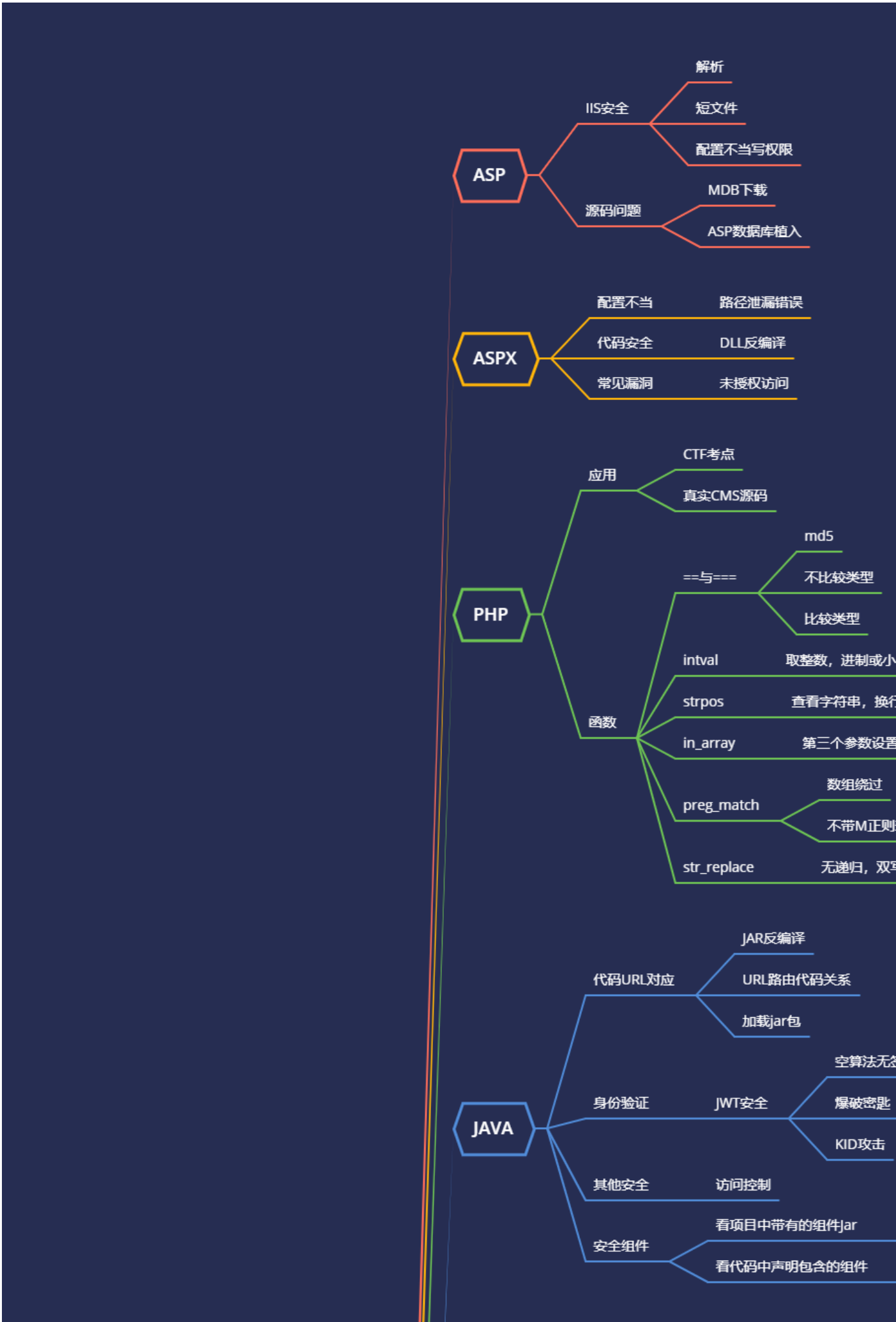
WEB 攻防-通用漏洞&文件上传&黑白盒审计&逻辑&中间件&外部引用


ASP
IIS安全
解析
短文件
配置不当写权限
源码问题
MDB下载
ASP数据库植入
ASPX
配置不当
路径泄漏错误
代码安全
DLL反编译
常见漏洞
未授权访问
PHP
应用
CTF考点
真实CMS源码
函数
==与===
md5
不比较类型
比较类型
intval
取整数，进制或小
strpos
查看字符串，换行
in_array
第三个参数设置
preg_match
数组绕过
不带M正则
str_replace
无递归，双写
JAVA
代码URL对应
JAR反编译
URL路由代码关系
加载jar包
身份验证
JWT安全
空算法无签
爆破密匙
KID攻击
其他安全
访问控制
安全组件
看项目中带有的组件jar
看代码中声明包含的组件

#知识点：

1、白盒审计三要素

2、黑盒审计四要素

3、白黑测试流程思路

#详细点：

1、检测层面：前端，后端等

2、检测内容：文件头，完整性，二次渲染等

3、检测后缀：黑名单，白名单，MIME 检测等

4、绕过技巧：多后缀解析，截断，中间件特性，条件竞争等

#本章课程内容：

1、文件上传-CTF 赛题知识点

2、文件上传-中间件解析&编辑器安全

3、文件上传-实例 CMS 文件上传安全分析

#前置：

后门代码需要用特定格式后缀解析，不能以图片后缀解析脚本后门代码(解析漏洞除外)

如：jpg 图片里面有 php 后门代码，不能被触发，所以连接不上后门

如果要图片后缀解析脚本代码，一般会利用包含漏洞或解析漏洞，还有.user.ini&.htaccess

演示案例：

- 白盒审计-Finecms-代码常规-处理逻辑
- 白盒审计-CuppaCms-中间件-.htaccess
- 白盒审计-Metinfo-编辑器引用-第三方安全

#白盒审计-Finecms-代码常规-处理逻辑

黑盒思路：寻找上传点抓包修改突破获取状态码及地址

审计流程：功能点-代码文件-代码块-抓包调试-验证测试

#白盒审计-CuppaCms-中间件-.htaccess

黑盒思路：存在文件管理上传改名突破，访问后在突破

审计流程：功能点-代码文件-代码块-抓包调试-验证测试

#白盒审计-Metinfo-编辑器引用-第三方安全

黑盒思路：探针目录利用编辑器漏洞验证测试

审计流程：目录结构-引用编辑器-编辑器安全查询-EXP 利用验证

#文件上传：

黑盒：寻找一切存在文件上传的功能应用

1、个人用户中心是否存在文件上传功能

2、后台管理系统是佛存在文件上传功能

3、字典目录扫描探针文件上传构造地址

4、字典目录扫描探针编辑器目录构造地址

白盒：看三点，中间件，编辑器，功能代码

1、中间件直接看语言环境常见搭配

2、编辑器直接看目录机构或搜索关键字

3、功能代码直接看源码应用或搜索关键字

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址