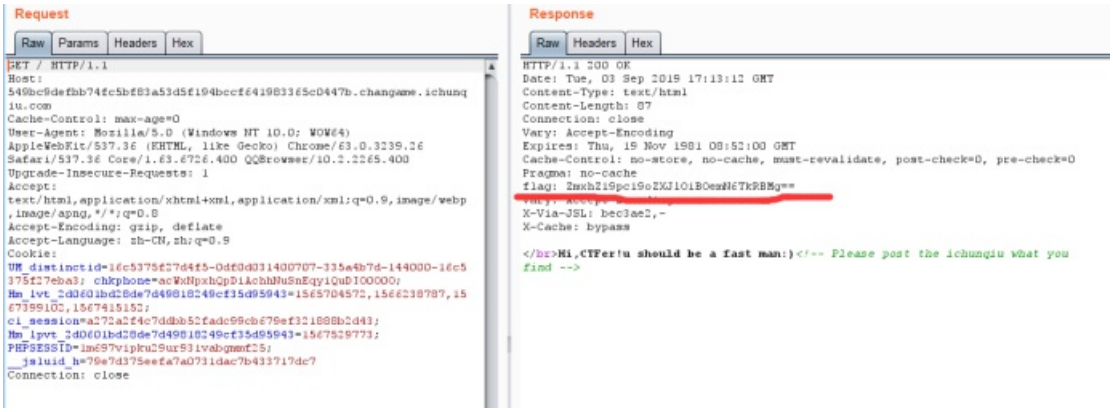
i春秋Upload

转载

weixin_30701575 于 2019-09-04 23:11:00 发布 155 收藏
文章标签： php
原文链接：http://www.cnblogs.com/wosun/p/11462252.html

打开是一句普普通通的话，先查看源码，发现提示，我们需要post我们从i春秋得到的东西

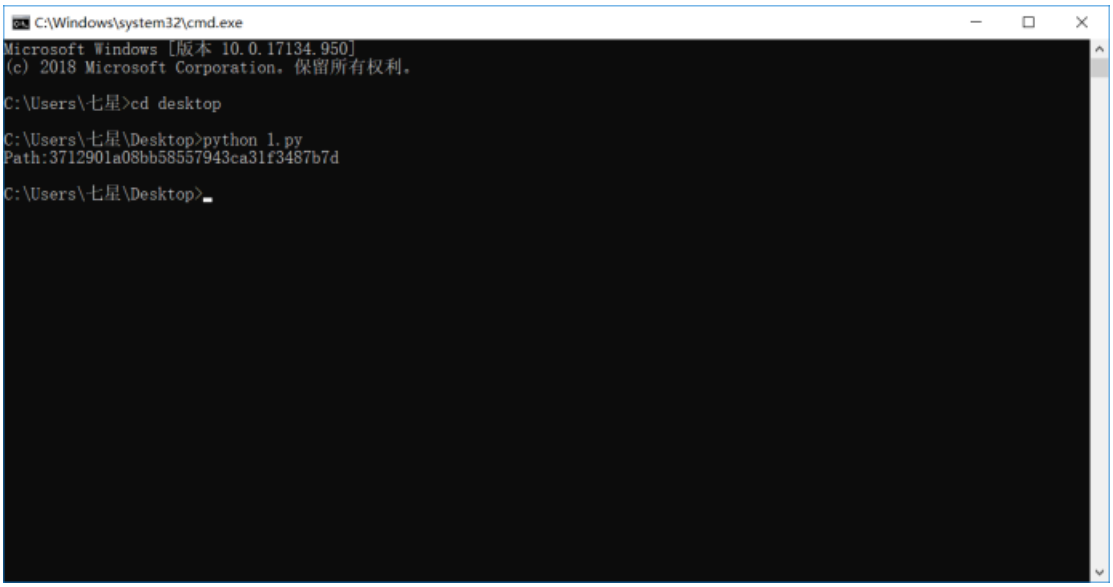
得到了什么呢？不知道，去看看cookie，没什么特别的地方，再去抓包试试



找到了我们需要post的东西，不过这东西会一直刷新，并且频率很快，所以这里只能借助脚本

```
import base64,requests

def main():

    a = requests.session()

    b = a.get("http://549bc9defbb74fc5bf83a53d5f194bccf641983365c0447b.changame.ichunqiu.com/")

    key1 = b.headers["flag"]

    c = base64.b64decode(key1)

    d = str(c).split(':')

    key = base64.b64decode(d[1])

    body = {"ichunqiu":key}

    f = a.post("http://549bc9defbb74fc5bf83a53d5f194bccf641983365c0447b.changame.ichunqiu.com/",data=body)

    print (f.text)

if __name__ == '__main__':

    main()
```

