第一届“百度杯”信息安全攻防总决赛 线上选拔赛 Upload

原创

bfengj 于 2020-10-03 18:44:49 发布 749 收藏 2

分类专栏： 文件上传 python脚本 泄露 文章标签： 信息安全 web post 密码学 python

本文链接：https://blog.csdn.net/rfrder/article/details/108912162

前言

有一说一，这题应该算是比较全面，而且难度适中的一题。全是都是固定的套路，知道怎么绕过， 怎么去做，就很简单。我做的时候卡在了第一个点上。。只能说，凡是遇到写python脚本的我都没做出来过。唉。还是畏惧了。因为python很差，遇到题目自己的思路里就没有写python脚本。还是能力的问题，需要加强。

WP

首先进入环境，提示我们要做个fast man。我的第一反应是302跳转，但其实是写python脚本去post。f12看看源代码发现了：
Please post the ichunqiu what you find
看了WP才知道post的内容应该是 ichunqiu:xxx。我还以为是flag:xxx。还是基本功的问题。
抓包看一看发现响应头中有flag:

```
flag: ZmxhZ19pc19oZXJl0iBNamN4TmpVMA==
```

然后base64解码，还有一段出不来，再base64是一段奇怪的数字。我以为是我解密的问题，因为密码学也是知识盲区。。然后就卡住了。。
其实多请求几遍，会发现这个flag会变化的。所以其实最终的结果就是那个数字。
即使我们请求后进行二次base64解码然后进行post请求，还是得不到结果，因为不够快。。所以写一个python脚本来请求，这里的脚本参考了网上的代码：

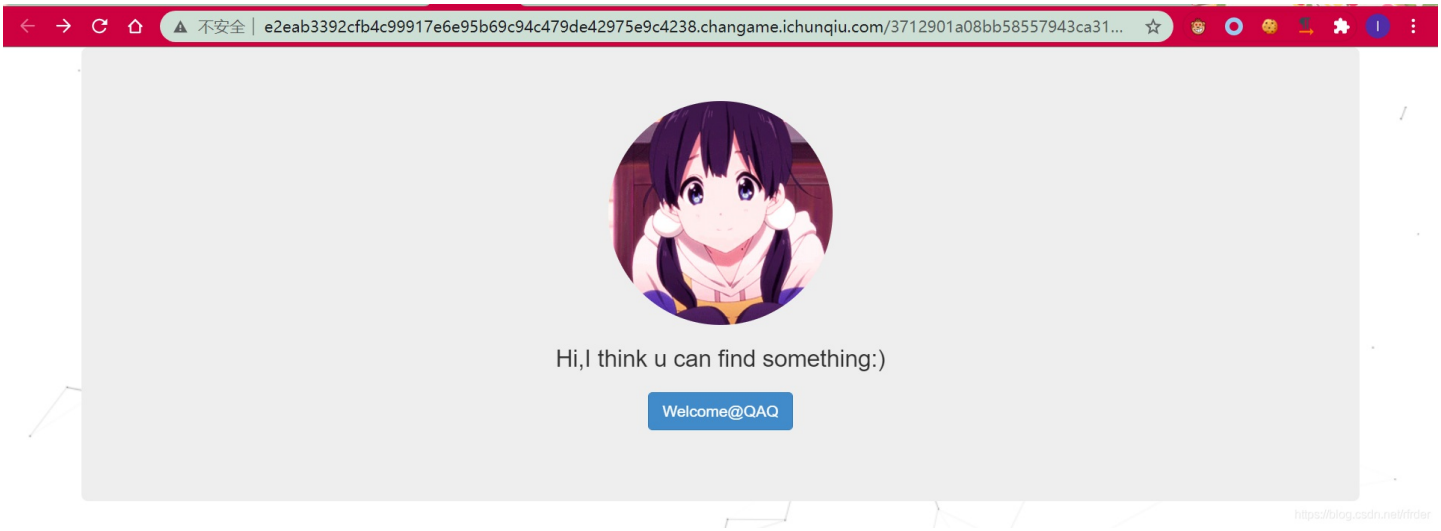
```python
import requests
import base64

url = 'http://e2eab3392cfb4c99917e6e95b69c94c479de42975e9c4238.changame.ichunqiu.com/'
s = requests.session()
r = s.get(url)
fh = r.headers["flag"]
b = base64.b64decode(fh)
f = str(b).split(':')
data = base64.b64decode(f[1])
payload = {"ichunqiu":data}
fl = s.post(url, data = payload)
print(fl.text)
```

