**信息收集？**

在企业src中，通常会给定一些目标和属于该公司的系统这样之类的，如何扩大攻击面？

子域名

1. 子域名的爆破(看字典)(二三级域名)(goby这种)(水泽自动化)
2. c段
3. github
4. 爬虫js文件中获取到其他根域名或者子域名
5. 小程序和app中发现更多的根域名和子域名

**看到这这么麻烦就怕了？没事，我发现成集成工具(oneforall+fscan+爱企查爬虫调用)**

**Js文件蕴含大秘密 crawlego**

app.xxxx.js这种js文件

有些站点可能调用的是其他站点的js文件,例如：password.xxxx.com调用password-test.xxx.com/js/xxxx.js这种

浏览器Findsomething插件



**Webpack的配置不当导致的api路径泄露**

**其他隐藏根域名或者多级域名泄露**

**Bp导出js 用jsfinder**



**微信公众号，小程序，app**

**<https://www.xiaolanben.com/> 小蓝本一键搞定**



**小程序和app主要按照web那样测试即可，或者寻找下敏感信息的泄露，反编译一下等等**