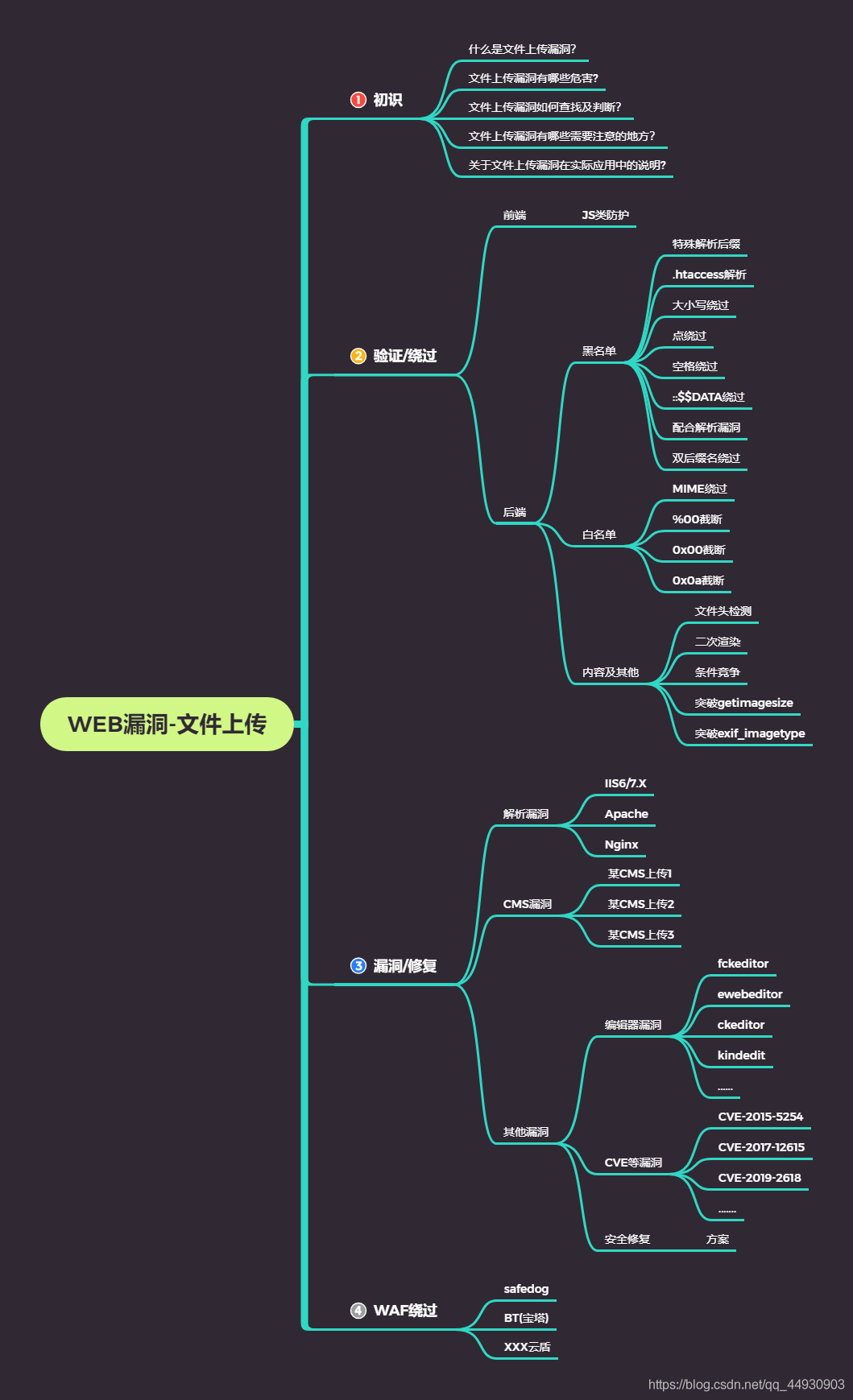
# 22 WEB漏洞-文件上传之内容逻辑数组绕过



图片一句话制作方法（或者打开文件把代码加进去）：

copy 1.png /b + shell.php /a webshell.jpg

文件头检测

图像文件信息判断

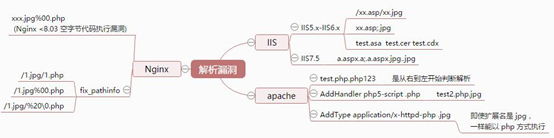
逻辑安全=二次渲染

逻辑安全-条件竞争

目录命名-x.php/.

脚本函数漏洞-CVE-2015-2348

数组接受+目录命名



演示案例：

● Uploadlabs-pass13-20关卡测试

● CVE-2017-12615-上传-Tomcat

● 中间件解析漏洞+配合文件上传测试

○ IIS-上传-解析-(panfei806)

○ Apache-上传-解析-vulhub

○ Nginx-上传-解析-vulhub

涉及资源：

https://www.smi1e.top/文件解析漏洞总结/

腾讯文档-与我共享-Web中间件常见漏洞总结.pdf

https://pan.baidu.com/s/1UfHvoS1BlYZ8SXgUKXnOxw 提取码：7ucg