基础入门-WEB 源码拓展

前言：WEB 源码在安全测试中是非常重要的信息来源，可以用来代码审计漏洞也可以用来做信息突破口，其中 WEB 源码有很多技术需要简明分析。比如：获取某 ASP 源码后可以采用默认数据库下载为突破，获取某其他脚本源码漏洞可以进行代码审计挖掘或分析其业务逻辑等，总之源码的获取将为后期的安全测试提供了更多的思路。

知识点：

- ✓ 关于 WEB 源码目录结构
- ✓ 关于 WEB 源码脚本类型
- ✓ 关于 WEB 源码应用分类
- ✓ 关于 WEB 源码其他说明

#数据库配置文件，后台目录，模版目录，数据库目录等

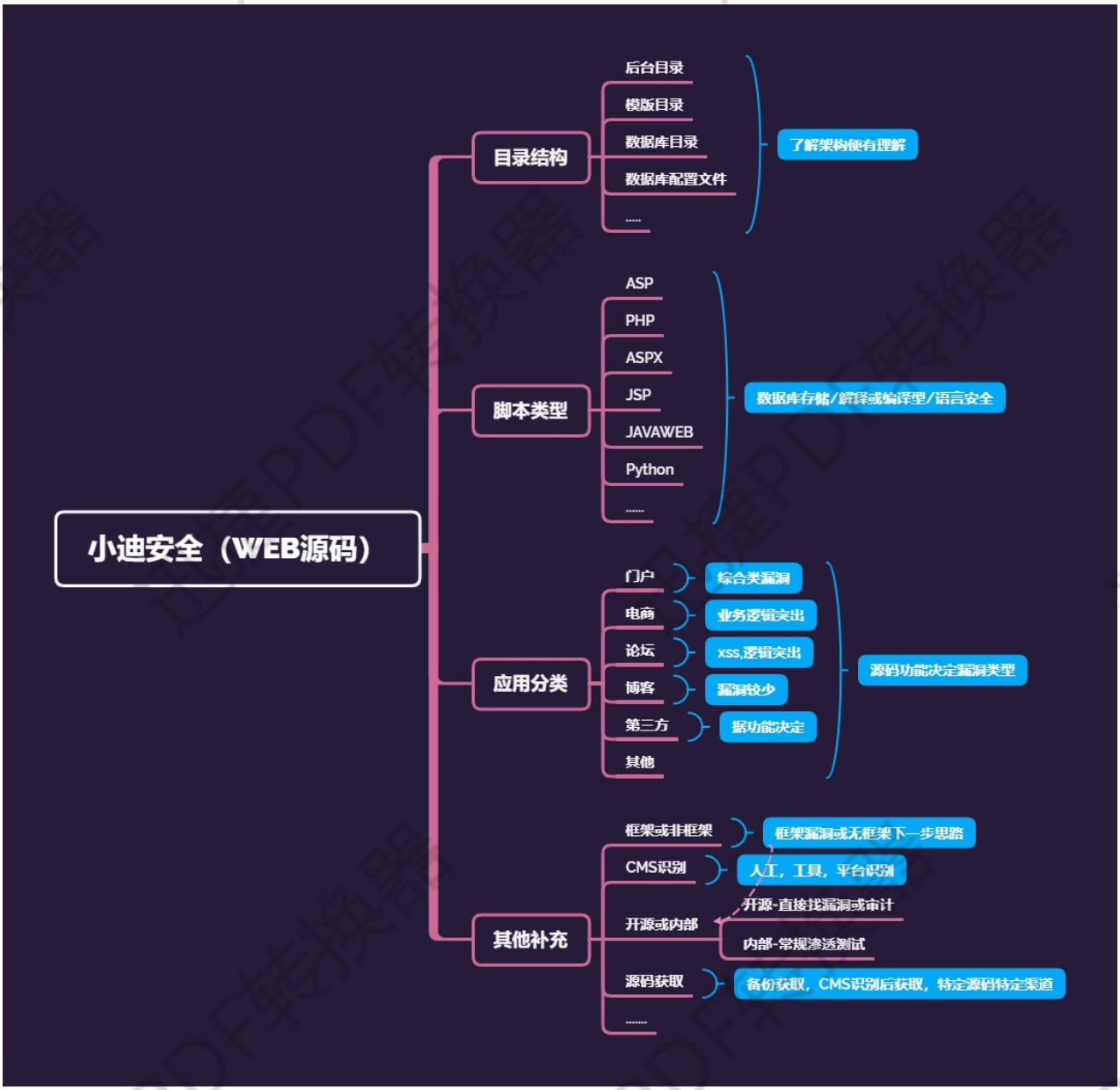
#ASP,PHP,ASPX,JSP,JAVAWEB 等脚本类型源码安全问题

#社交，论坛，门户，第三方，博客等不同的代码机制对应漏洞

#开源，未开源问题，框架非框架问题，关于 CMS 识别问题及后续等

#关于源码获取的相关途径：搜索，咸鱼淘宝，第三方源码站，各种行业对应

#总结：
关注应用分类及脚本类型估摸出可能存在的漏洞（其中框架类例外），在获取源码后可进行本地安全测试或代码审计，也可以分析其目录工作原理（数据库备份，bak 文件等），未获取到的源码采用各种方法想办法获取！



演示案例：

➢ ASP,PHP 等源码下安全测试

平台识别-某 CMS 无漏洞-默认数据库
平台识别-某 CMS 有漏洞-漏洞利用

➢ 源码应用分类下的针对漏洞

niushop 电商类关注漏洞点-业务逻辑

➢ 简要目标从识别到源码获取

本地演示个人博客-手工发现其 CMS-漏洞搜索或下载分析
http://weipan.1016sangshen.cn/ 内部搭建的靶场
人工爆框架-搜索特定 url-获取其他相符站点-漏洞测试
借助特定行业源码或咸鱼进行搜索获取-本地搭建-代码审计或其他

涉及资源：

https://cnmmm.com

https://www.yunsee.cn

https://w.ddosi.workers.dev

http://whatweb.bugscaner.com

https://github.com/Lucifer1993/cmsprint

https://github.com/M4tir/Github-Monitor

https://websec.readthedocs.io/zh/latest/language/index.html

另外还有 windows 靶机集合部分源码，在群文件靶机目录下载文本文件
