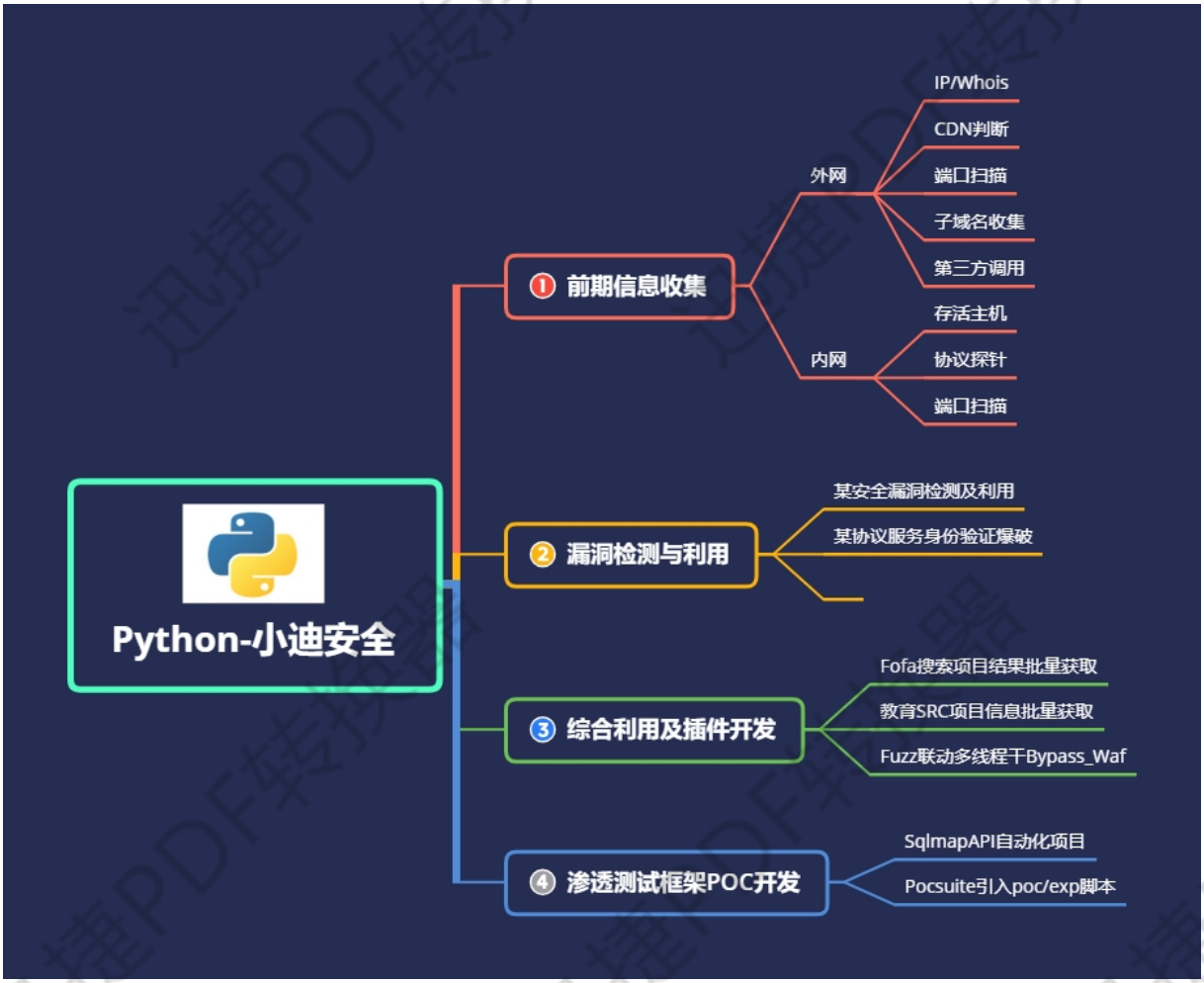
Python 开发-sqlmapapi&Tamper&Pocsuite



#本课知识点：
Request 爬虫技术，Sqlmap 深入分析，Pocsuite 分析，框架代码二次修改等

#本课目的：
掌握安全工具的 API 接口开发利用，掌握优秀框架的二次开发插件引用等

演示案例：

- Sqlmap_Tamper 模块脚本编写绕过滤

- SqlmapAPI 调用实现自动化 SQL 注入安全检测
- Pocsuite3 漏扫框架二次开发 POC/EXP 引入使用

#案例 1-Sqlmap_Tamper 模块脚本编写绕过滤

#案例 2-SqlmapAPI 调用实现自动化 SQL 注入安全检测
参考：https://www.freebuf.com/articles/web/204875.html
应用案例：前期通过信息收集拿到大量的 URL 地址，这个时候可以配合 SqlmapAPI 接口进行批量的 SQL 注入检测（SRC 挖掘）
开发当前项目过程：（利用 sqlmapapi 接口实现批量 URL 注入安全检测）
1.创建新任务记录任务 ID　　@get("/task/new")
2.设置任务 ID 扫描信息　　@post("/option/<taskid>/set　　")
3.开始扫描对应 ID 任务　　@post("/scan/<taskid>/start")
4.读取扫描状态判断结果　　@get("/scan/<taskid>/status")
5.如果结束删除 ID 并获取结果　　@get("/task/<taskid>/delete")
6.扫描结果查看@get("/scan/<taskid>/data")

#案例 3-Pocsuite3 漏扫框架二次开发 POC/EXP 引入使用
参考：https://www.freebuf.com/articles/people/162868.html
开发当前项目过程：（利用已知框架增加引入最新或内部的 EXP 进行安全检测）
1.熟悉 Pocsuite3 项目使用及介绍
2.熟悉使用命令及代码文件对应情况
3.选取 Glassfish 漏洞进行编写测试
4.参考自带漏洞模版代码模仿写法测试
python cli.py -u x.x.x.x -r Glassfish.py --verify

涉及资源：

http://sqlmap.org/

https://github.com/knownsec/pocsuite/

https://www.freebuf.com/articles/web/204875.html

https://www.freebuf.com/articles/people/162868.html

https://pan.baidu.com/s/13y3U6jX3WUYmnfKnXT8abQ 提取码：xiao