跑出来是一串字符串

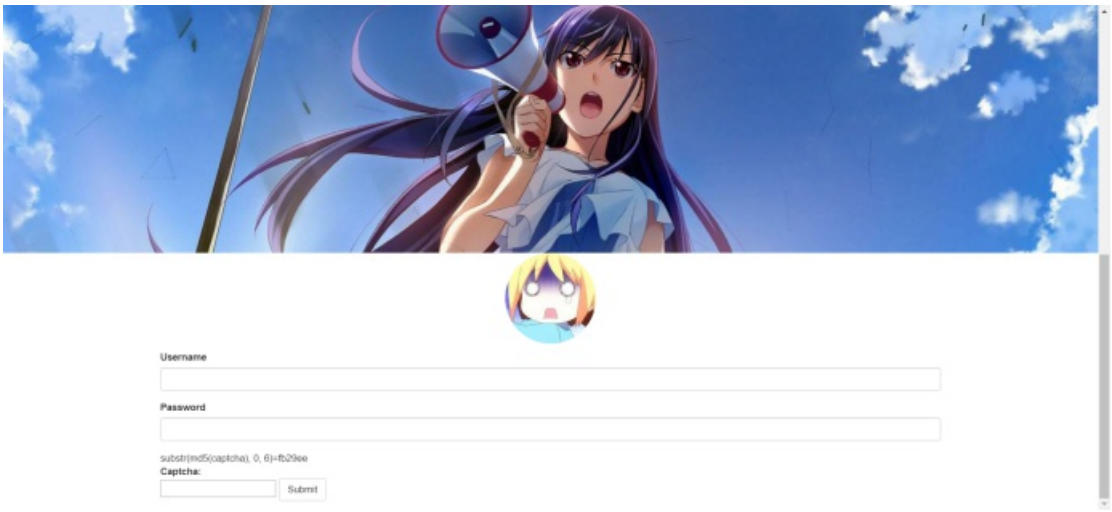


字符串的意思是提示我们一个路径，不管了，访问之

Url/3712901a08bb58557943ca31f3487b7d

进去是一个普普通通的跳转界面，看源码没什么特别的

点按钮进入下一界面



就是一个登录界面了

尝试注入

注入失败。。。

下面还有给验证码，这个验证码我还真遇到过，就一字符串取其前六位再md5加密后得到的东西，反向解密就可以得到验证码

然后试试再在username中注入。。。。注入失败，看来这里就不是注入可能

看了别人的wp才知道这里是svn泄露（目前还不知道这么测，难道一个个排查吗）

直接访问http://549bc9defbb74fc5bf83a53d5f194bccf641983365c0447b.changame.ichunqiu.com/3712901a08bb58557

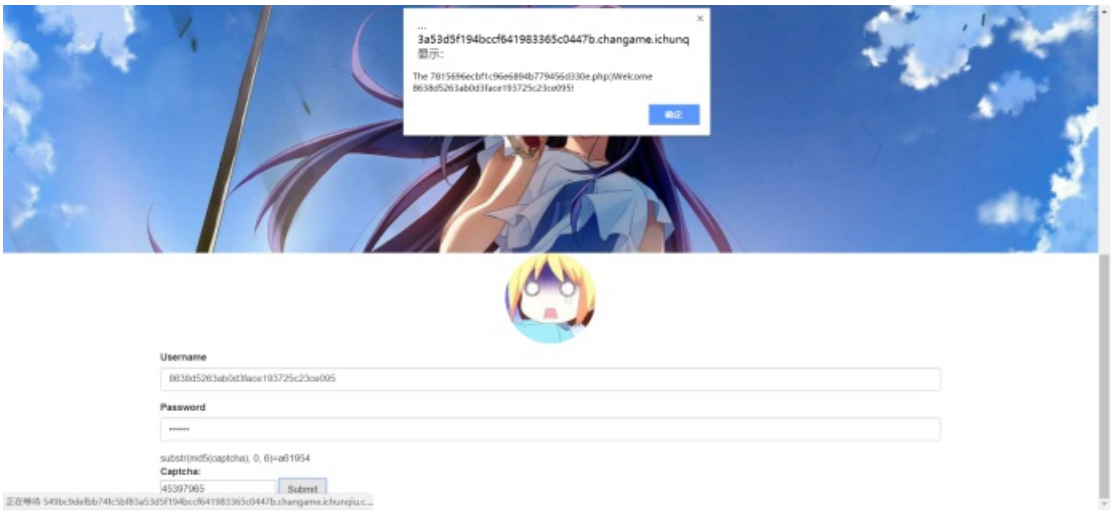
得到username和password（md5加密的，直接用解码工具解开就行了）

