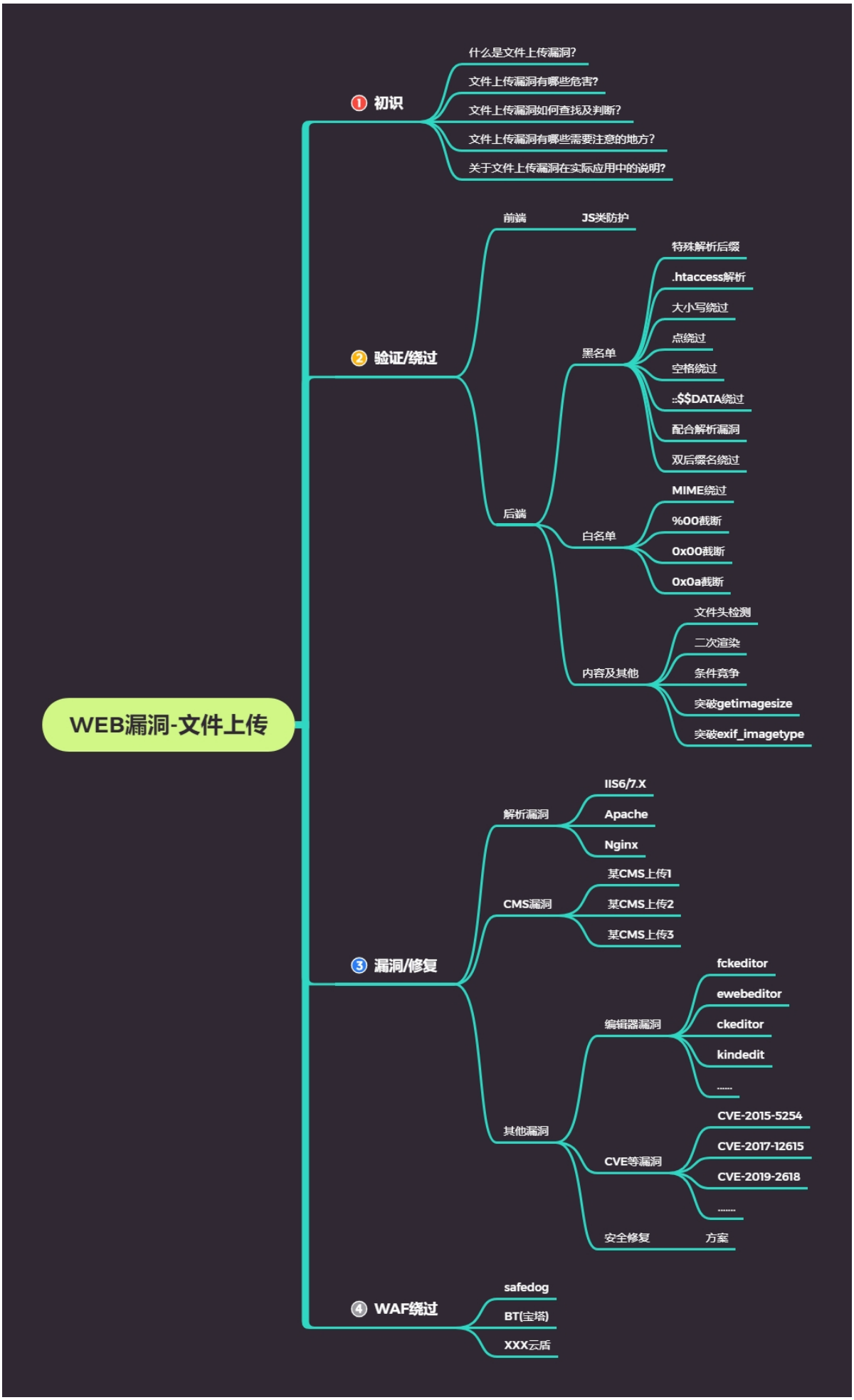
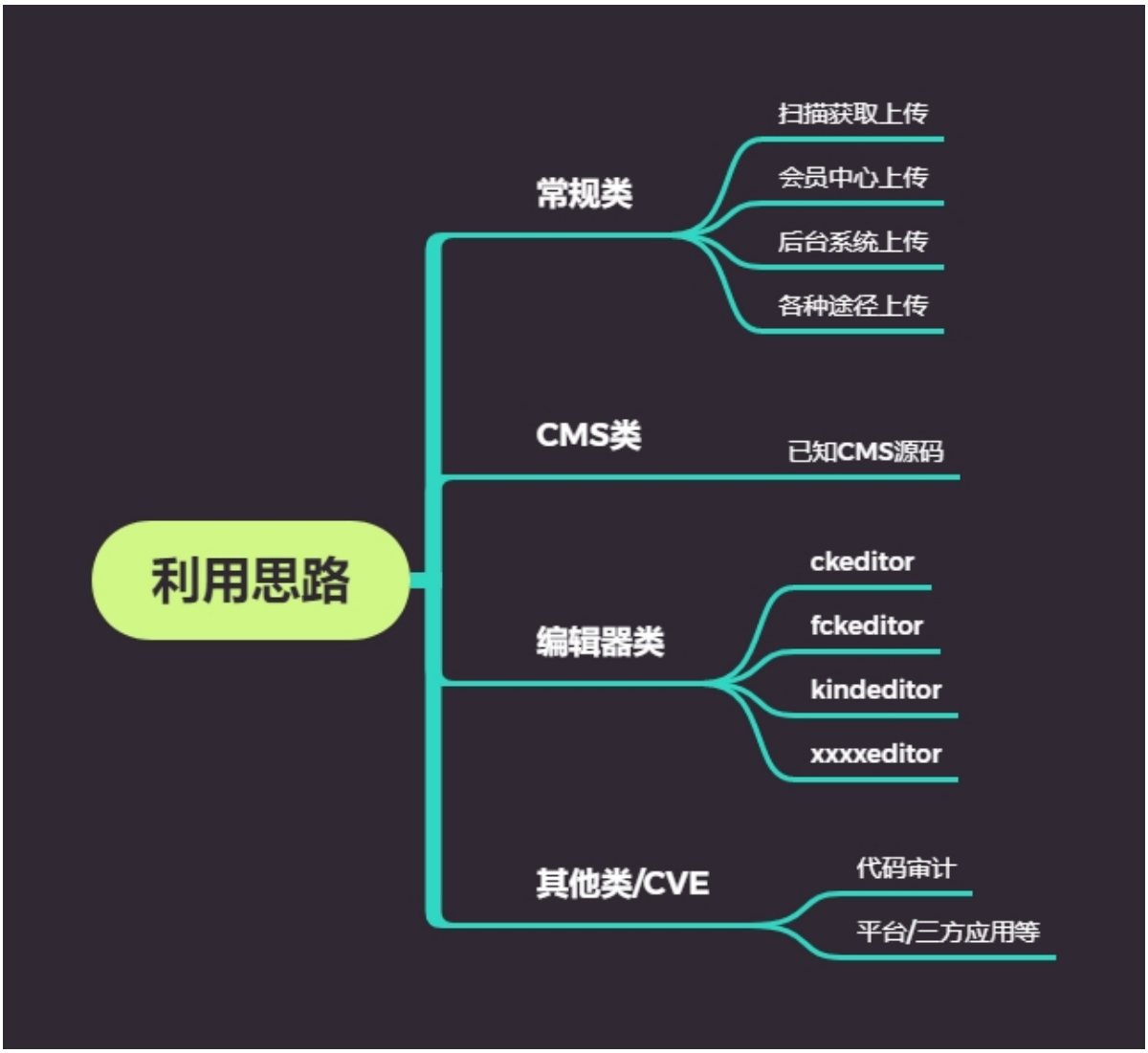
Day20　WEB漏洞–文件上传基础及过滤方式


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



20.1 什么是文件上传漏洞?

指程序对文件的上传未作全面的限制，导致用户可以上传一些超越用户权限的一些文件，可以是木马，shell脚本，病毒等。

20.2 文件上传漏洞有哪些危害?

可以通过文件上传漏洞上传webshell后门。

20.3 文件上传漏洞如何查找及判断?

- 黑盒：使用扫描工具扫描打开网站。
- 黑盒：测试会员中心，测试后台。
- 白盒：直接撸源代码。

20.4 文件上传漏洞有哪些需要注意的地方?

- 拿到漏洞后要对漏洞类型进行区分，编辑器、第三方应用、常规等。
- 区分漏洞类型

20.5 关于文件上传漏洞在实际应用中的说明?

- 上传后门脚本获取网站权限。

20.6 演示案例

- 常规文件上传地址的获取说明：上传的文件要执行的话，要按照对应代码执行。
- 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+解析漏洞=高危漏洞。
- 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：这种第三方插件的漏洞测试和常规漏洞测试是不一样的。

资源

```
1  靶场源码：https://github.com/c0ny1/upload-labs/releases
```