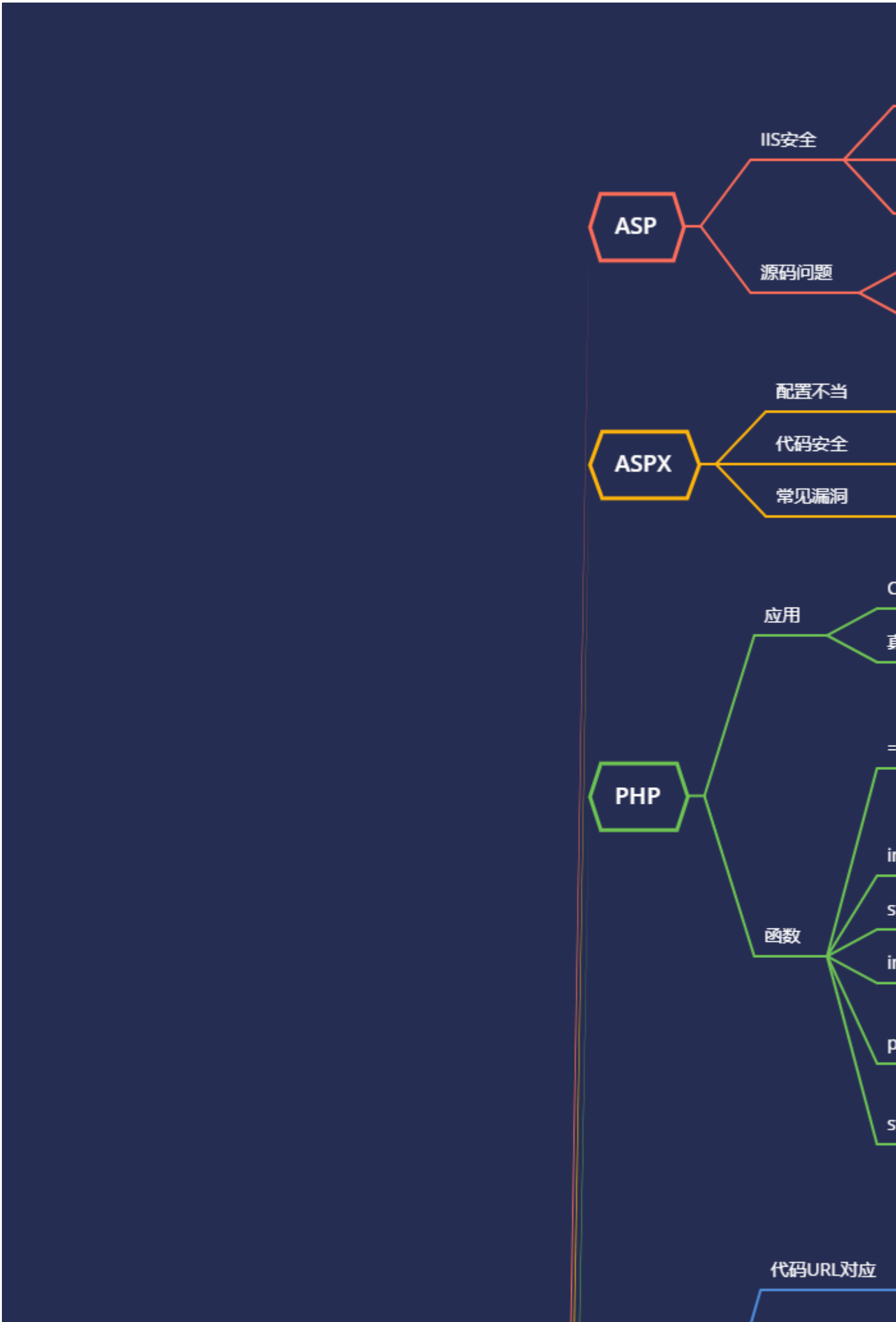
WEB 攻防-通用漏洞&业务逻辑&水平垂直越权&访问控制&脆弱验证


IIS安全
ASP
源码问题
配置不当
ASPX
代码安全
常见漏洞
应用
PHP
函数
代码URL对应

#知识点：

1、水平越权-同级用户权限共享

2、垂直越权-低高用户权限共享

3、访问控制-验证丢失&取消验证

4、脆弱验证-Cookie&Token&Jwt 等

#前置知识：

1、逻辑越权原理-

-水平越权：用户信息获取时未对用户与 ID 比较判断直接查询等

-垂直越权：数据库中用户类型编号接受篡改或高权限操作未验证等

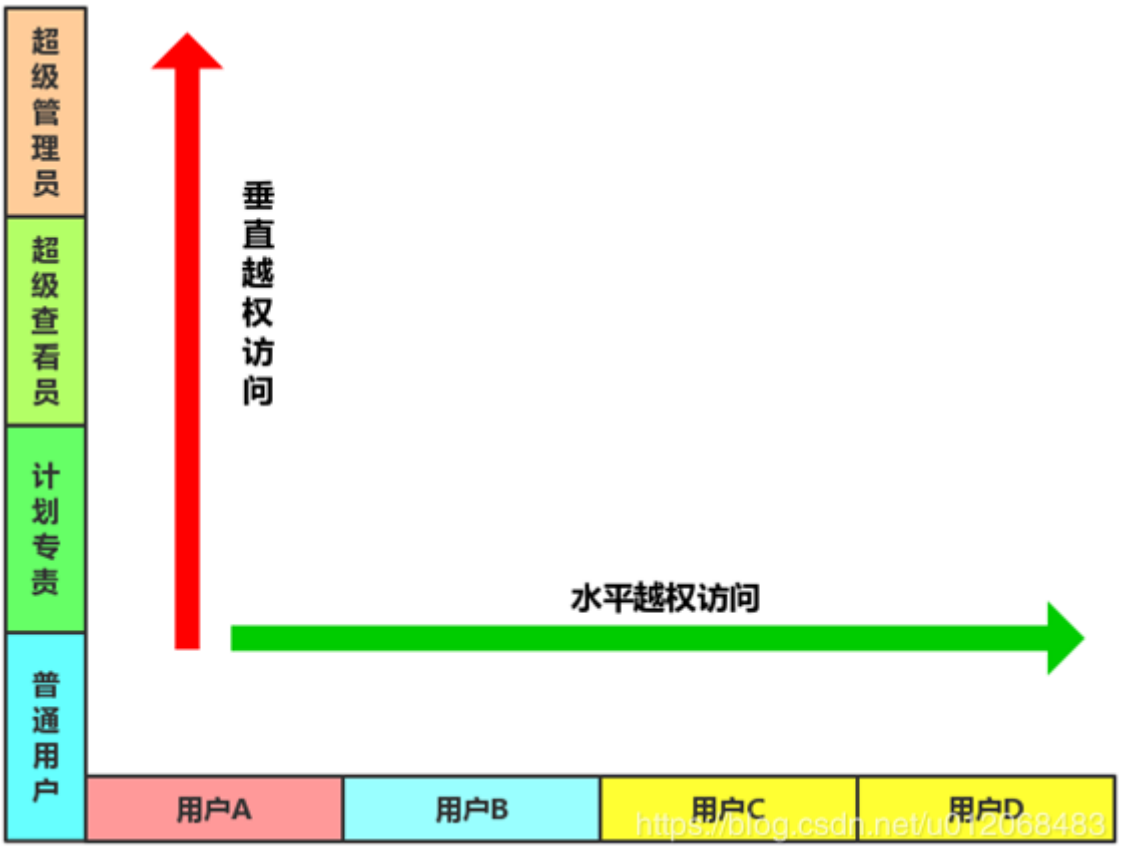
2、访问控制原理-

-验证丢失：未包含引用验证代码文件等

-取消验证：支持空口令,匿名,白名单等

3、脆弱验证原理-

-Cookie&Token&Jwt：不安全的验证逻辑等



演示案例：

- 权限-水平越权-YXCMS-检测数据比对弱
- 权限-垂直越权-MINICMS-权限操作无验证
- 未授权-访问控制-XHCMS-代码未引用验证
- 未授权-脆弱机制-XHCMS-Cookie 脆弱验证
- 弱机制-空口令机制-Redis&Weblogic 弱机制
- 检测类-工具项目-Authz&Secscan-Authcheck

```
#权限-水平越权-YXCMS-检测数据比对弱
只检测用户和 ID 对应关系，没检测当前操作用户是不是当前用户

#权限-垂直越权-MINICMS-权限操作无验证
后台数据包访问先执行后判断登录等于无效

#未授权-访问控制-XHCMS-代码未引用验证
#未授权-脆弱机制-XHCMS-Cookie 脆弱验证
app="熊海内容管理系统(SEACMS)"

#弱机制-空口令机制-Redis&Weblogic 弱机制
http://vulfocus.io/
https://vulhub.org/
"weblogic" && port="7001"

#检测类-工具项目-Authz&Secscan-Authcheck
安装踩坑：https://bigyoung.cn/posts/250/
https://github.com/ztosec/secscan-authcheck
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址
