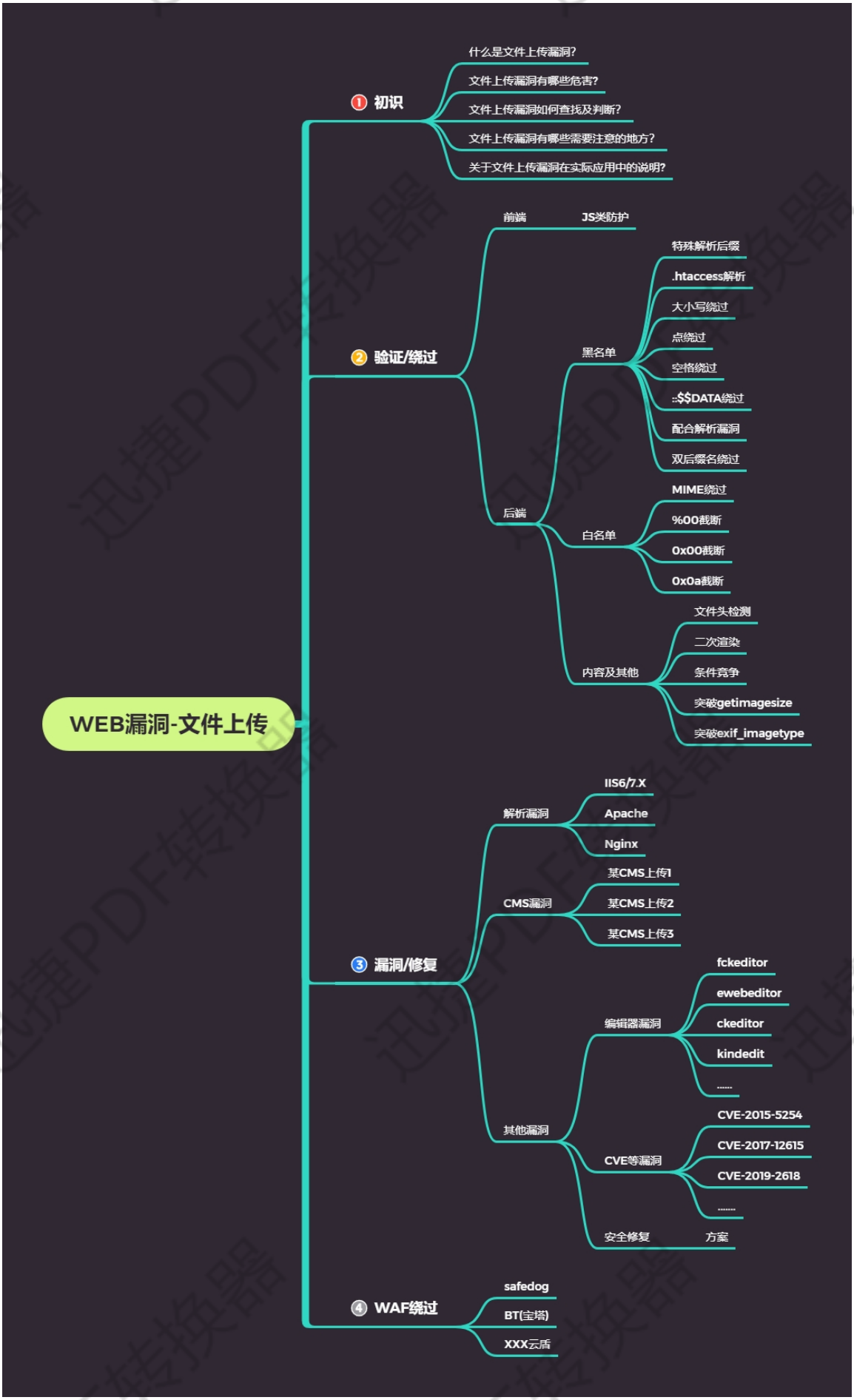
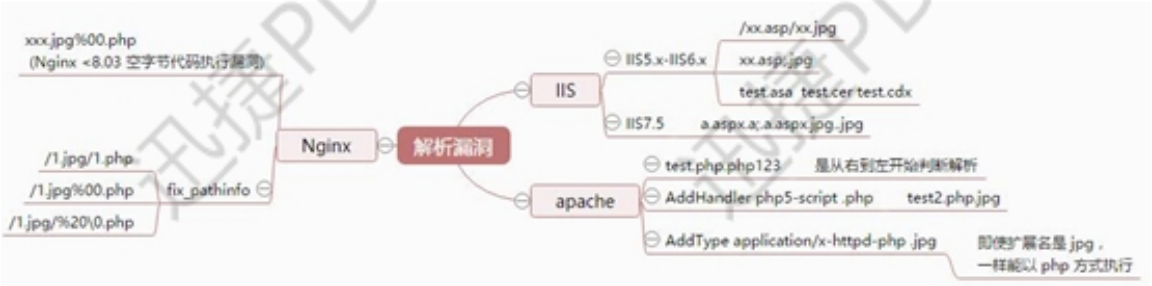
WEB 漏洞-文件上传之内容逻辑数组绕过


WEB漏洞-文件上传
① 初识
什么是文件上传漏洞?
文件上传漏洞有哪些危害?
文件上传漏洞如何查找及判断?
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?
② 验证/绕过
前端
JS类防护
后端
黑名单
特殊解析后缀
.htaccess解析
大小写绕过
点绕过
空格绕过
::$$DATA绕过
配合解析漏洞
双后缀名绕过
白名单
MIME绕过
%00截断
0x00截断
0x0a截断
内容及其他
文件头检测
二次渲染
条件竞争
突破getimagesize
突破exif_imagetype
③ 漏洞/修复
解析漏洞
IIS6/7.X
Apache
Nginx
CMS漏洞
某CMS上传1
某CMS上传2
某CMS上传3
其他漏洞
编辑器漏洞
fckeditor
ewebeditor
ckeditor
kindedit
.....
CVE等漏洞
CVE-2015-5254
CVE-2017-12615
CVE-2019-2618
.....
安全修复
方案
④ WAF绕过
safedog
BT(宝塔)
XXX云盾

图片一句话制作方法：
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
