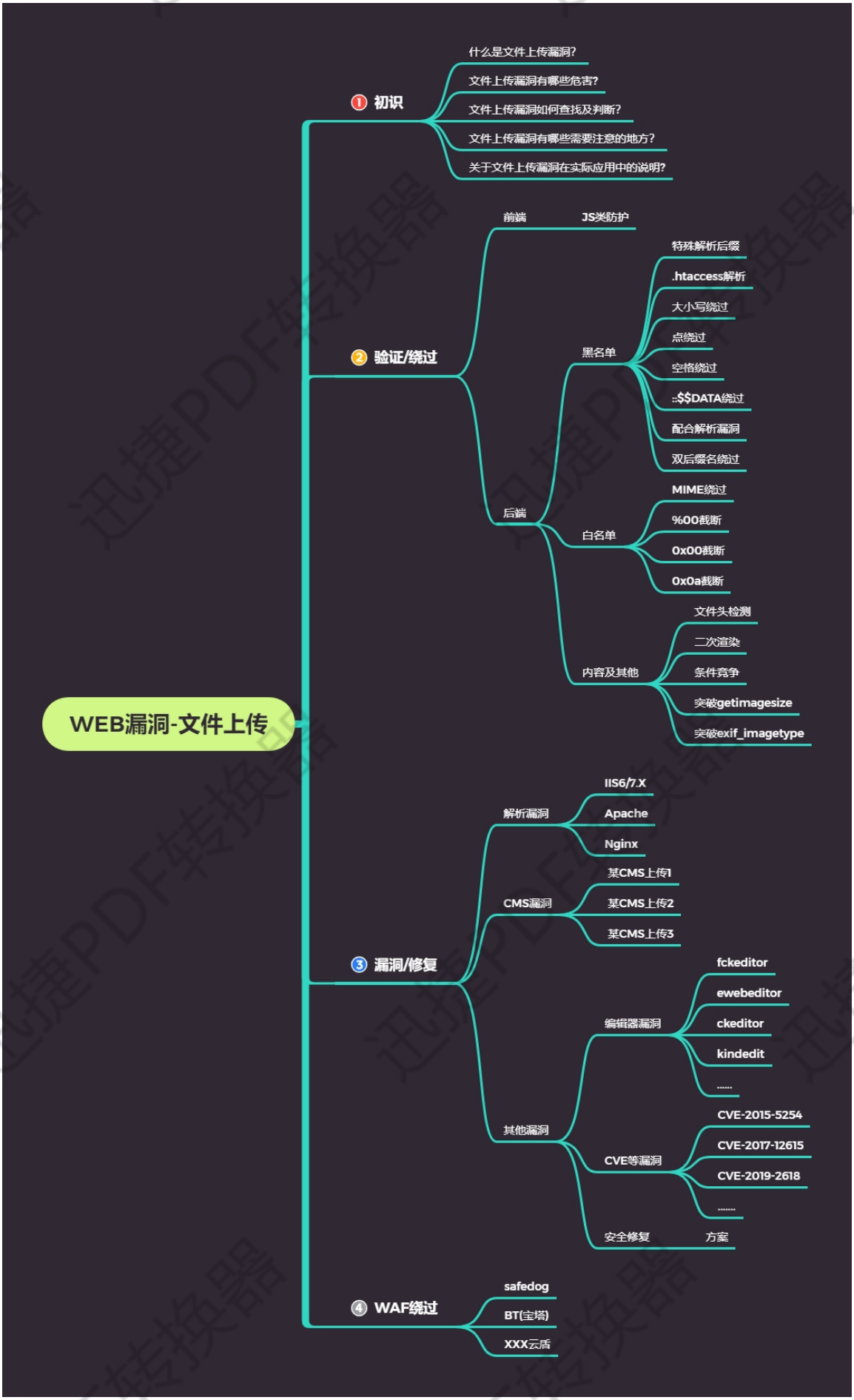
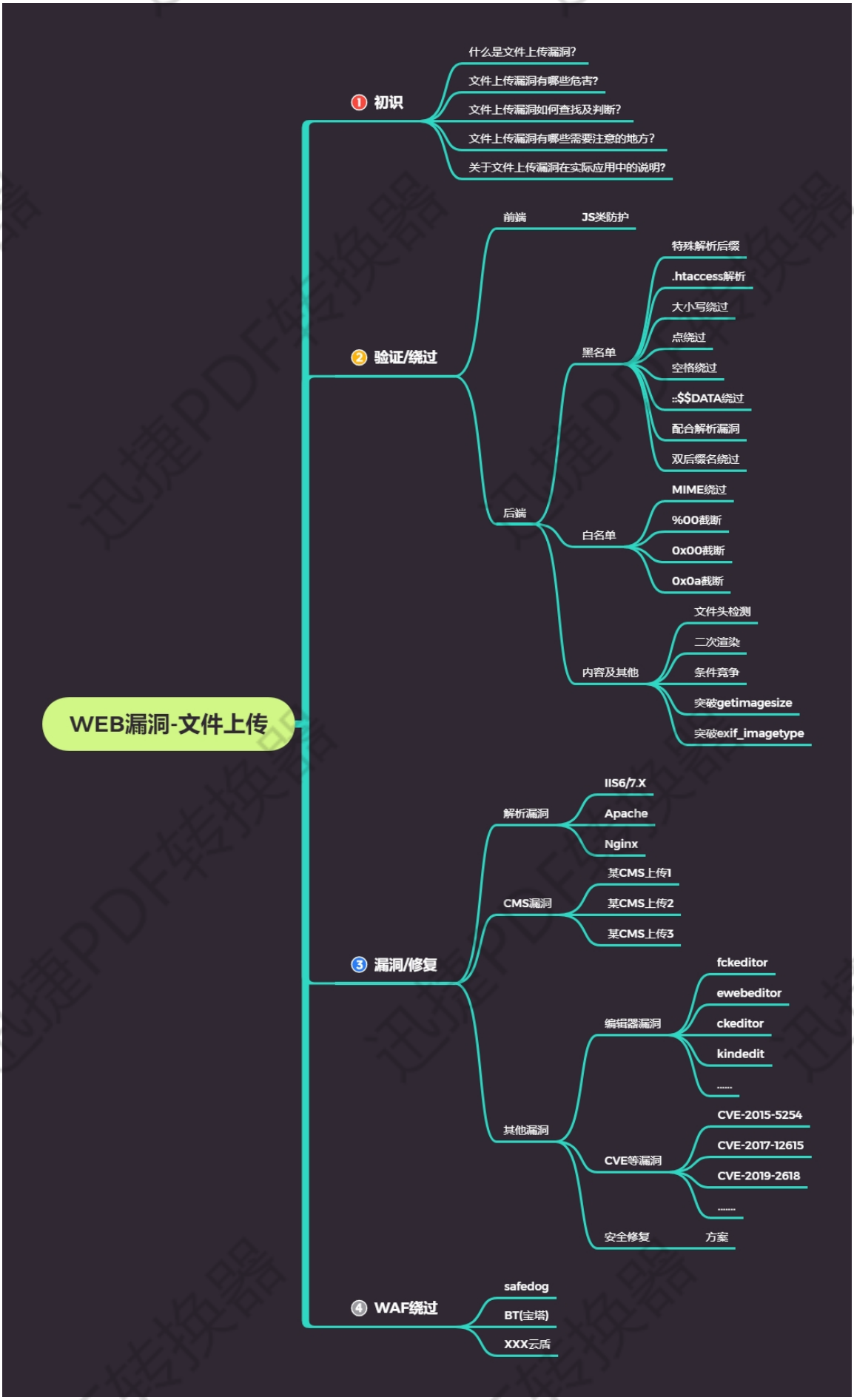
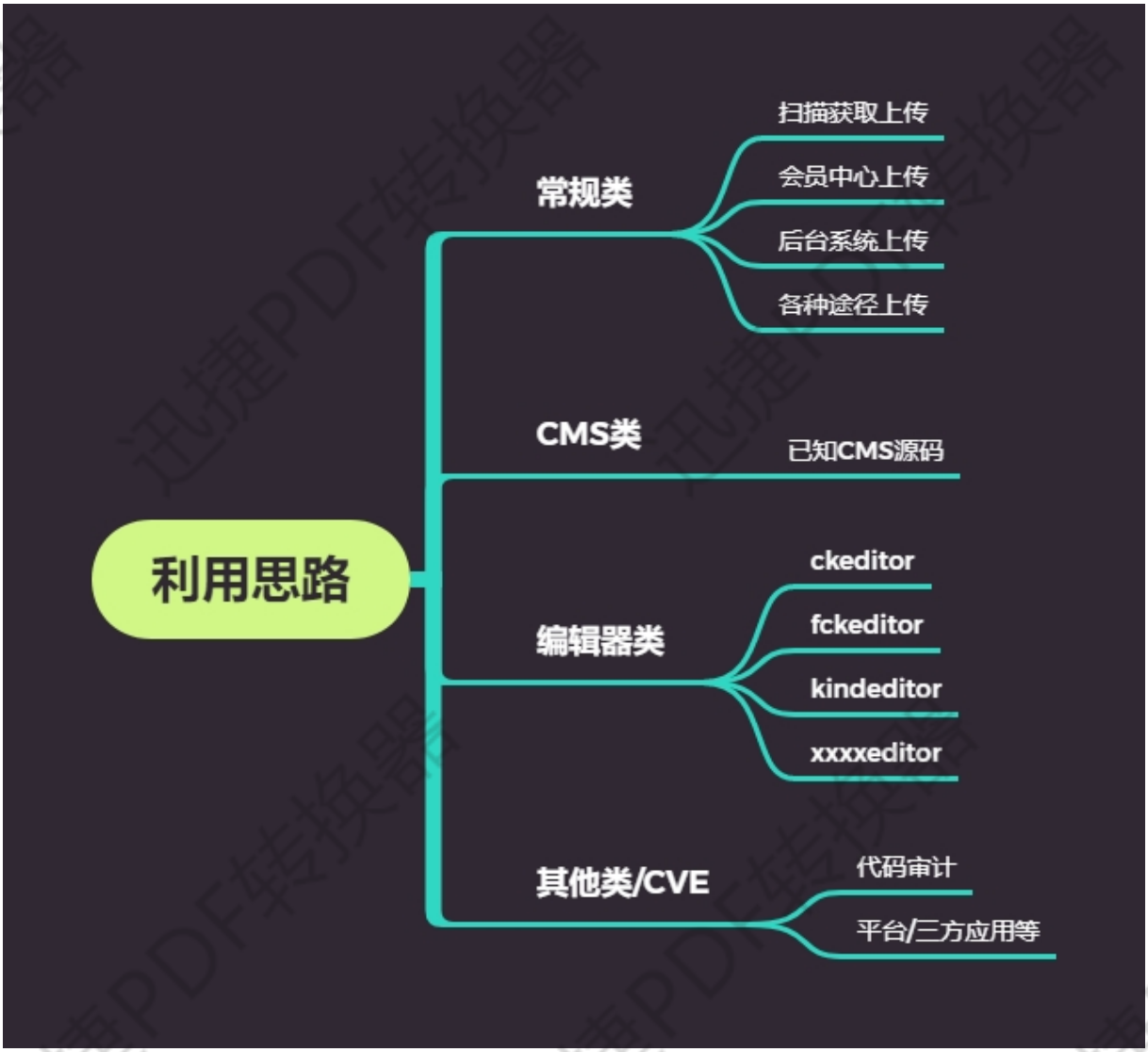
WEB 漏洞-文件上传之基础及过滤方式


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

WEB 漏洞-文件上传之基础及过滤方式


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

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？



演示案例：

- ✧ 常规文件上传地址的获取说明
- ✧ 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 编号文件上传漏洞测试