返回了：

Path:3712901a08bb58557943ca31f3487b7d

因此我们请求一下这个网页，出现重定向到了另一个地方：



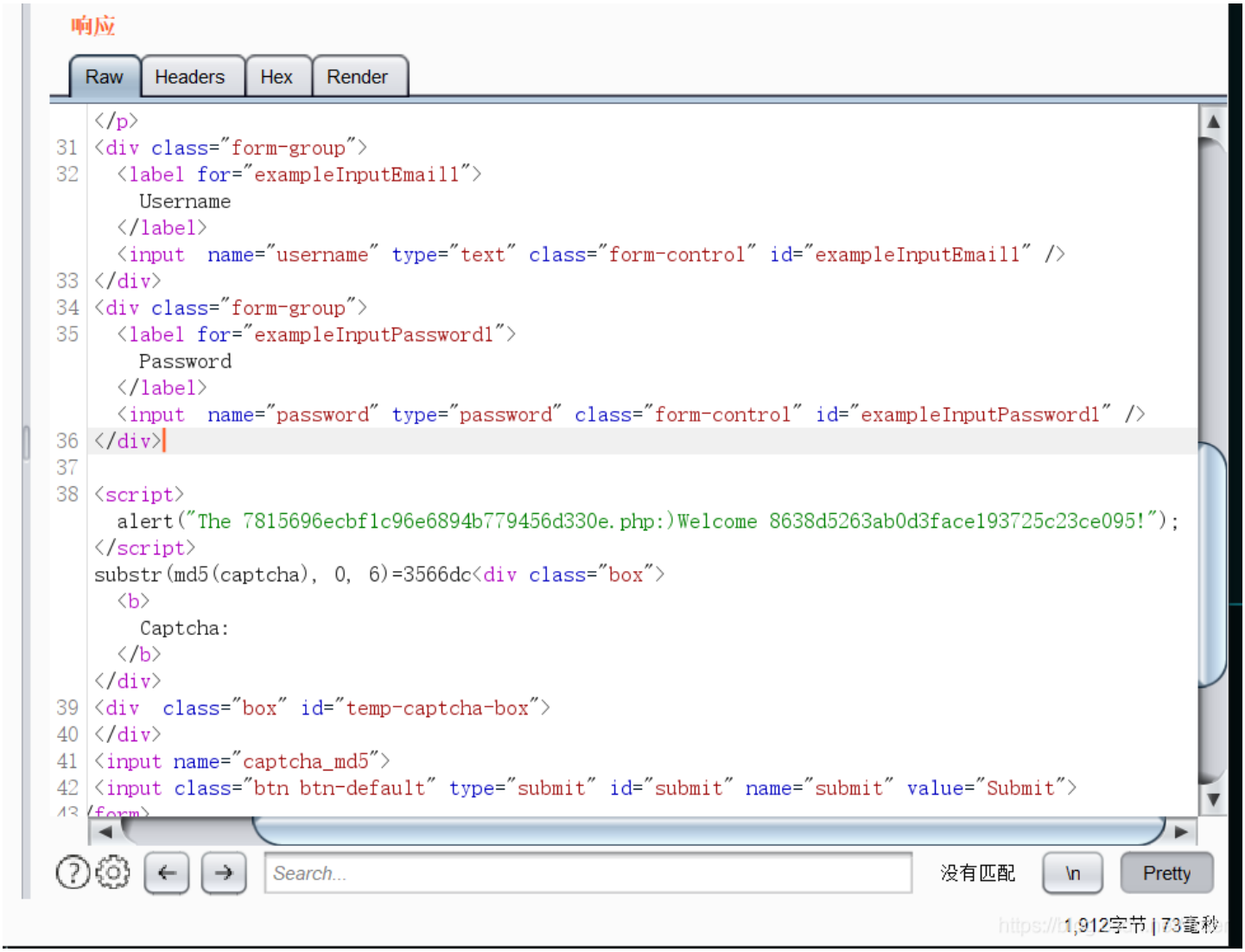
点击welcome后发现是一个登录的界面，而且很熟悉，好像前几天刚做过一模一样的登录界面。但是按照以前的那种方法不行，进行SQL注入还是失败了。最后我用dirsearch扫了一下上面的那个网页，发现了wc.db文件！原来存在SVN泄露。我们直接访问一下/.svn/wc.db，出现了username:

```
OK!
Congratulations!
My username is md5(HEL1OW1OrDEveryOn3)
:)
```

