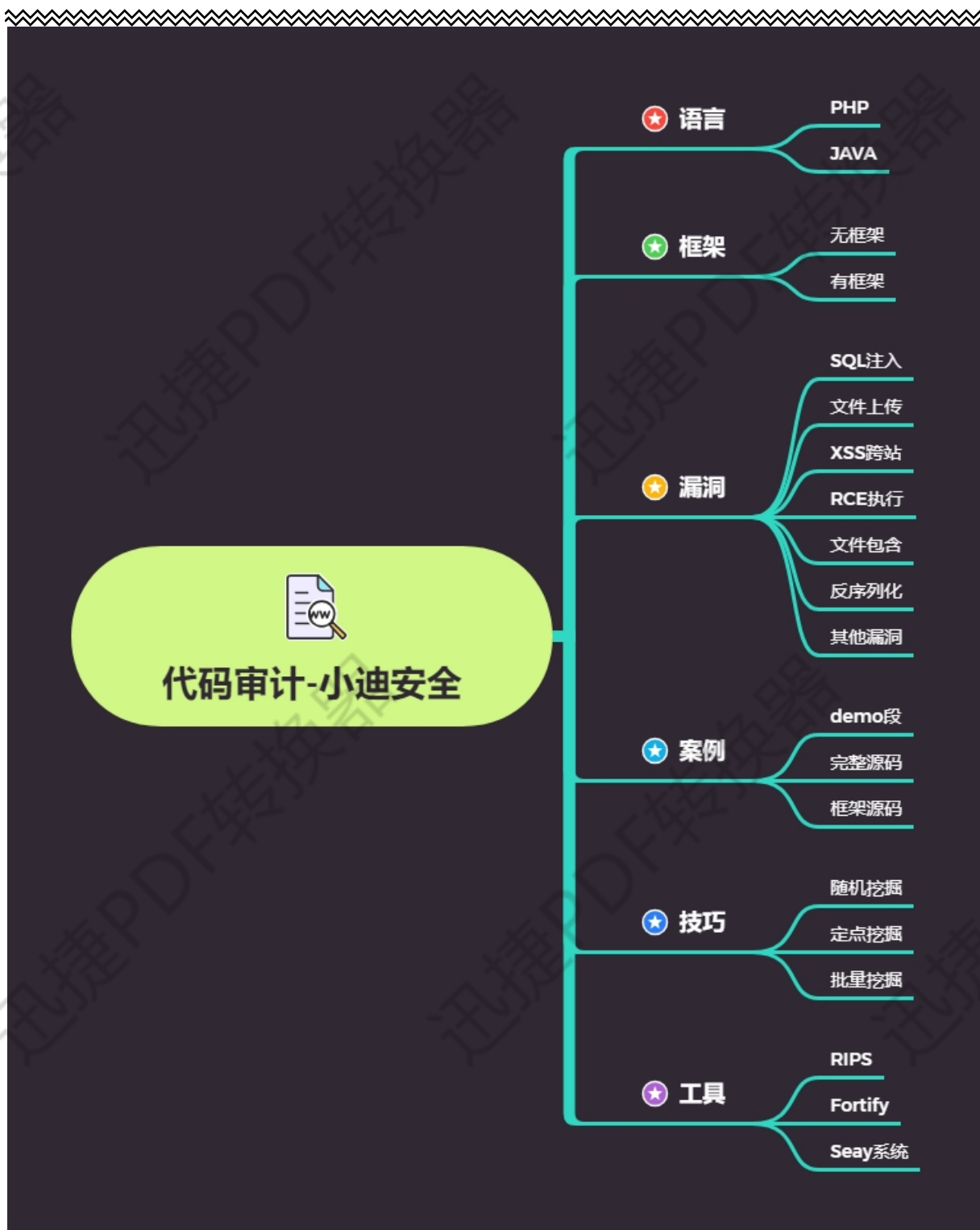


代码审计-PHP 无框架项目 SQL 注入挖掘技巧



#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)

二次注入原理，主要分为两步

第一步：插入恶意数据

第一次进行数据库插入数据的时候，仅仅对其中的特殊字符进行了转义，在写入数据库的时候还是保留了原来的数据，但是数据本身包含恶意内容。

第二步：引用恶意数据

在将数据存入到了数据库之后，开发者就认为数据是可信的。在下次需要进行查询的时候，直接从数据库中取出了恶意数据，没有进行进一步的检验和处理，这样就会造成SQL的二次注入。

二次注入原理示意图



#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