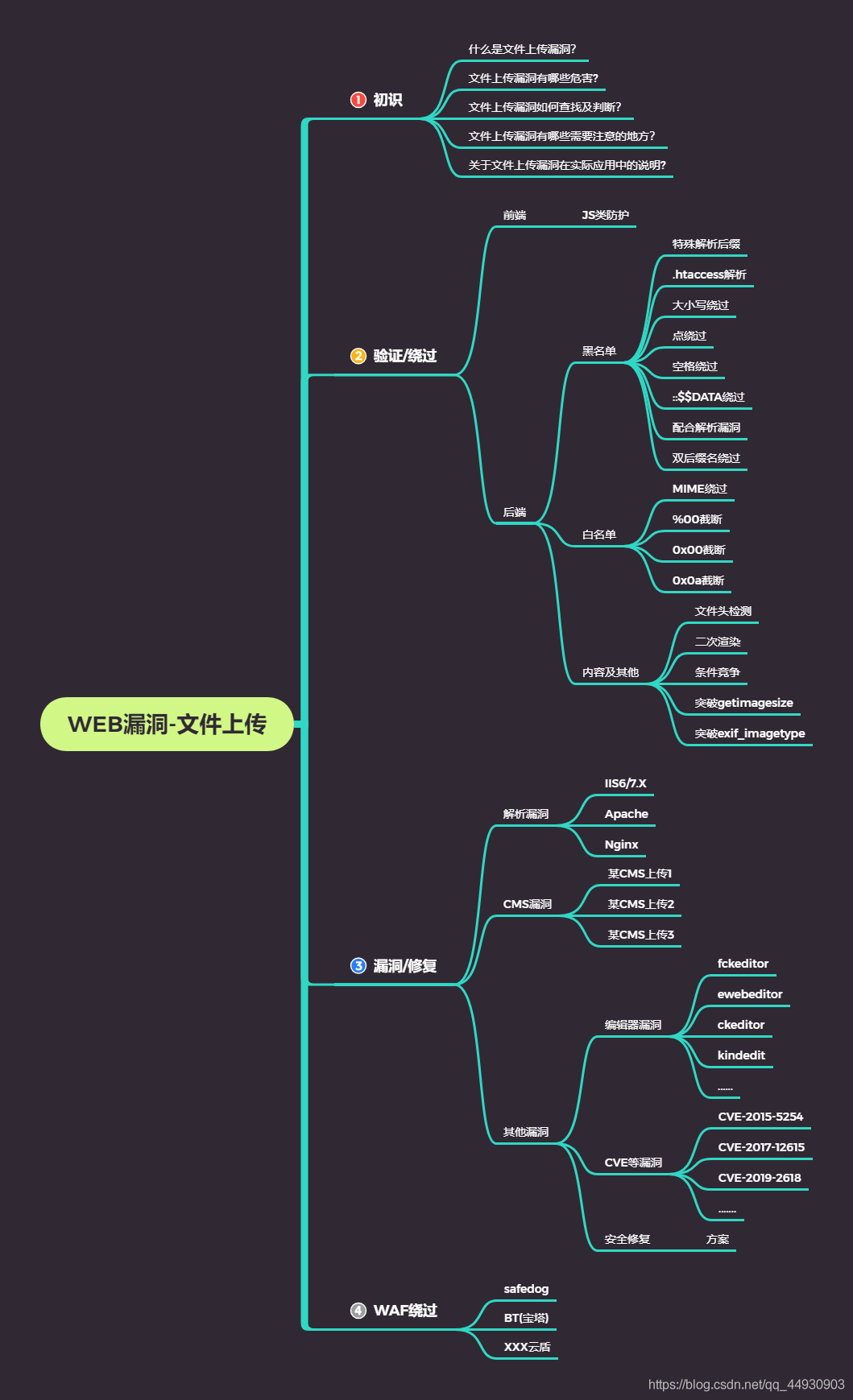
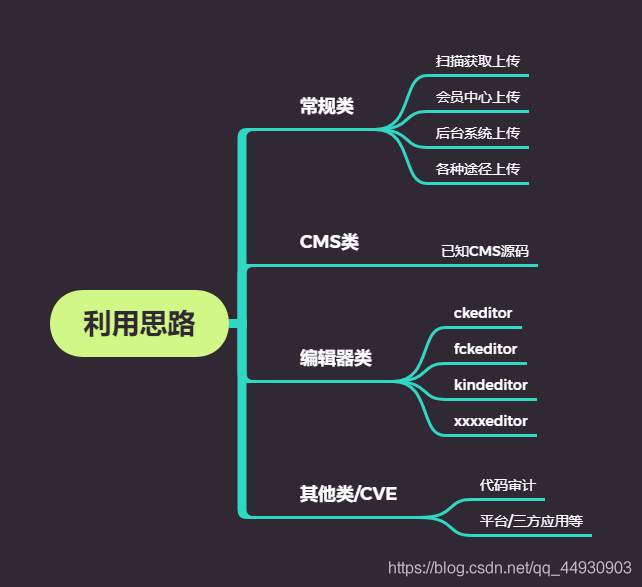
# 20 WEB漏洞-文件上传之基础及过滤方式



什么是文件上传漏洞？  
文件上传漏洞有哪些危害?  
比如上传后门文件，进而拿权限等等（一句话木马）  
文件上传漏洞如何查找及判断？  
扫描、会员中心、后台系统、代码分析等等  
文件上传漏洞有哪些需要注意的地方？  
关于文件上传漏洞在实际应用中的说明?



演示案例：

✧ 常规文件上传地址的获取说明https://www.cnblogs.com/backlion/p/10421405.html

比如vip账号的url(例：https://www.easyicon.net/vip/)，再用铸剑或者御剑扫描，可以得出漏洞的url(用铸剑可以扫出https://www.easyicon.net/vip/kindeditor，说明此url有漏洞)

✧ 不同格式下的文件类型后门测试

✧ 配合解析漏洞下的文件类型后门测试

✧ 本地文件上传漏洞靶场环境搭建测试

✧ 某CMS及CVE编号（cve-2018-2894）文件上传漏洞测试

涉及资源：

https://github.com/c0ny1/upload-labs