原来用户名不是admin。。怪不得之前尝试会失败。知道了用户名，就是老办法了，利用下面的python脚本得到验证码。

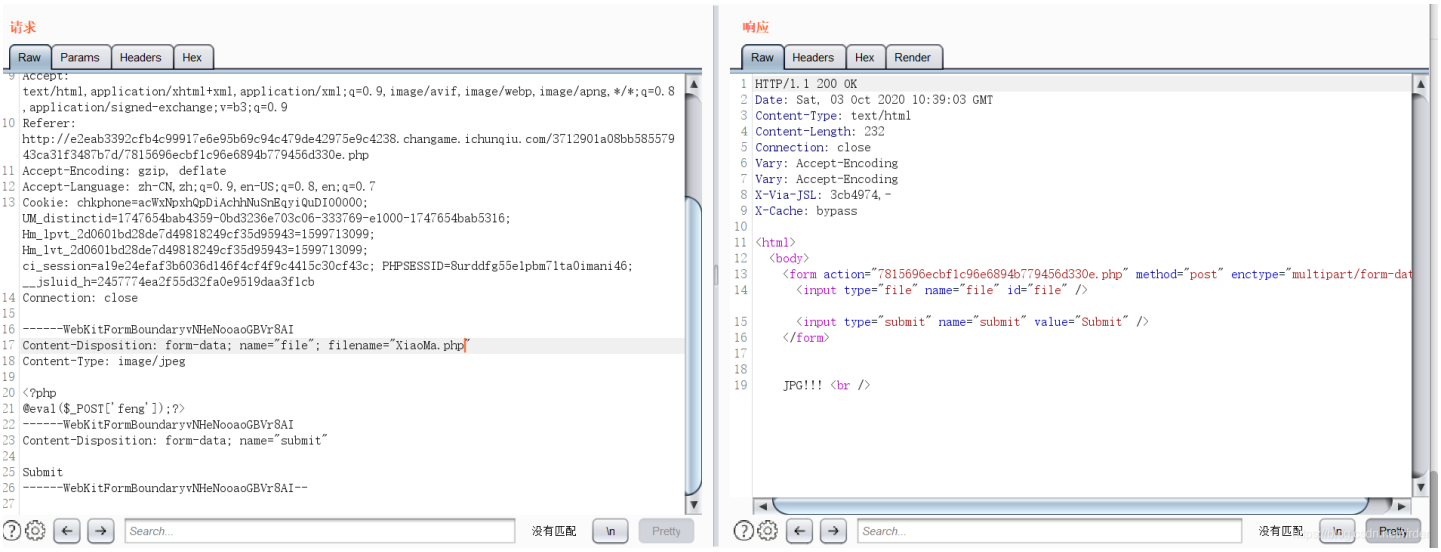
```python
import hashlib
for v1 in 'abcdefghijklmnopqrstuvwxyz123456789':
    for v2 in 'abcdefghijklmnopqrstuvwxyz123456789':
        for v3 in 'abcdefghijklmnopqrstuvwxyz123456789':
            for v4 in 'abcdefghijklmnopqrstuvwxyz123456789':
                for v5 in 'abcdefghijklmnopqrstuvwxyz123456789':
                    for v6 in 'abcdefghijklmnopqrstuvwxyz123456789':
                        v=v1+v2+v3+v4+v5+v6
                        m=hashlib.md5()
                        m.update(v.encode("utf-8"))
                        n=m.hexdigest()
                        if n[0:6] == '508be7' :
                            print(v)
```

