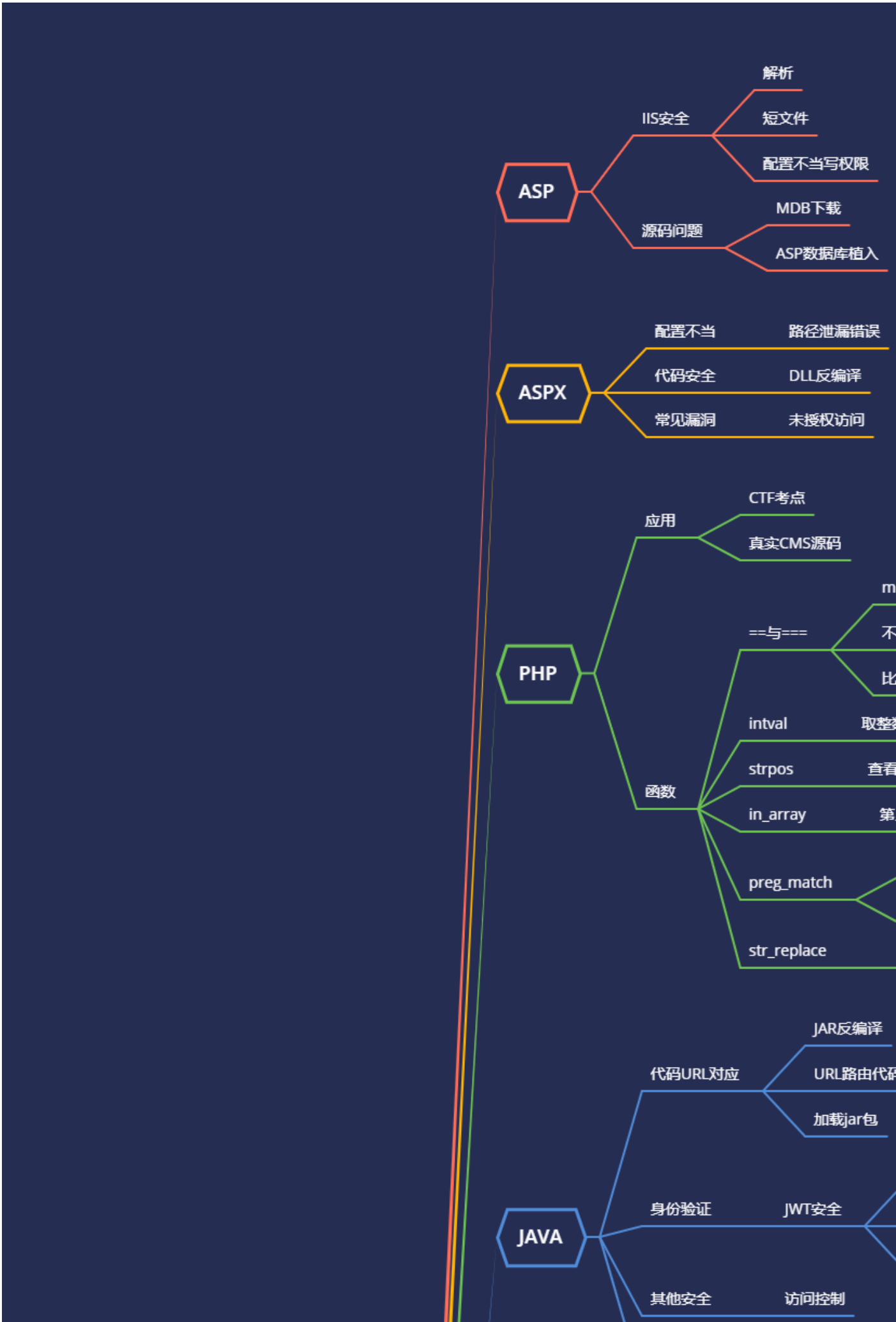
WEB 攻防-通用漏洞&SQL 注入&Tamper 脚本 &Base64&Json&md5 等


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===
intval
strpos
in_array
preg_match
str_replace
JAVA
代码URL对应
JAR反编译
URL路由代
加载jar包
身份验证
JWT安全
其他安全
访问控制

#知识点：

1、数据表现格式类型注入

2、字符转义绕过-宽字节注入

3、数字&字符&搜索&编码&加密等

#参考资料：

https://www.cnblogs.com/bmjoker/p/9326258.html

扫描，利用工具等都不会自动判断数据类型，格式等，所以即使有漏洞也测不出来，具体还是需要人工的去观察，进行工具的修改或加载插件再次探针才可以。

#SQL 注入课程体系：

1.数据库注入 - access mysql mssql oracle mongodb postgresql 等

2.数据类型注入 - 数字型 字符型 搜索型 加密型(base64 json)等

3.提交方式注入 - get post cookie http 头等

4.查询方式注入 - 查询 增加 删除 更新 堆叠等

5.复杂注入利用 - 二次注入 dnslog 注入 绕过 bypass 等

演示案例：

- 本地源码-数字&字符&搜索&编码&JSON
- 墨者靶场-字符转义处理防护-宽字节注入
- 真实 WEB-数据编码接受处理-base64 注入
- 真实 WEB-JSON 数据格式&MD5 加密数据
- 工具脚本-SQLMAP-脚本 Tamper 使用指南

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址
