一、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

语言与框架（还包含内网渗透等web安全知识）：https://websec.readthedocs.io/zh/latest/language/index.html

(如果能得到源码，可以查看config.php，一般这个文件会有用户名和密码，找到后台管理登录界面后。。。。你懂得)

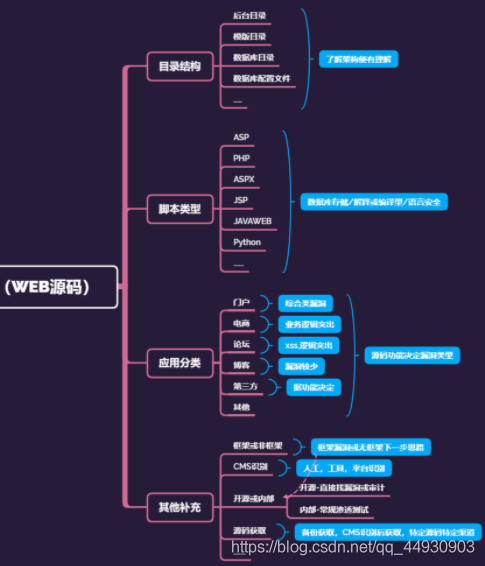
#社交，论坛，门户，第三方，博客等不同的代码机制对应漏洞

#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（CMS：内容管理系统，通过CMS识别，可以判断对方的网站搭建框架（有可能是用网上的源码稍加修改搭建起来的）；如果对方是用框架搭建的，则可以根据对应框架的漏洞进行分析；如果不是，则需要分析源码了）

#关于源码获取的相关途径：搜索，咸鱼淘宝，第三方源码站（菜鸟源码、tor，tg等），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！



二、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

windows下查看文件MD5值：

certutil -hashfile 文件名

1

➢ 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

商品支付漏洞利用：购买商品，通过bp抓包（点击“立即购买”时抓）、改包（商品数量改为<=0），再Forward让网页页面跳转到支付界面，即可实现0元支付。

➢ 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（输入index/login/login/token搜索有漏洞的网站，还可以搜网站文件名如arc.listview.class.php）–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

  还可以把url放到ThinkPHP进行漏洞检测、命令执行、getshell；可以尝试去搜索引擎搜一下index/login/login/token，找到对应网站再放到thnkphp中检测

三、涉及资源：

如果访问不进去直接搜菜鸟源码（十二堂等，建议挂科学冲浪）https://pt.cnmmm.com

云悉指纹识别：

https://www.yunsee.cn

CMS识别工具（如果失效就去小迪博客里找）：

https://w.ddosi.workers.dev/

http://whatweb.bugscaner.com

https://github.com/Lucifer1993/cmsprint

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

语言与框架（还包含内网渗透等web安全知识）：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