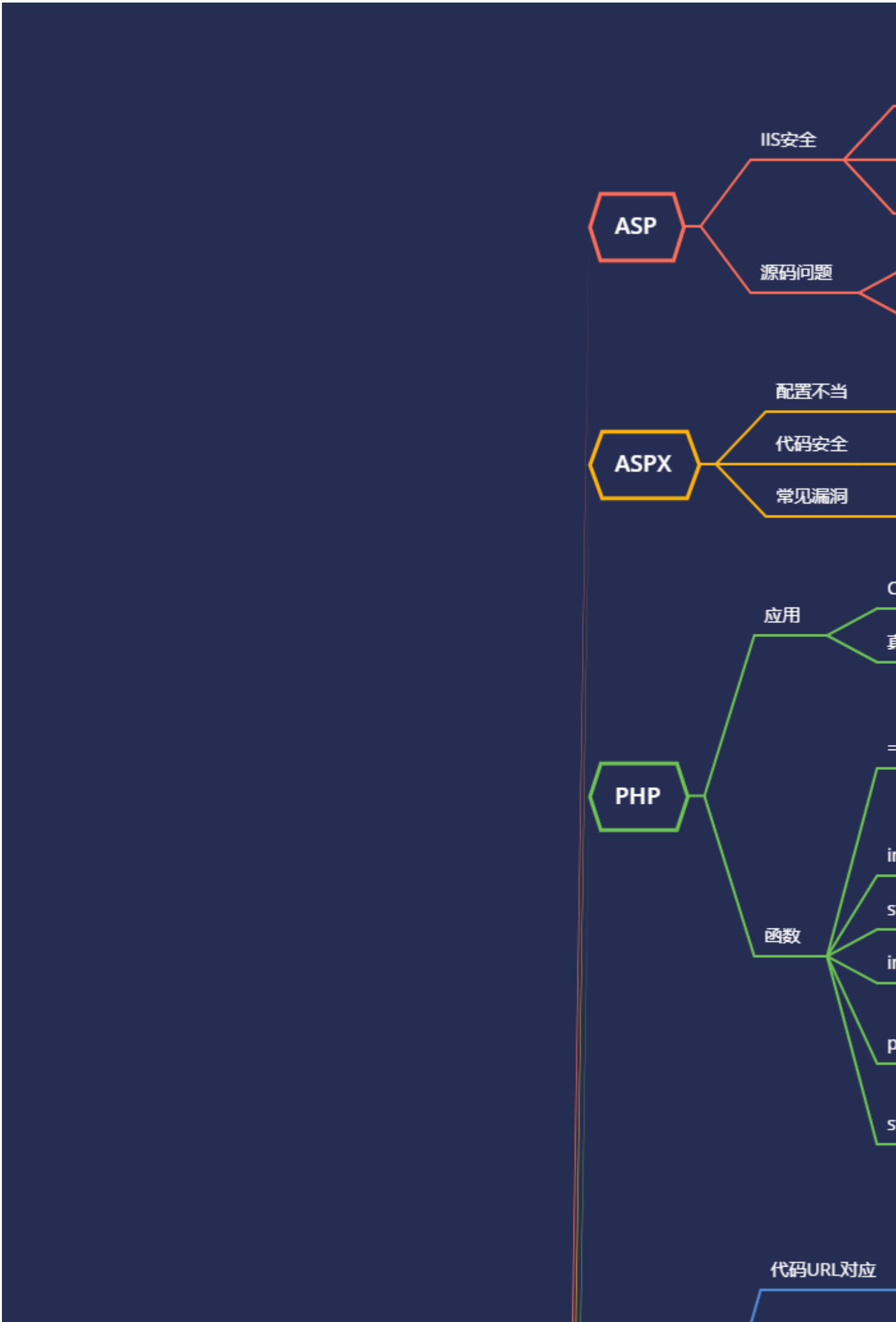
WEB 攻防-通用漏洞&弱口令安全&社工字典生成&服务协议&Web 应用


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、弱口令安全&配置&初始化等

2、弱口令对象&Web&服务&应用等

3、弱口令字典&查询&列表&列表等

#前置知识：

弱口令(weak password) 没有严格和准确的定义，通常认为容易被别人（他们有可能对你很了解）猜测到或被破解工具破解的口令均为弱口令，通常与管理的安全意识和平台的初始化配置等相关，通过系统弱口令，可被黑客直接获得系统控制权限。

在常见的安全测试中，弱口令会产生安全的各个领域，包括 Web 应用，安全设备，平台组件，操作系统等；如何获取弱口令，利用弱口令成为了此类安全问题的关键！

演示案例：

- Web 类-加密&验证码后台猜解
- 服务类-SSH&RDP 远程终端猜解
- 应用类-ZIP&Word 文件压缩包猜解
- 字典类-密文收集&弱口令&自定义生成

#Web 类-加密&验证码后台猜解

https://github.com/smxiazi/NEW_xp_CAPTCHA

-Zblog-密文 MD5 传输加密猜解

-Seacms-登录验证码识别猜解

#服务类-SSH&RDP 远程终端猜解

https://github.com/vanhauser-thc/thc-hydra

hydra 是一个自动化的爆破工具，暴力破解弱密码，

是一个支持众多协议的爆破工具，已经集成到 KaliLinux 中，直接在终端打开即可

-s PORT 可通过这个参数指定非默认端口。

-l LOGIN 指定破解的用户，对特定用户破解。

-L FILE 指定用户名字典。

-p PASS 小写，指定密码破解，少用，一般是采用密码字典。

-P FILE 大写，指定密码字典。

-e ns 可选选项，n：空密码试探，s：使用指定用户和密码试探。

-C FILE 使用冒号分割格式，例如"登录名:密码"来代替-L/-P 参数。

-M FILE 指定目标列表文件一行一条。

-o FILE 指定结果输出文件。

-f 在使用-M 参数以后，找到第一对登录名或者密码的时候中止破解。

-t TASKS 同时运行的线程数，默认为 16。

-w TIME 设置最大超时的时间，单位秒，默认是 30s。

-v / -V 显示详细过程。

server 目标 ip

service 指定服务名，支持的服务和协议：telnet ftp pop3[-ntlm] imap[-ntlm] smb smbnt http-{head|get} http-{get|post}-form http-proxy cisco cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5 rexec rlogin pcnfs snmp rsh cvs svn icq sapr3 ssh smtp-auth[-ntlm] pcanywhere teamspeak sip vmauthd firebird ncp afp 等等。

```
hydra -l root -P UserPassCombo-Jay.txt -t 5 -vV 47.110.73.12 ssh -f
hydra -l administrator -P UserPassCombo-Jay.txt -t 5 -vV 47.99.218.105 rdp -f
```

#应用类-ZIP&WORD 文件压缩包猜解

PassFab for Word

Advanced Archive Password Recovery

#字典类-密文收集+弱口令+自定义生成

涉及资源:

补充：涉及录像课件资源软件包资料等下载地址