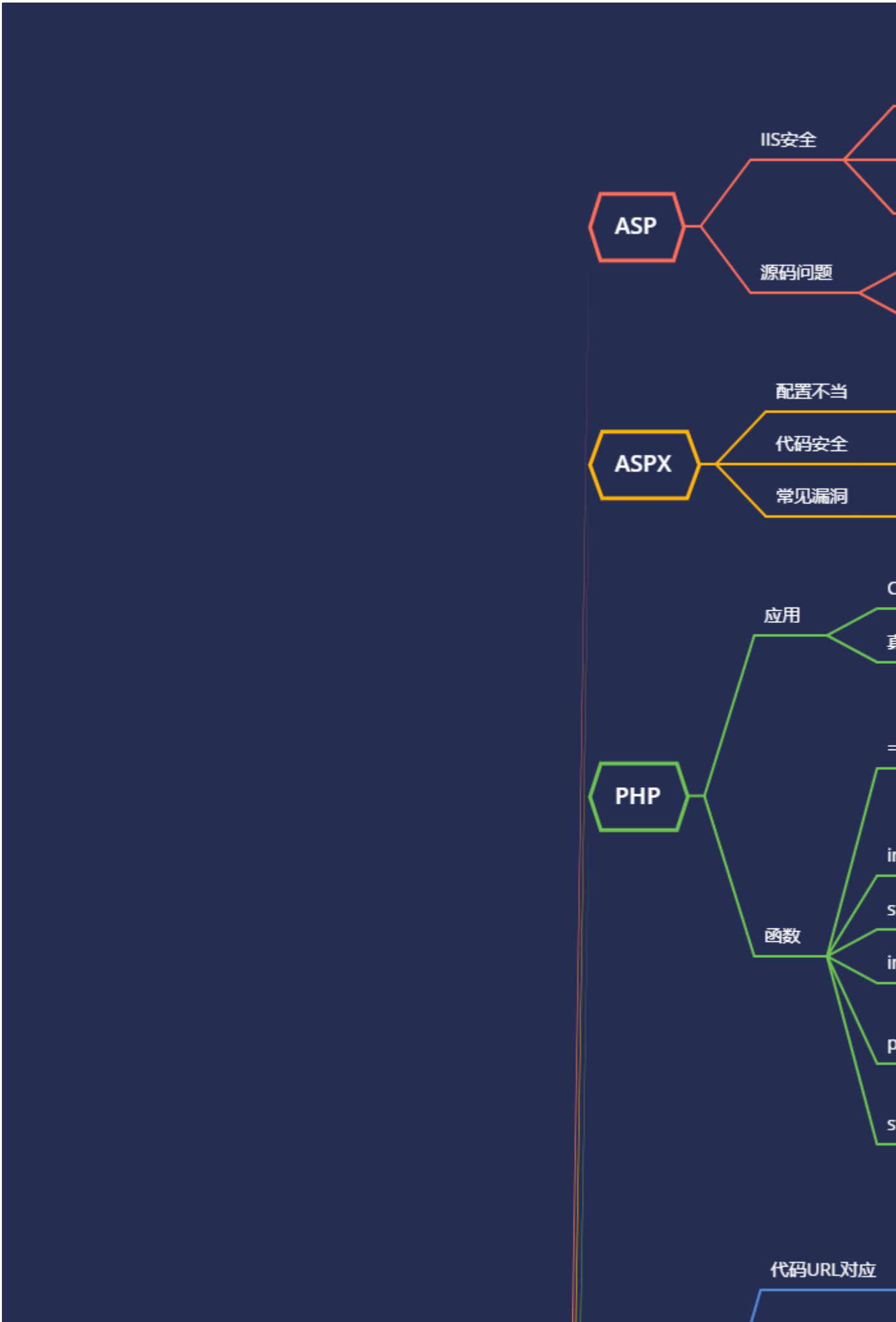
WEB 攻防-通用漏洞&跨域 CORS 资源&JSONP 回调&域名接管劫持


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、子域名接管-检测&探针&利用

2、COSP 跨域资源-检测&探针&利用

3、JSONP 跨域回调-检测&探针&利用

#前置知识点：

-同源策略(SOP)-"同源"包括三个条件：同协议 同域名 同端口

同源策略限制从一个源加载的文档或脚本与来自另一个源的资源进行交互,这是一个用于隔离潜在恶意文件的关键的安全机制.简单说就是浏览器的一种安全策略。

虽然同源策略在安全方面起到了很好的防护作用,但也在一定程度上限制了一些前端功能的实现,所以就有了许多跨域的手段。

-子域名接管：

域名解析记录指向域名，对应主机指向了一个当前未在使用或已经删除的特定服务，攻击者通过注册指向域名，从而控制当前域名的控制权，实现恶意软件分发、网络钓鱼/鱼叉式网络钓鱼、XSS 、身份验证绕过等。子域名接管不仅仅限于 CNAME 记录，NS,MX 甚至 A 记录也会受到影响。

检测项目：

https://github.com/pwnesia/dnstake

https://github.com/anshumanbh/tko-subs

https://github.com/mhmdiaa/second-order

https://github.com/r3curs1v3-pr0xy/sub404

https://github.com/Echocipher/Subdomain-Takeover

-COSP 跨域资源

CORS 全称 Cross-Origin Resource Sharing, 跨域资源共享，是 HTML5 的一个新特性，已被所有浏览器支持，跨域资源共享(CORS)是一种放宽同源策略的机制，它允许浏览器向跨源服务器，发出 XMLHttpRequest 请求，从而克服了 AJAX 只能同源使用的限制，以使不同的网站可以跨域获取数据。

Access-Control-Allow-Origin：指定哪些域可以访问域资源。例如，如果 requester.com 想要访问 provider.com 的资源，那么开发人员可以使用此标头安全地授予 requester.com 对 provider.com 资源的访问权限。

Access-Control-Allow-Credentials：指定浏览器是否将使用请求发送 cookie。仅当 allow-credentials 标头设置为 true 时，才会发送 Cookie。

Access-Control-Allow-Methods：指定可以使用哪些 HTTP 请求方法（GET，PUT，DELETE 等）来访问资源。此标头允许开发人员通过在 requester.com 请求访问 provider.com 的资源时，指定哪些方法有效来进一步增强安全性。

检测项目：https://github.com/chenjj/CORScanner

演示案例：

- CORS 资源跨域-敏感页面源码获取
- JSONP 回调跨域-某牙个人信息泄露
- 子域名接管-瓜迪个人子域名劫持接管
- 检测项目-CORS&JSONP&子域名接管

```
#CORS 资源跨域-敏感页面源码获取
复现步骤：
1、本地搭建访问页面跨域调用 URL
2、受害者访问当前页面被资源共享

#JSONP 回调跨域-某牙个人信息泄露
复现步骤：
1、登录某牙找到回调有敏感信息
2、本地搭建访问页面跨域调用 URL
3、访问本地页面可获取当前某牙信息

#子域名接管-瓜迪个人子域名劫持接管
复现步骤：:xiaodi8.com
1、通过检测 cname 获取指向
2、发现 testxiaodi.fun 过期受控
3、注册 testxiaodi.fun 实现控制

#检测项目-CORS&JSONP&子域名接管
1、python cors_scan.py -i top_100_domains.txt -t 100
2、人工排查+burpsuite 安装 Jsonp_Hunter.py 抓包使用
3、dnsub 爬取子域名筛选接管
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址