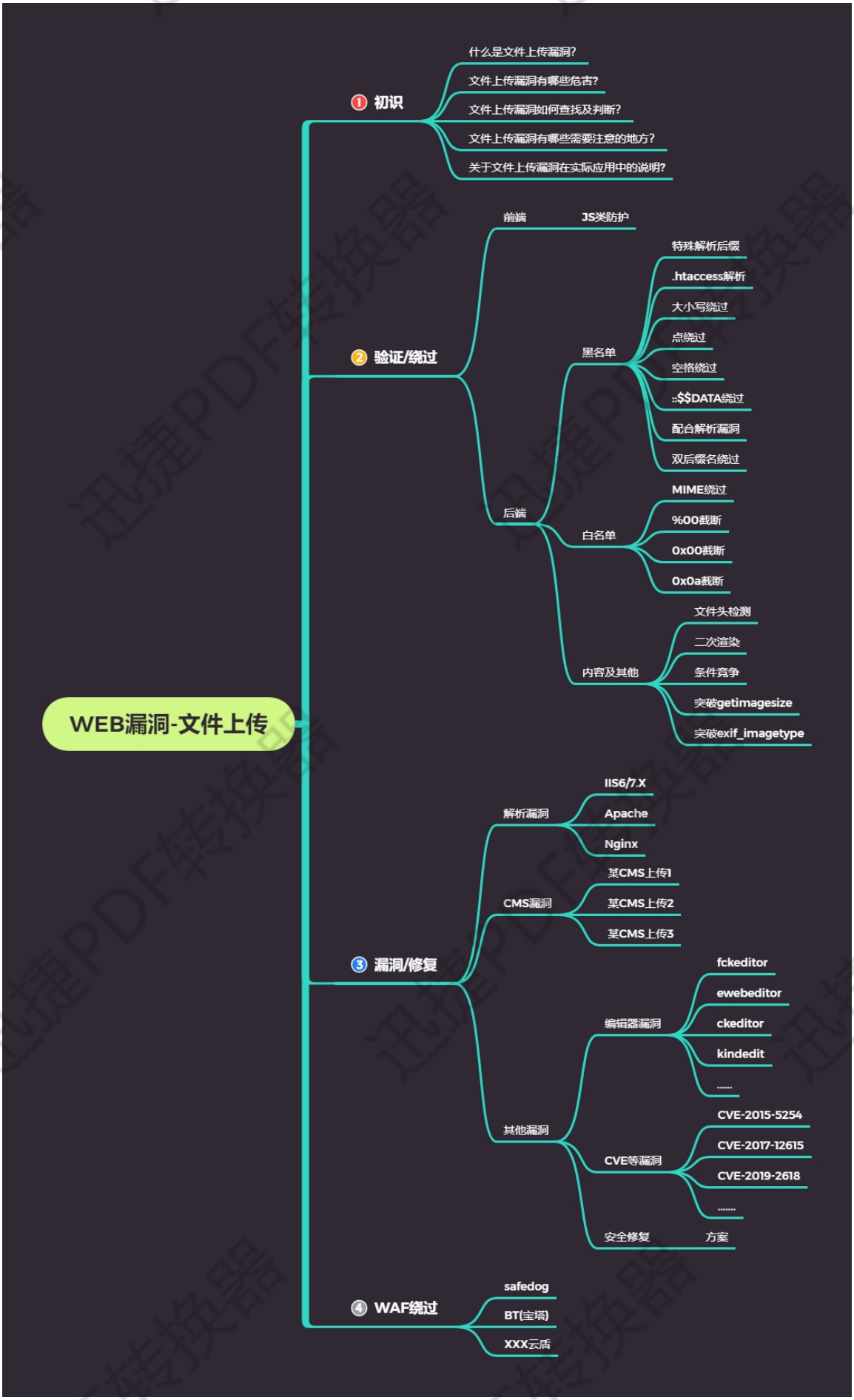
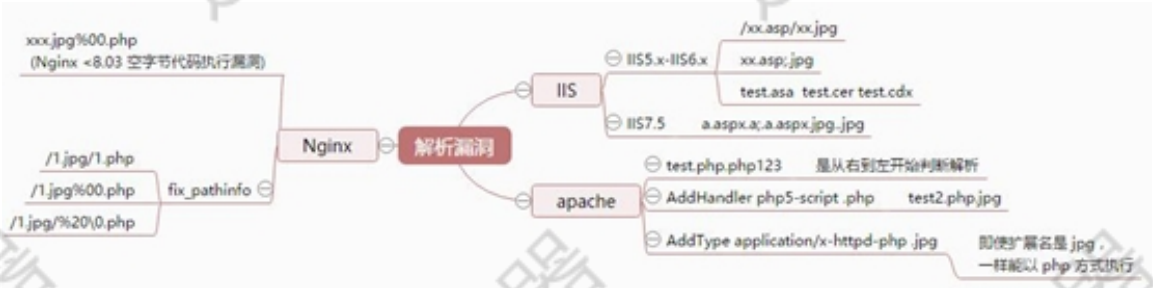
WEB 漏洞-文件上传之解析漏洞编辑器安全

迅捷PDF转换器


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



各个平台解析漏洞讲解
IIS,Apache,Nginx
各个 WEB 编辑器安全讲解
https://navisec.it/编辑器漏洞手册/
各个 CMS 文件上传简要讲解
wordpress,phpcms,

演示案例：

➢ 几种中间件解析漏洞简要演示

参考共享的中间件漏洞 PDF
IIS6/7 简要说明-本地搭建
Apache 配置安全--vulhub
Apache 解析漏洞-低版本
Apache 换行解析-vulhub
Nginx 解析漏洞-vulhub
Nginx 文件名逻辑-vulhub

➢ 几种常见 WEB 编辑器简要演示

Fckeditor exp 利用
ueditor 漏洞利用

➢ 几种常见 CMS 文件上传简要演示

通达 OA 系统

➢ 贴近实际应用下的以上知识点演示

判断中间件平台，编辑器类型或 CMS 名称进行测试

涉及资源：

https://navisec.it/编辑器漏洞手册/

https://www.jb51.net/softs/75619.html

https://pan.baidu.com/share/init?surl=5gcdBuOFrN1F9xVN7Q7GSA 

迅捷PDF转换器