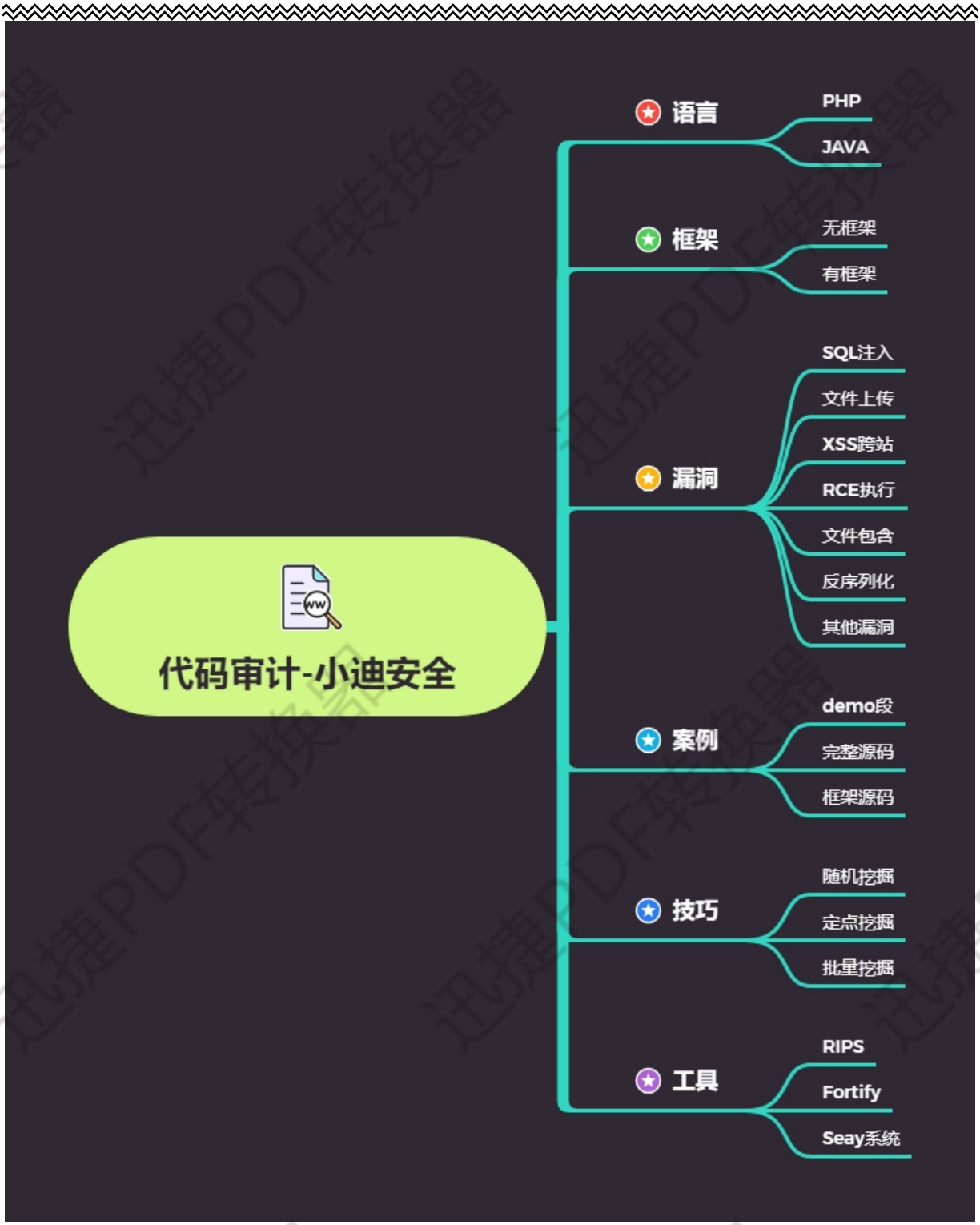
代码审计-PHP 无框架项目 SQL 注入挖掘技巧



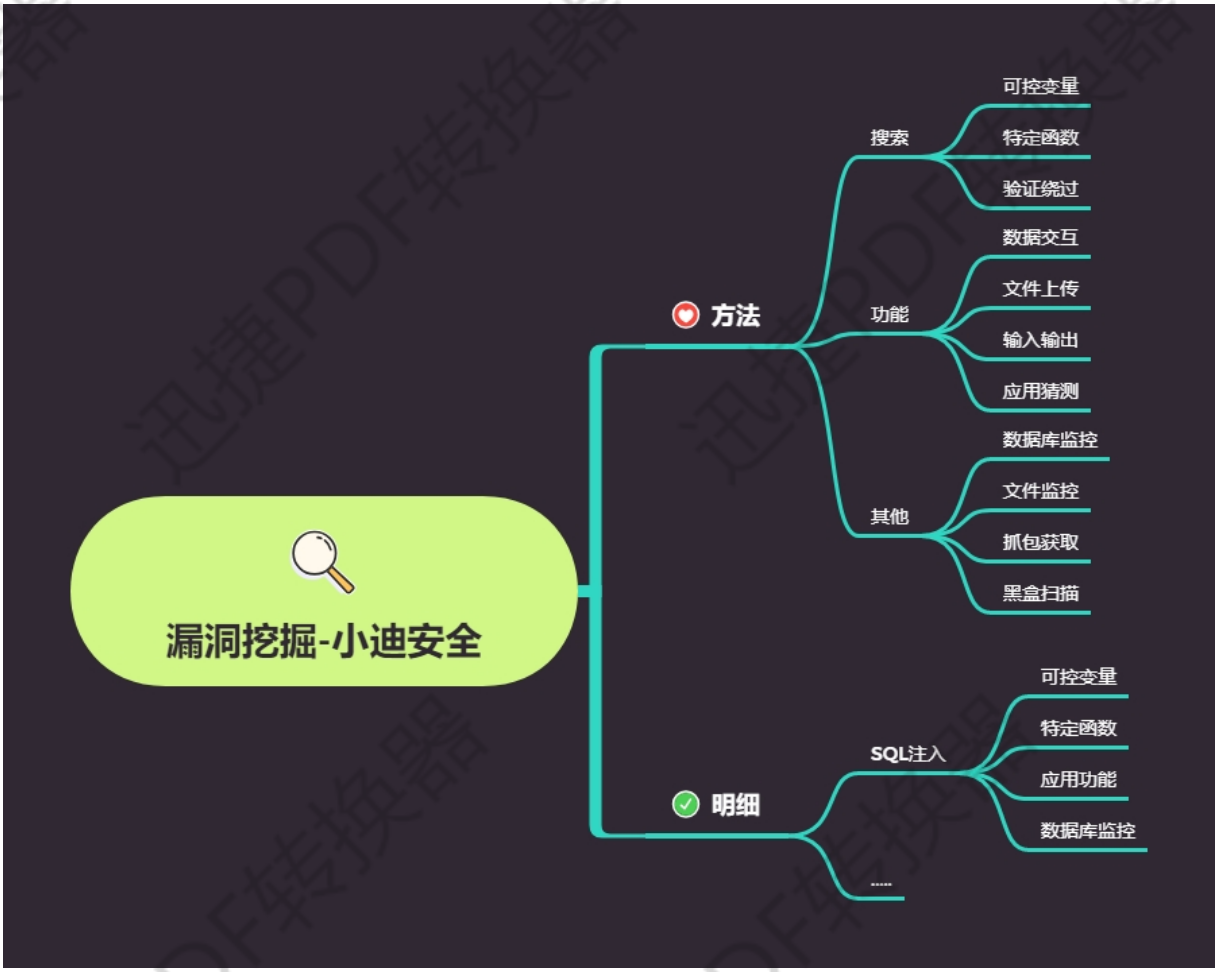
#代码审计教学计划：

审计项目漏洞 Demo->审计思路->完整源码框架->验证并利用漏洞

#代码审计教学内容：

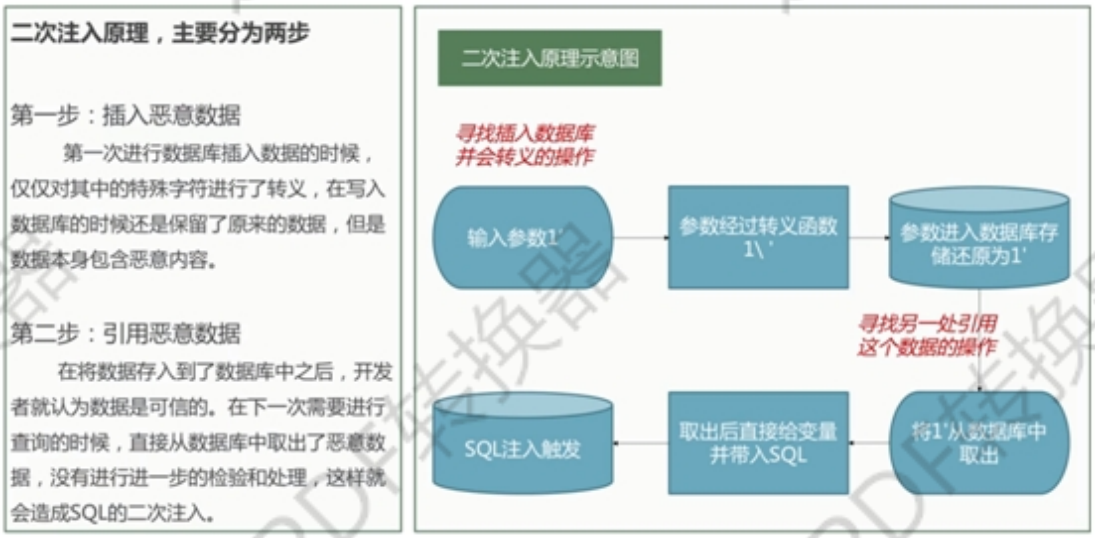
PHP,JAVA 网站应用，引入框架类开发源码，相关审计工具及插件使用

#代码审计必备知识点：
环境安装搭建使用，相关工具插件安装使用，掌握前期各种漏洞原理及利用
#代码审计开始前准备：
审计目标的程序名，版本，当前环境(系统,中间件,脚本语言等信息),各种插件等
#代码审计挖掘漏洞根本：
可控变量及特定函数，不存在过滤或过滤不严谨存在绕过导致的安全漏洞



演示案例：

- 简易 SQL 注入代码段分析挖掘思路
- QQ 业务图标点亮系统挖掘-数据库监控追踪
- 74CMS 人才招聘系统挖掘-2 次注入应用功能(自带转义)
- 苹果 CMS 影视建站系统挖掘-数据库监控追踪(自带过滤)



#技巧分析：
数据库监控脚本类，关键字搜索，业务应用分析等
https://www.cnblogs.com/ichunqiu/p/9548754.html

涉及资源：

https://pan.baidu.com/s/1QF2kqkUUZgPtwbmKBtg4bw 提取码：

xiao
