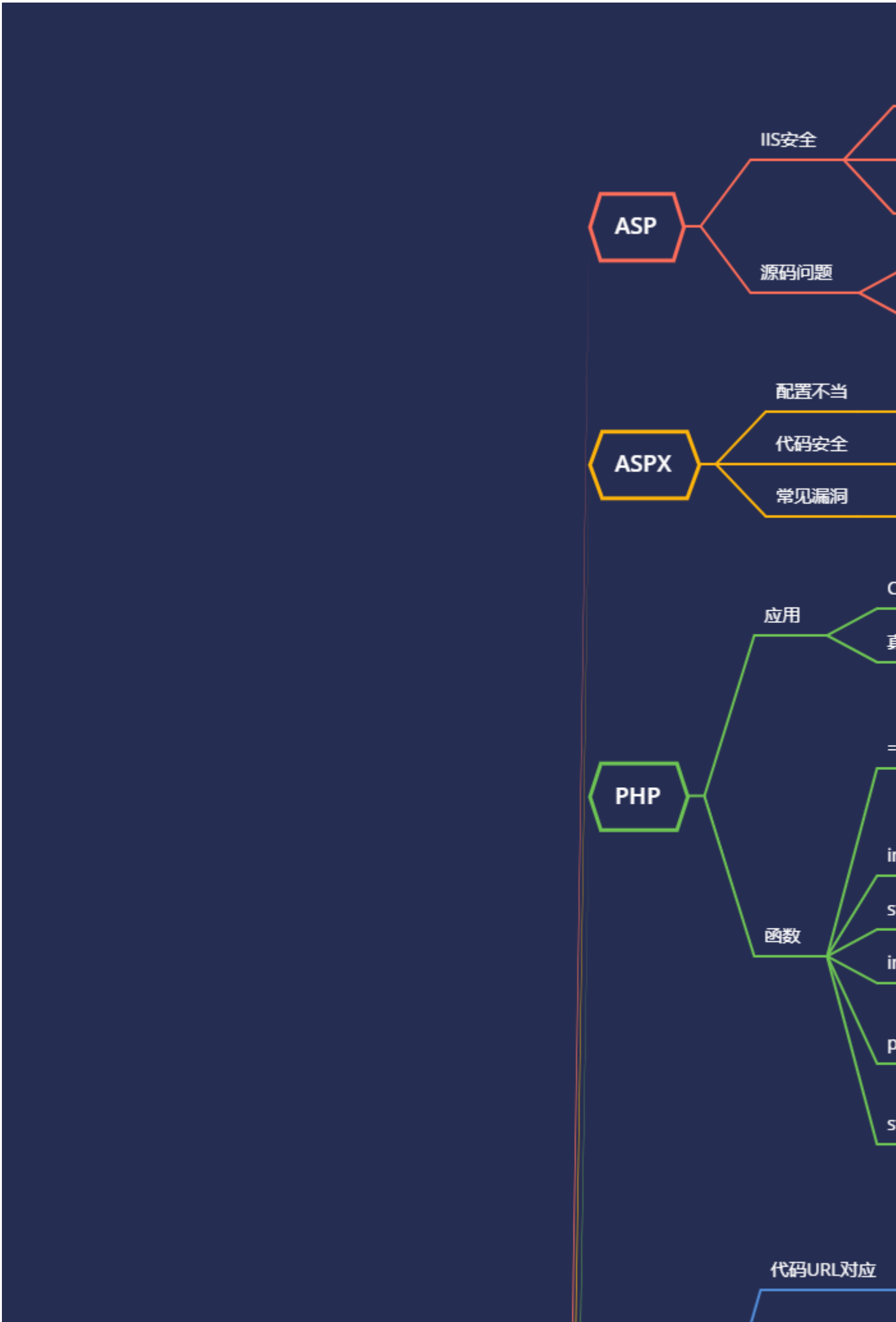
WEB 攻防-通用漏洞&CRLF 注入&URL 重定向&资源处理拒绝服务


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、CRLF 注入-原理&检测&利用

2、URL 重定向-原理&检测&利用

3、Web 拒绝服务-原理&检测&利用

#下节预告：

1、JSONP&CORS 跨域

2、域名安全-接管劫持

#详细点：

1.CRLF 注入漏洞，是因为 Web 应用没有对用户输入做严格验证，导致攻击者可以输入一些恶意字符。攻击者一旦向请求行或首部中的字段注入恶意的 CRLF，就能注入一些首部字段或报文主体，并在响应中输出，所以又称为 HTTP 响应拆分漏洞。

如何检测安全问题：CRLFuzz

2.URL 重定向跳转

写代码时没有考虑过任意 URL 跳转漏洞，或者根本不知道/不认为这是个漏洞；

写代码时考虑不周,用取子串、取后缀等方法简单判断，代码逻辑可被绕过；

对传入参数做一些奇葩的操作(域名剪切/拼接/重组)和判断，适得其反，反被绕过；

原始语言自带的解析 URL、判断域名的函数库出现逻辑漏洞或者意外特性,可被绕过；

原始语言、服务器/容器特性、浏览器等对标准 URL 协议解析处理等差异性导致绕过；

3.Web 拒绝服务

现在有许多资源是由服务器生成然后返回给客户端的，而此类"资源生成"接口如若有参数可以被客户端控制（可控），并没有做任何资源生成大小限制，这样就会造成拒绝服务风险，导致服务器处理不过来或占用资源去处理。

演示案例：

- CRLF 注入-原理&检测&利用
- URL 重定向-原理&检测&利用
- WEB 拒绝服务-原理&检测&利用

#案例 1-CRLF 注入原理&检测&利用

vulhub nginx

%0aSet-cookie:JSPSESSID%3Ddrops

url=%0d%0a%0d%0a<img src=1 onerror=alert(/xss/)>/

CRLFuzz：https://github.com/dwisiswant0/crlfuzz/releases

#案例 2-URL 重定向&原理&检测&利用

http://xxx/zb_system/login.php?url=http://www.xiaodi8.com/zb_system/login.php

大概意思是讲重定向漏洞的危害：网站接受用户输入的链接，跳转到一个攻击者控制的网站，可能导致跳转过去的用户被精心设置的钓鱼页面骗走自己的个人信息和登录口令。国外大厂的一个任意 URL 跳转都 500$、1000$了，国内看运气~

业务：

用户登录、统一身份认证处，认证完后会跳转

用户分享、收藏内容过后，会跳转

跨站点认证、授权后，会跳转

站内点击其它网址链接时，会跳转

黑盒看参数名：

redirect

redirect_to

redirect_url

url

jump

jump_to

target

to

link

linkto

domain

白盒看代码块：

Java：response.sendRedirect(request.getParameter("url"))

PHP：

```
$redirect_url = $_GET['url'];
header("Location: " . $redirect_url)
```

.NET：

```
string redirect_url = request.QueryString["url"];
Response.Redirect(redirect_url);
```

Django：

```
redirect_url = request.GET.get("url")
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址