[ACTF2020 新生赛]Upload

原创

Kradress 于 2022-02-14 00:16:37 发布 148 收藏

分类专栏： BUUCTF 文章标签： 安全 php 开发语言

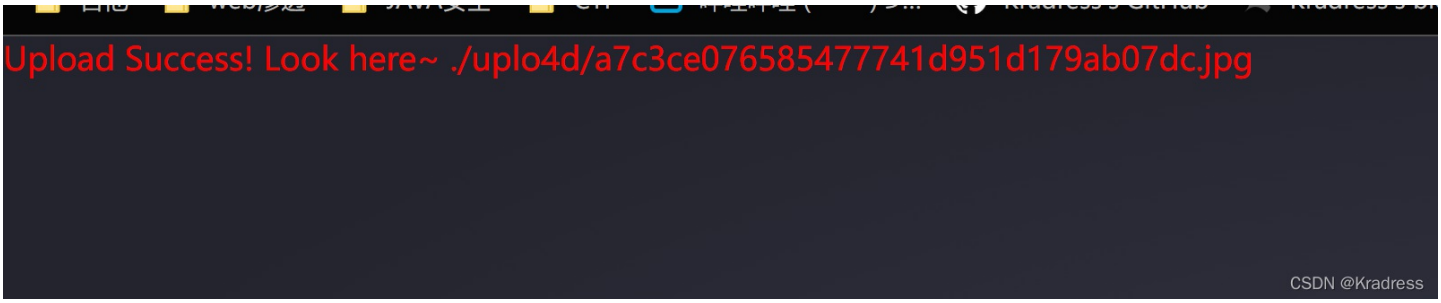
本文链接：https://blog.csdn.net/Kracxi/article/details/122916435

