

Day04 基础入门-WEB源码扩展

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。

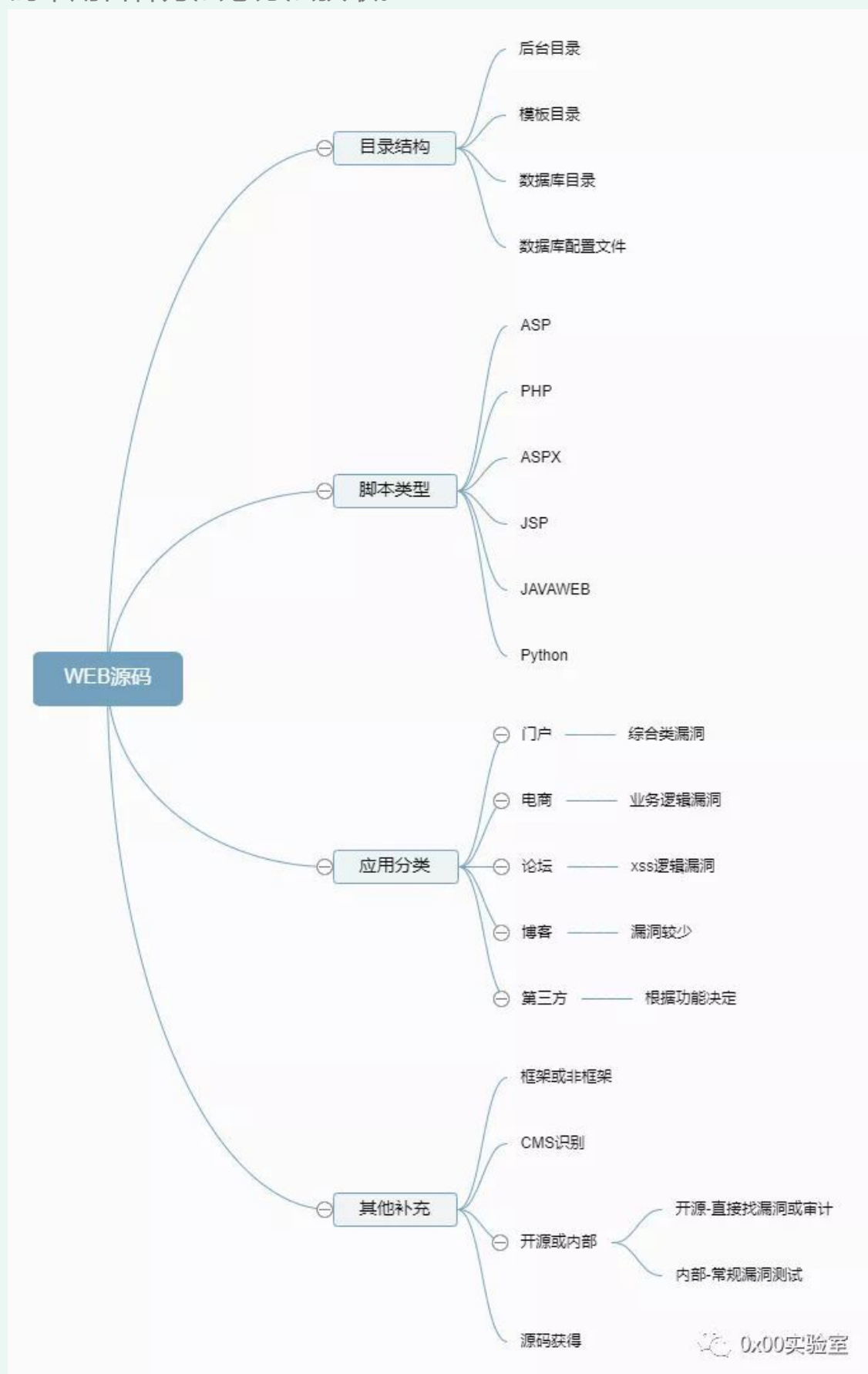
4.1 知识点

- 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
-

4.2 信息敏感点

- 敏感目录结构：数据库配置文件，后台目录，模版目录，数据库目录等
- web脚本类型：ASP,PHP,ASPX,JSP,JAVAWEB 等脚本类型源码
- 应用分类：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

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。



style.css: 这个文件可以用来生成md5值来查寻cms框架。可以通过网页刷新时加载的文件来搜索cms。

资源



```
1  https://www.yunsee.cn  
2  https://w.ddosi.workers.dev  
3  http://whatweb.bugscaner.com  
4  https://github.com/Lucifer1993/cmsprint  
5  https://github.com/M4t1r/Github-Monitor  
6  https://websec.readthedocs.io/zh/latest/language/  
index.html
```