然后输入用户名，密码随便填，提交后会弹出个框：

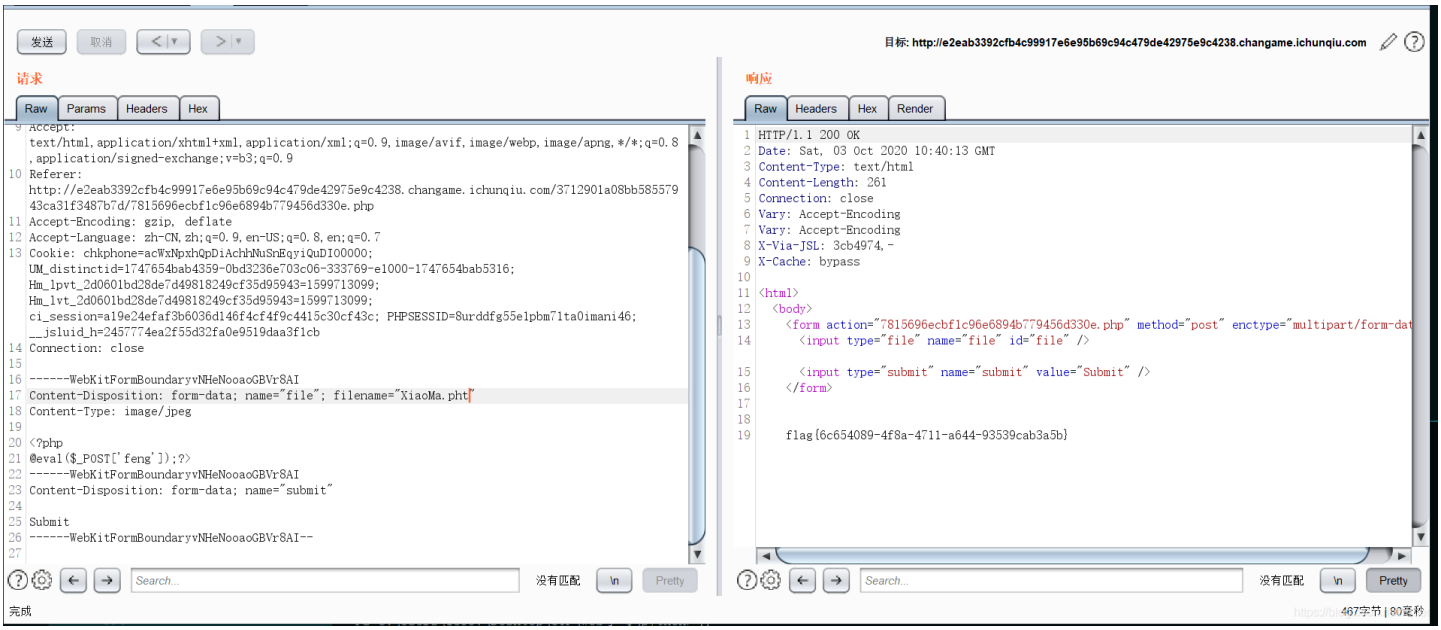


我们访问一下这个7815696ecbf1c96e6894b779456d330e.php，发现是一个文件上传的页面。

果然是老套路了，上传个一句话木马，提示必须是JPG：



尝试换成php的其他别名，使用pht的时候成功获得了flag:



总结

怎么说呢，python真的是自己的弱项，自己还需要养成一种写python作为一种非常常规的解题手段的习惯。以前的自己遇到要写python脚本的题就头大。但是在接触了越来越多的要写脚本的题之后，自己如果还是这么不长进的话，真的就太tmfw了。