目录

思路

先上传一个包含shell的jpg文件

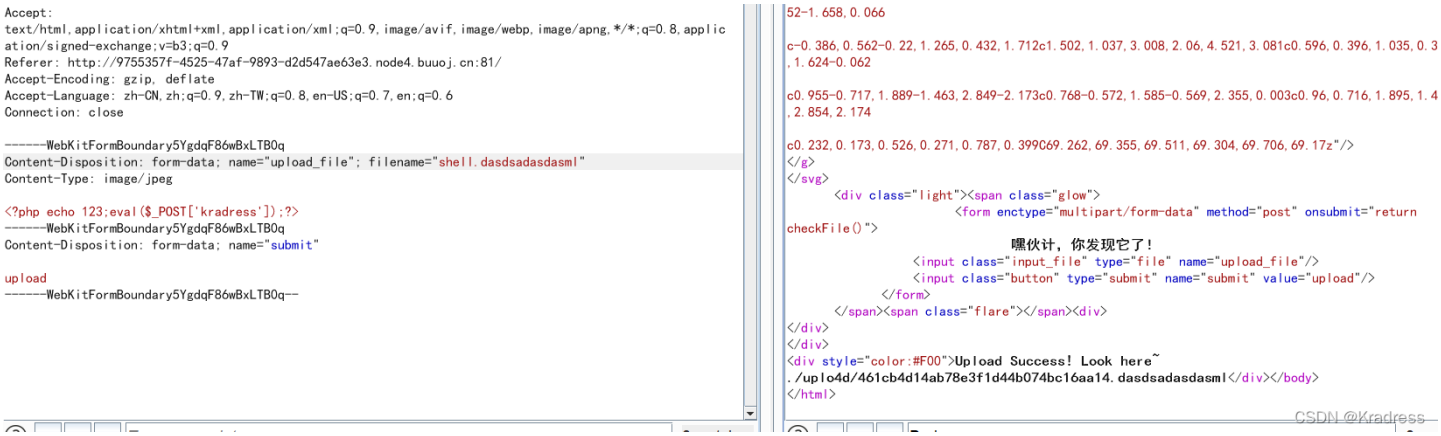
上传成功,说明不对文件内容进行过滤



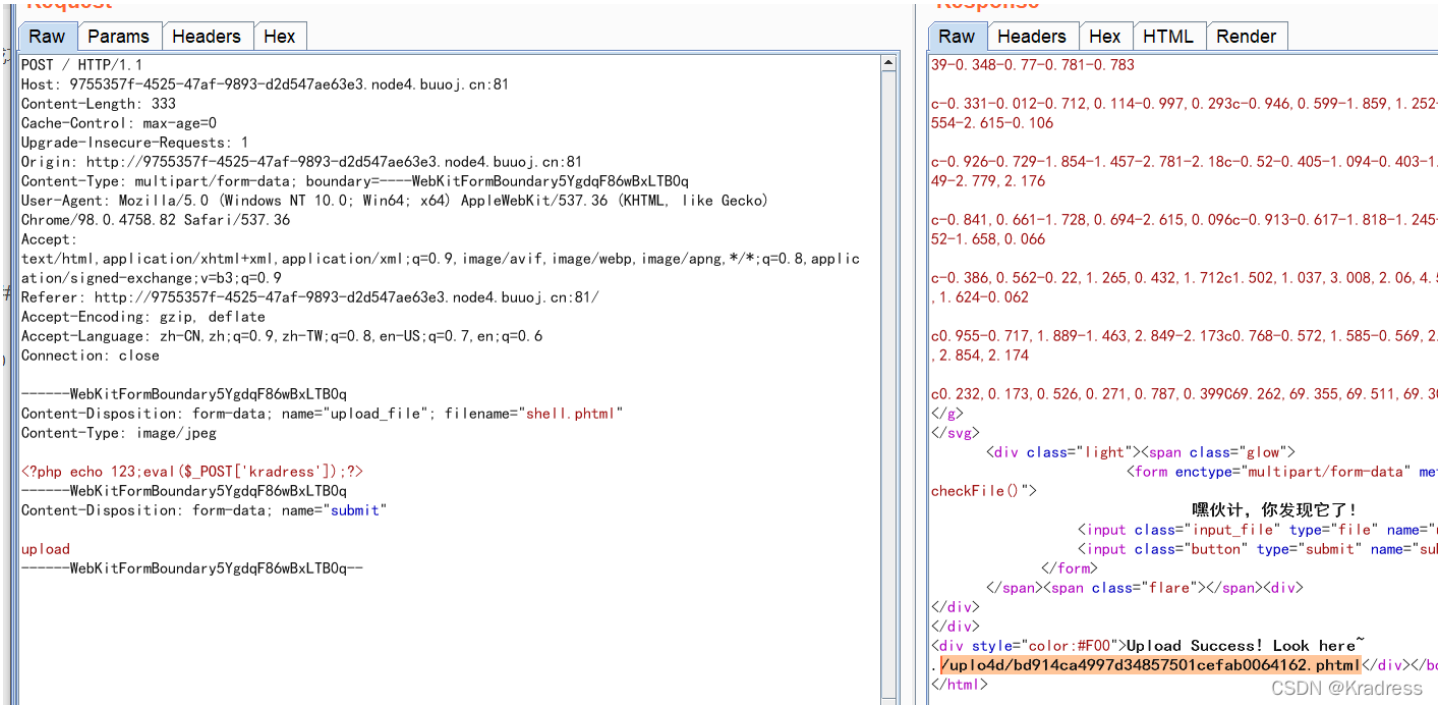
用bp抓包把后缀改成php,被拦截,说明对文件后缀有检测

```
</div>
nonono~ Bad file!
```

接来下把文件后缀名改成任意字符,上传成功,说明是黑名单



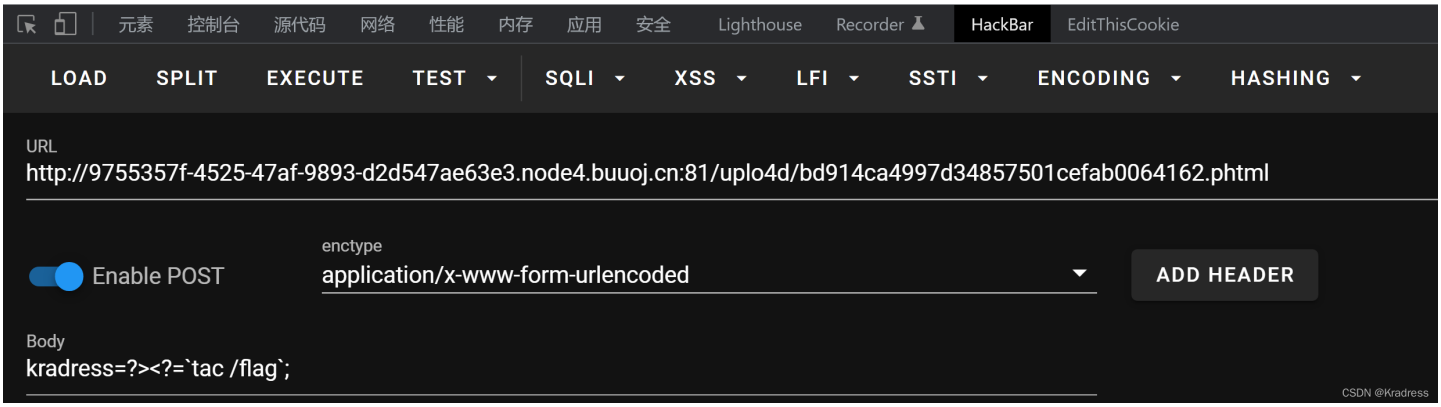
把后缀改成php3,php4,php5,phtml逐个尝试,最后phtml成功上传



然后去访问上传的文件验证文件是否被解析

发现页面成功显示123,就可以RCE了

123flag{b81c1845-3ac1-46a8-9bca-028522882555}



总结

水题