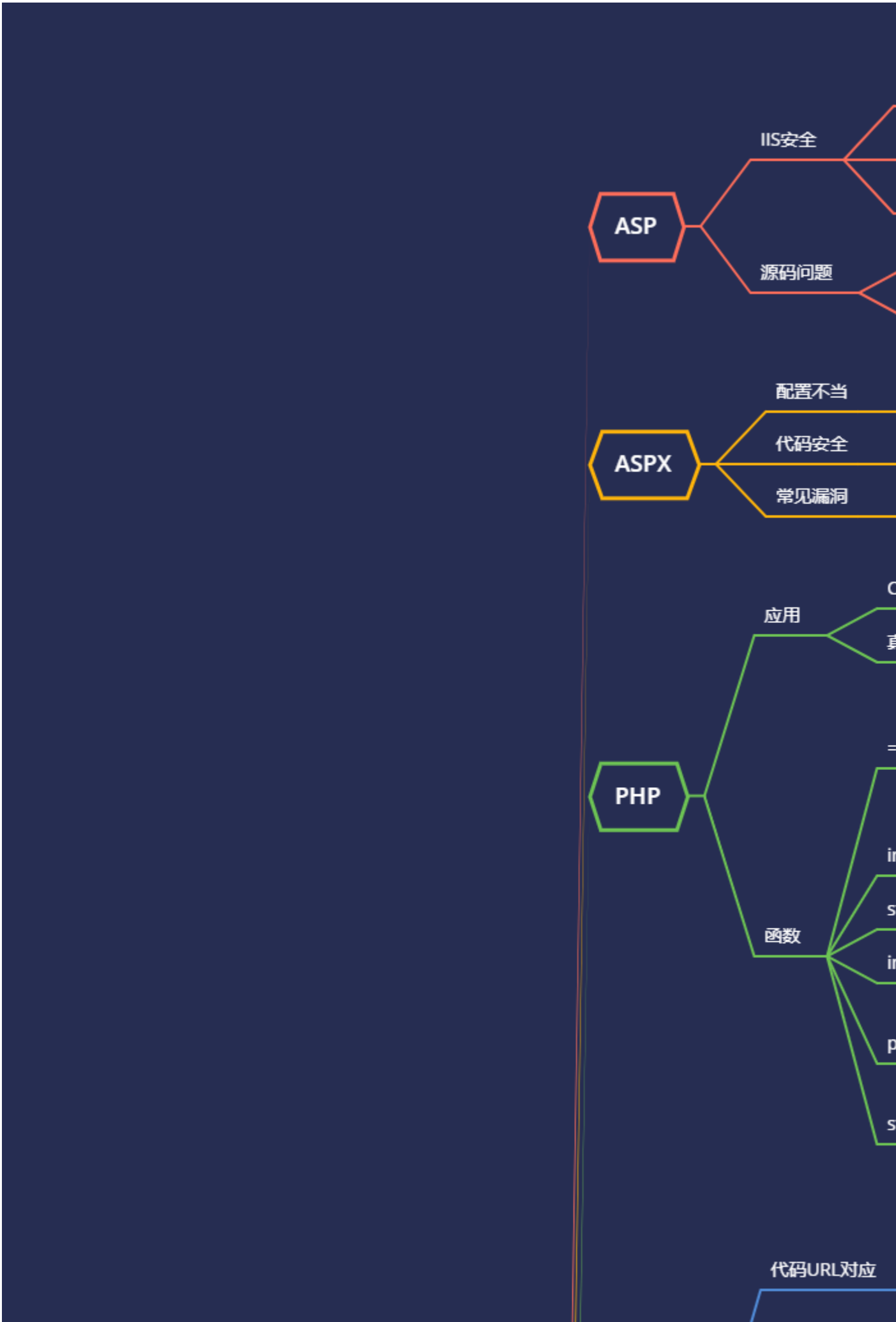
WEB 攻防-通用漏洞&验证码识别&复用&调用&找回密码重定向&状态值


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、找回密码逻辑机制-回显&验证码&指向

2、验证码验证安全机制-爆破&复用&识别

3、找回密码-客户端回显&Response 状态值&修改重定向

4、验证码技术-验证码爆破，验证码复用，验证码识别等

#详细点：

-找回密码流程安全：

1、用回显状态判断-res 前端判断不安全

2、用用户名重定向-修改标示绕过验证

3、验证码回显显示-验证码泄漏验证虚设

4、验证码简单机制-验证码过于简单爆破

-验证码绕过安全：

1、验证码简单机制-验证码过于简单爆破

2、验证码重复使用-验证码验证机制绕过

3、验证码智能识别-验证码图形码被识别

4、验证码接口调用-验证码触发机制枚举

#安全修复方案：

-找回机制要进行每一步验证-防绕过重定向

-找回机制要进行服务端验证-防 res 数据修改

-找回机制要控制验证码安全-防验证码攻击

-验证码接口需验证后被调用-防接口被乱调用

-验证码引用智能化人工判断-防验证码被识别

-验证码采用时间段生效失效-防验证码被复用

演示案例：

- phpun-res 值修改&验证码回显&爆破
- 某 APP-res 值修改&验证码接口调用&复用
- seacms-验证码识别&找回机制对应值修改

#phpun-res 值修改&验证码回显&爆破

res 修改-绑定手机号时修改返回状态值判定通过

验证码回显-绑定手机号时验证码前端泄漏被获取

验证码爆破-知道验证码规矩进行无次数限制爆破

#某 APP-res 值修改&验证码接口调用&复用

res 修改-找回密码修改返回状态值判定验证通过

验证码接口调用-抓当前发送验证码数据包后调用

验证码复用-抓第一次验证通过的验证码进行复用

#seacms-验证码识别&找回机制对应值修改

-找回机制对应值修改：

注册两个帐号，尝试找回密码，重置连接重定向绕过

代码审计后分析 Poc：

member.php?mod=repsw3&repswcode=y&repswname=targetUser

-验证码识别：xp_CAPTCHA

https://github.com/c0ny1/captcha-killer

https://github.com/smxiazi/NEW_xp_CAPTCHA

使用环境：windows 10 python3.6.5

安装使用：具体看直播操作

1、burp 安装 jypython 后导入 py 文件

2、安装所需库后 python 运行 server.py

3、抓操作数据包后设置参数设置引用

参考案例：https://www.cnblogs.com/punished/p/14746970.html

应用：爆破密码时，接口调用时，测试其他时等