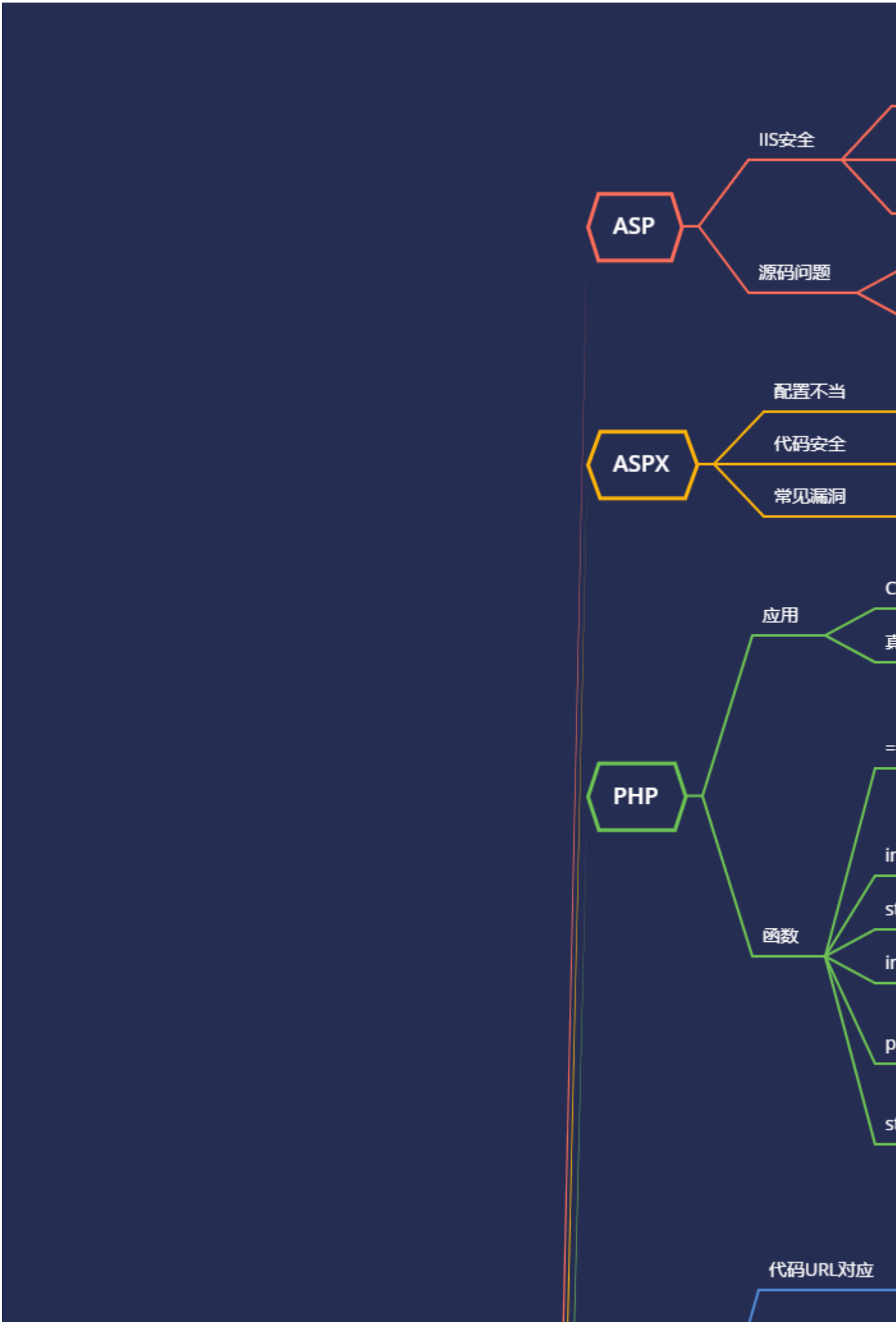
WEB 攻防-通用漏洞&CSRF&SSRF&代码审计&同源策略&加载函数


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、CSRF-审计-复现测试&同源策略

2、SSRF-审计-功能追踪&函数搜索

#详细点：

CSRF 全称：Cross-site request forgery，即，跨站请求伪造，也被称为 “One Click Attack” 或 “Session Riding”，通常缩写为 CSRF 或者 XSRF，是一种对网站的恶意利用。举个生活中的例子：就是某个人点了个奇怪的链接，自己什么也没输，但自己的 qq 号或其他的号就被盗了。即该攻击可以在受害者不知情的情况下以受害者名义伪造请求，执行恶意操作，具有很大的危害性。

CSRF 的攻击过程两个条件：

1、目标用户已经登录了网站，能够执行网站的功能。

2、目标用户访问了攻击者构造的 URL。

CSRF 安全问题黑盒怎么判断：

1、看验证来源不-修复

2、看凭据有无 token--修复

3、看关键操作有无验证-修复

-CSRF 安全问题白盒怎么审计：

同黑盒思路一样，代码中分析上述三看

SSRF(Server-Side Request Forgery:服务器端请求伪造） 是一种由攻击者构造形成由服务端发起请求的一个安全漏洞。一般情况下，SSRF 攻击的目标是从外网无法访问的内部系统。（正是因为它是由服务端发起的，所以它能够请求到与它相连而与外网隔离的内部系统）SSRF 形成的原因大都是由于服务端提供了从其他服务器应用获取数据的功能且没有对目标地址做过滤与限制。比如从指定 URL 地址获取网页文本内容，加载指定地址的图片，下载等等。

-SSRF 黑盒可能出现的地方：

1.社交分享功能：获取超链接的标题等内容进行显示

2.转码服务：通过 URL 地址把原地址的网页内容调优使其适合手机屏幕浏览

3.在线翻译：给网址翻译对应网页的内容

4.图片加载/下载：例如富文本编辑器中的点击下载图片到本地；通过 URL 地址加载或下载图片

5.图片/文章收藏功能：主要其会取 URL 地址中 title 以及文本的内容作为显示以求一个好的用具体验

6.云服务厂商：它会远程执行一些命令来判断网站是否存活等，所以如果可以捕获相应的信息，就可以进行 ssrf 测试

7.网站采集，网站抓取的地方：一些网站会针对你输入的 url 进行一些信息采集工作

8.数据库内置功能：数据库的比如 mongodb 的 copyDatabase 函数

演示案例：

- 代码审计-CSRF-SCMSFH 无验证
- 代码审计-CSRF-ZBLOG 同源策略
- 代码审计-SSRF-Yzmcms 功能&函数

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址