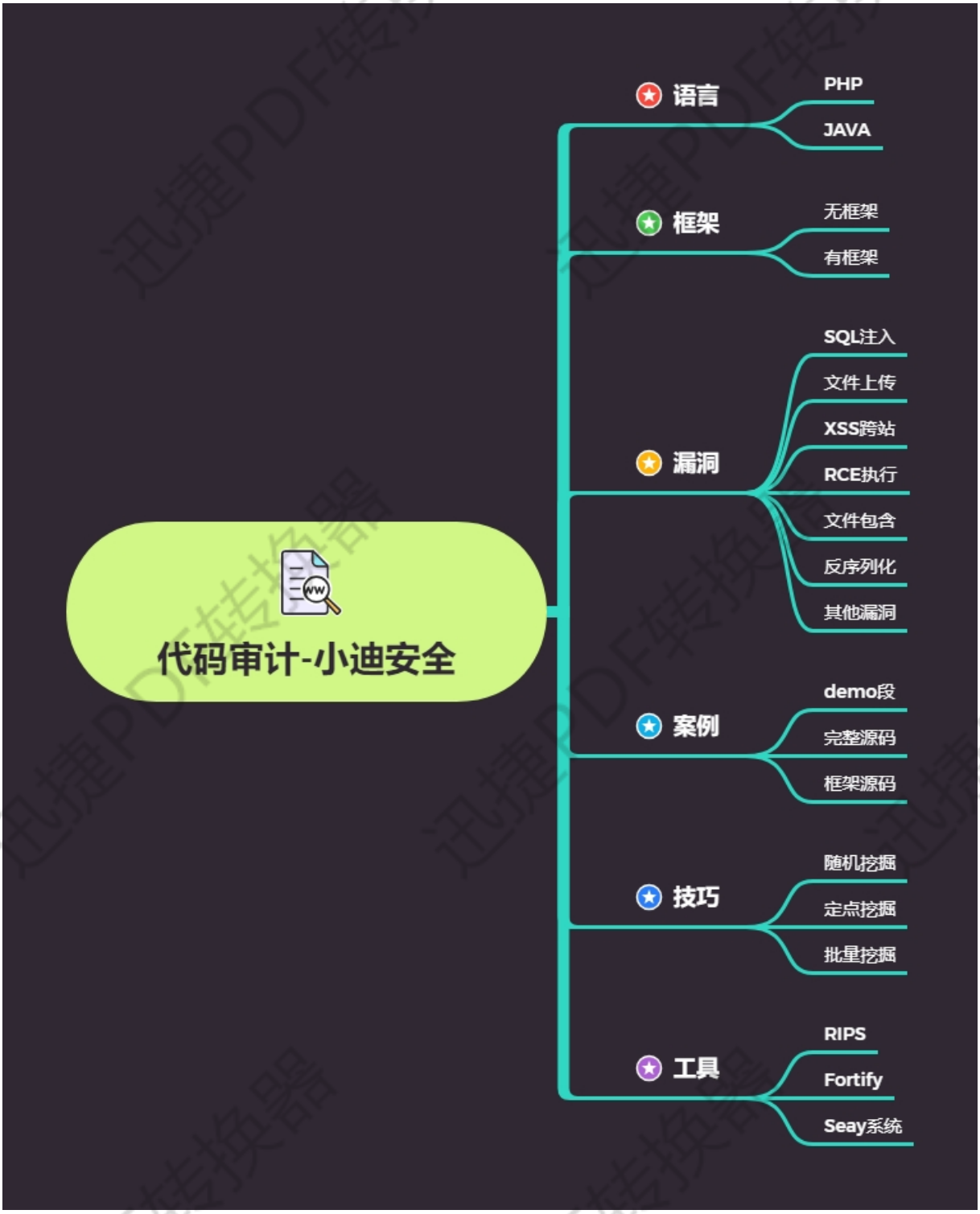
代码审计-TP5 框架及无框架变量覆盖反序列化



#漏洞关键字：
SQL 注入：
select insert update mysql_query mysqli 等
文件上传：
$_FILES，type="file"，上传，move_uploaded_file()等
XSS 跨站：
print print_r echo sprintf die var_dump var_export 等
文件包含：
include include_once require require_once 等
代码执行：
eval assert preg_replace call_user_func call_user_func_array 等
命令执行：
system exec shell_exec `` passthru pcntl_exec popen proc_open
变量覆盖：
extract() parse_str() importrequestvariables() $$等
反序列化：
serialize() unserialize() __construct __destruct 等
其他漏洞：
unlink() file_get_contents() show_source() file() fopen()等

#通用关键字：
$_GET,$_POST,$_REQUEST,$_FILES,$_SERVER 等

功能点或关键字分析可能存在漏洞
抓包或搜索关键字找到代码出处及对应文件
追踪过滤或接受的数据函数，寻找触发此函数或代码的地方进行触发测试

演示案例：

- Metinfo-无框架-变量覆盖-自动审计或搜索
- phpmydmin-无框架-反序列化-自动审计或搜索
- Thinkphp5-有框架-搭建使用入口访问调试 SQL 等

#变量覆盖配合文件包含实现任意文件包含
自动审计或搜索关键字找到文件及代码段，全局配置文件
搜索或访问触发全局配置文件配合手写代码测试变量覆盖
配合文件包含漏洞覆盖指定文件实现文件包含攻击获取权限
追踪$module 变量出处文件，然后分析如何覆盖它达到目的
Payload:/about/index.php?fmodule=7&module=1.txt

#反序列化

自动审计或搜索关键字找到文件及代码段
__wakeup() //使用 unserialize 时触发
__sleep() //使用 serialize 时触发
__destruct() //对象被销毁时触发
__call() //在对象上下文中调用不可访问的方法时触发
__callStatic() //在静态上下文中调用不可访问的方法时触发
__get() //用于从不可访问的属性读取数据
__set() //用于将数据写入不可访问的属性
__isset() //在不可访问的属性上调用 isset()或 empty()触发
__unset() //在不可访问的属性上使用 unset()时触发
__toString() //把类当作字符串使用时触发
__invoke() //当脚本尝试将对象调用为函数时触发
找到__wakeup()代码段，代码段调用函数中存在 eval 等函数操作，可调式 load
构造 getSource()利用 Payload,实现 file_get_contents 函数配合 eval 执行
Payload：action=test&configuration=O:10:"PMA_Config":1:{s:6:"source",s:11:"d:/test.txt";}

#Thinkphp5 简要知识点
入口文件，调试模式，访问路由，访问对应，内置安全等
测试访问不同方法名，不同文件不同方法名
测试常规写法 SQL 注入，TP5 规定写法 SQL 注入

涉及资源：

https://www.kancloud.cn/thinkphp/thinkphp5_quickstart

https://pan.baidu.com/s/1miETaZcez30jmUEA5n2EWw 提：xiao