解开username是8638d5263ab0d3face193725c23ce095

密码随便填

验证码爆破

就可以登录成功了



但是登录后并没有什么东西，还是原来的输入账号密码验证码。。。。

看了提示才知道弹窗上面有个文件名

不多说，访问之

http://549bc9defbb74fc5bf83a53d5f194bccf641983365c0447b.changame.ichunqiu.com/3712901a08bb585579

是一个文件上传的界面

这时我想到的是一句话木马，就直接上传个php文件上去，提交后提示我们需要JPG。。。这种题我也遇到过，抓包改就行了。。。。

选择文件 未选择任何文件 Submit

You got it!:)

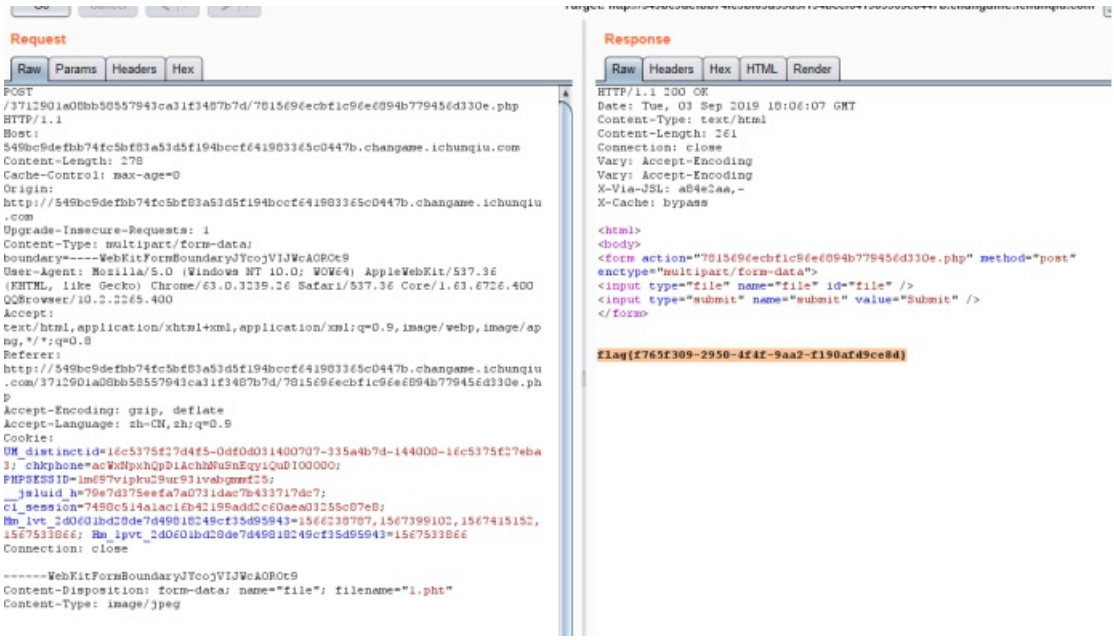
。。。。。

被嘲笑了似乎

看别人wp才知道这里原来是0x00截断

就先传一个jpg的图片文件上去再用bp抓submit的包再修改文件后缀为pht（这个我完全想不到。。。）

Go一遍得到flag



转载于:https://www.cnblogs.com/wosun/p/11462252.html