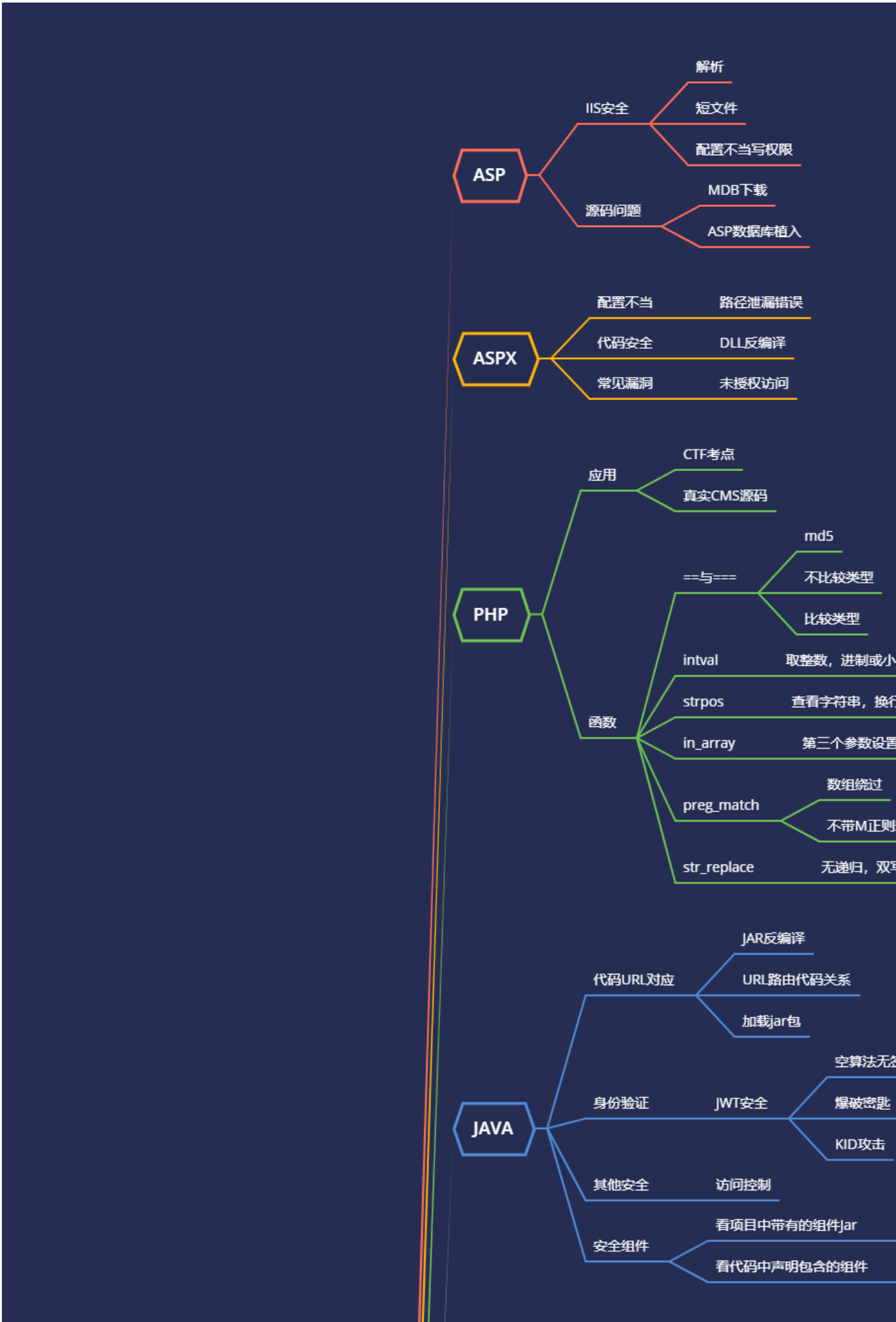
# WEB 攻防-通用漏洞&文件上传&中间件解析漏洞&编辑器安全


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、中间件安全问题

2、中间件文件上传解析

3、Web 应用编辑器上传

#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：

- 中间件文件解析-IIS&Apache&Nginx
- Web 应用编辑器-Ueditor 文件上传安全
- 实例 CMS&平台-中间件解析&编辑器引用

---

#中间件文件解析-IIS&Apache&Nginx

-IIS 6 7 文件名 目录名

1、文件名：x.asp;.x.jpg

2、目录名：x.asp/x.jpg

3、IIS7.X 与 Nginx 解析漏洞一致

-Apache 换行解析 配置不当

1、换行解析-CVE-2017-15715

其 2.4.0~2.4.29 版本中存在一个解析漏洞

2、配置不当-.htaccess 配置不当

AddHandler application/x-httpd-php .php

-Nginx 文件名逻辑 解析漏洞

1、文件名逻辑-CVE-2013-4547

影响版本：Nginx 0.8.41 ~ 1.4.3 / 1.5.0 ~ 1.5.7

2、解析漏洞-nginx.conf 配置不当

由此可知，该漏洞与 Nginx、php 版本无关，属于用户配置不当造成的解析漏洞。

#Web 应用编辑器-Ueditor 文件上传安全

```
<form
action="http://192.168.46.139/net/controller.ashx?action=catchima
ge" enctype="multipart/form-data" method="POST">
<p>shell addr: <input type="text" name="source[]" /></p>
<input type="submit" value="Submit" />
</form>
```

#实例 CMS&平台-中间件解析&编辑器引用

1、中间件配置不当导致文件被恶意解析

2、CMS 源码引用外部编辑器实现文件上传