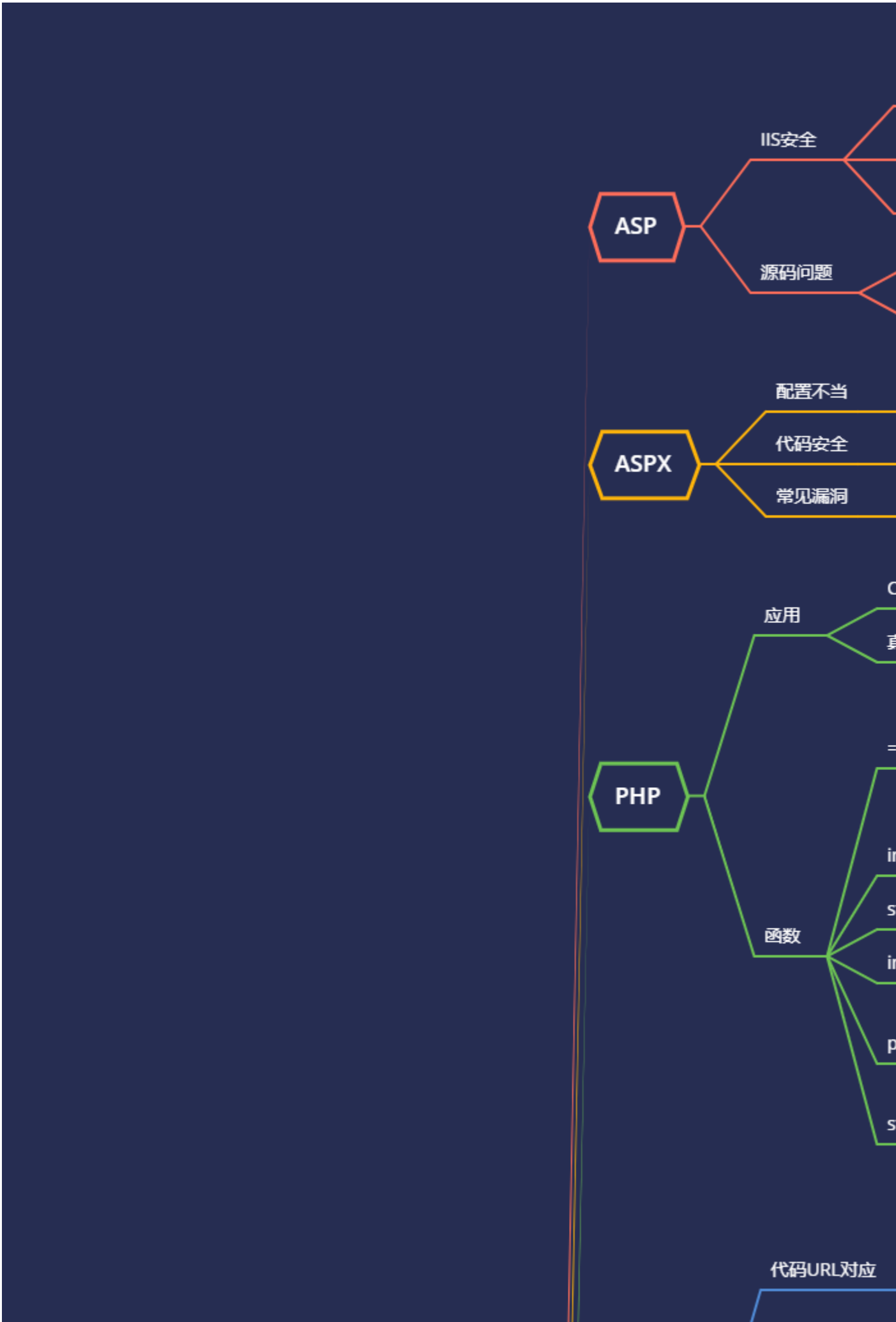
# WEB 攻防-通用漏洞&任意文件下载&删除重装&敏感读取&黑白审计


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、文件操作类安全问题

2、文件下载&删除&读取

3、白盒&黑盒&探针分析

#详细点：

文件读取：基本和文件下载利用类似

文件下载：利用下载获取源码或数据库配置文件及系统敏感文件为后续出思路

文件删除：除自身安全引发的文件删除外，可配合删除重装锁定文件进行重装

---

演示案例：

- 审计分析-文件下载-XHCMS-功能点
- 审计分析-文件读取-MetInfo-函数搜索
- 审计分析-文件删除-74CMS-函数搜索
- 黑盒分析-下载读取-下载资源 URL 参数

---

#白盒审计：

1、文件下载

流程-功能点抓包-寻代码文件-寻变量控制-构造测试

Payload: softadd=d:/1.txt softadd2=d:/1.txt

2、文件删除：74CMS-配合删除重装

流程-特定函数搜索-寻触发调用-构造 Payload 测试

Payload:

/admin/admin_article.php?act=del_img&img=../../data/install.lock

3、文件读取：MetInfo-任意读取

流程-特定函数搜索-寻触发调用-构造 Payload 测试

Payload：/include/thumb.php?dir=http\..\..\config\config_db.php

#黑盒探针

1、URL 参数名及参数值分析：

参数名：英文对应翻译

参数值：目录或文件名

2、功能点自行修改后分析：

文件下载，删除，读取等

涉及资源:

补充：涉及录像课件资源软件包资料等下载地址