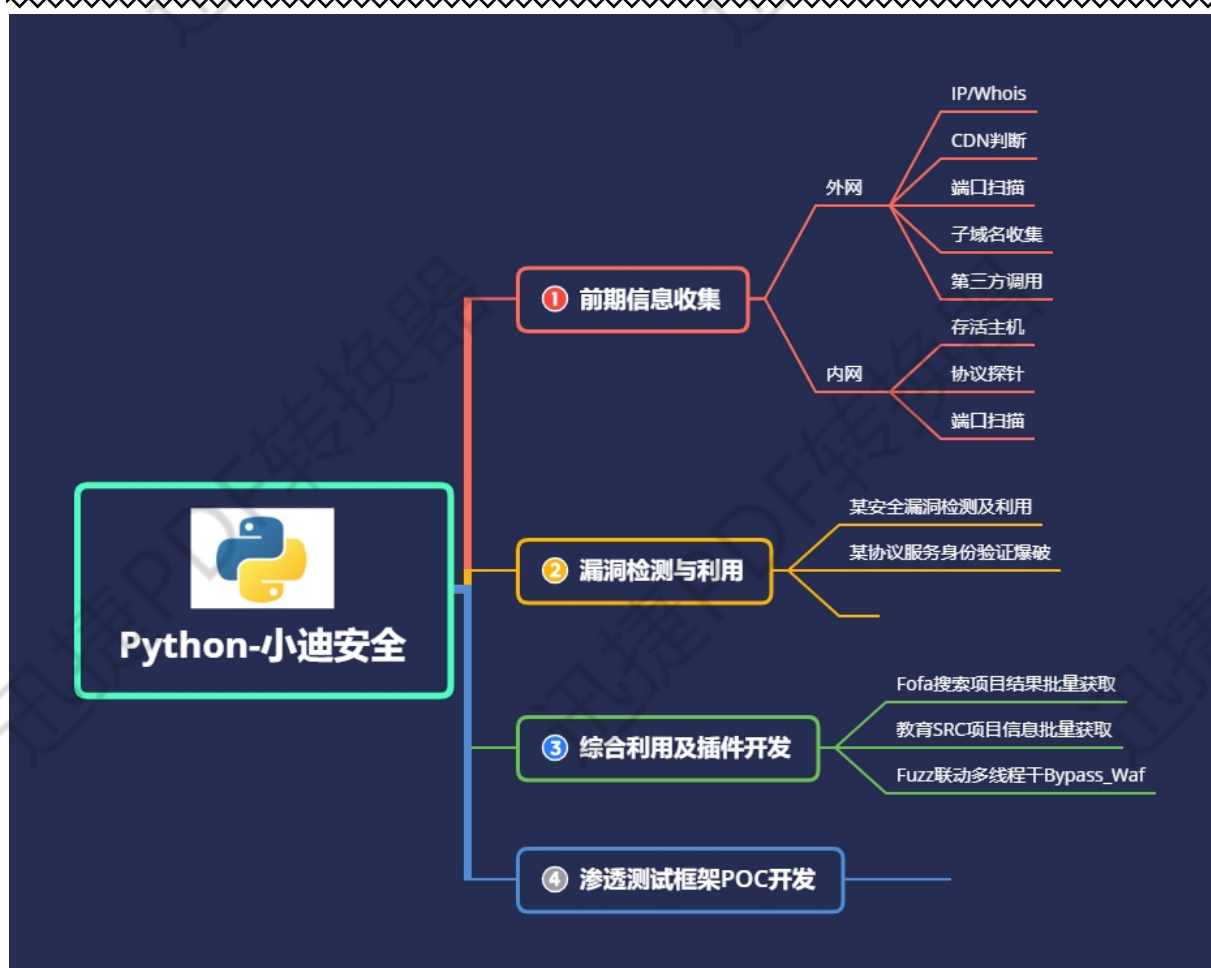


# Python 开发-多线程 Fuzz&Waf 异或免杀&爆破

# Python 开发-多线程 Fuzz&Waf 异或免杀&爆破



#本课知识点:

协议模块使用, Request 爬虫技术, 简易多线程技术, 编码技术, Bypass 后门技术

#学习目的:

掌握利用强大的模块实现各种协议连接操作(爆破或利用等)，配合 Fuzz 吊打 WAF 等

---

### 演示案例：

- Python 开发-简单多线程技术实现脚本
- Python 开发-利用 FTP 模块实现协议爆破脚本
- Python 开发-配合 Fuzz 实现免杀异或 Shell 脚本

#案例 1-Python 开发-简单多线程技术实现脚本  
queue, threading 模块使用

#案例 2-Python 开发-利用 FTP 模块实现协议爆破脚本  
1.ftplib 模块使用  
2.遍历用户及密码字典  
3.尝试连接执行命令判断

#案例 3-Python 开发-配合 Fuzz 实现免杀异或 Shell 脚本  
1.免杀异或 Shell 原理讲解及开发思路（参考及举例：!^@,"^?等）  
2.基于 Fuzz 思路生成大量 Payload 代码并有序命名写入网站文件中  
3.基于多线程实现批量访问 Shell 文件并提交测试是否正常连接回显

---

### 涉及资源：

<https://github.com/zhanye/fuzzdb>

<https://github.com/stemmm/fuzzDicts>

<https://www.cnblogs.com/liujizhou/p/11806497.html>

<https://www.cnblogs.com/kaituorensheng/p/4480512.html>

[https://blog.csdn.net/qq\\_41617034/article/details/104441032](https://blog.csdn.net/qq_41617034/article/details/104441032)

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

[xiao](#)

