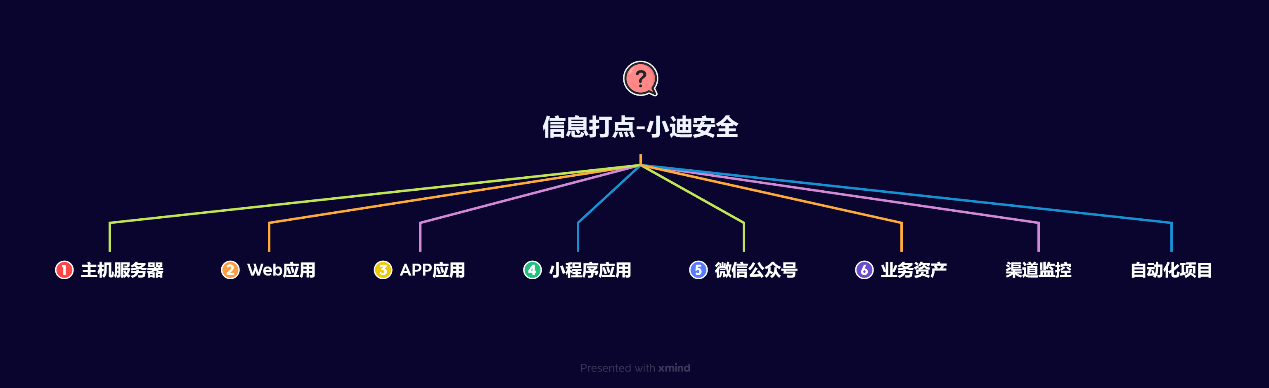
信息收集-公众号资产&供应链回溯&Github泄漏&多渠道泄漏&资产监控&引擎语法



#知识点：  
1、信息收集-服务器系统-操作系统&IP资产  
2、信息收集-服务器系统-端口扫描&服务定性  
---------------------------------------------------  
1、信息收集-Web应用-机构产权&域名相关性  
2、信息收集-Web应用-DNS&证书&枚举子域名  
---------------------------------------------------  
1、信息收集-Web应用-架构分析&指纹识别  
2、信息收集-Web应用-架构分析&WAF&蜜罐  
3、信息收集-Web应用-架构分析&框架组件识别  
---------------------------------------------------  
1、信息收集-Web应用-源码获取-已知指纹&未知指纹  
2、信息收集-Web应用-源码获取-泄漏问题&发现指纹  
---------------------------------------------------  
1、信息收集-Web应用-JS提取分析-人工&插件\*项目  
2、信息收集-Web应用-JS提取分析-URL&配置&逻辑  
---------------------------------------------------  
1、信息收集-Web应用-CDN加速-如何识别  
2、信息收集-Web应用-CDN加速-绕过方法  
---------------------------------------------------  
1、信息收集-Web应用-开发框架-识别安全  
2、信息收集-Web应用-安全组件-特征分析  
---------------------------------------------------  
1、信息收集-APP应用-公开信息-知识产权&开发者定位  
2、信息收集-APP应用-资产信息-抓包&静态提取&动态调试  
---------------------------------------------------  
1、信息收集-小程序应用-公开信息-知识产权&平台搜索  
2、信息收集-小程序应用-资产信息-抓包&提取&动态调试  
---------------------------------------------------  
1、信息收集-项目推荐-自动化环境部署  
2、信息收集-项目推荐-自动化资产收集管理  
---------------------------------------------------  
1、信息收集-泄漏安全-信息监控&搜索语法  
2、信息收集-供应链安全-收集&ICO&目标溯  
3、信息收集-公众号资产-官方服务&第三方引用  
  
#章节点：(待补充)  
#具体点：(待补充)

演示案例：

* 公众号-渠道资产-第三方引入
* 供应链-目标旁路-获取和拓展
* 信息泄漏-源码文档-敏感配置监控

#公众号-渠道资产-第三方引入  
目标公众号服务获取   
官方服务&第三方资产  
  
#信息泄漏-源码文档-敏感配置监控  
1、Github监控  
GITHUB资源搜索：  
in:name test #仓库标题搜索含有关键字   
in:descripton test #仓库描述搜索含有关键字   
in:readme test #Readme文件搜素含有关键字   
stars:>3000 test #stars数量大于3000的搜索关键字   
stars:1000..3000 test #stars数量大于1000小于3000的搜索关键字 forks:>1000 test #forks数量大于1000的搜索关键字   
forks:1000..3000 test #forks数量大于1000小于3000的搜索关键字 size:>=5000 test #指定仓库大于5000k(5M)的搜索关键字 pushed:>2019-02-12 test #发布时间大于2019-02-12的搜索关键字 created:>2019-02-12 test #创建时间大于2019-02-12的搜索关键字 user:test #用户名搜素   
license:apache-2.0 test #明确仓库的 LICENSE 搜索关键字 language:java test #在java语言的代码中搜索关键字   
user:test in:name test #组合搜索,用户名test的标题含有test的  
关键字配合谷歌搜索：  
site:Github.com smtp   
site:Github.com smtp @qq.com   
site:Github.com smtp @126.com   
site:Github.com smtp @163.com   
site:Github.com smtp @sina.com.cn   
site:Github.com smtp password   
site:Github.com String password smtp  
  
系统源码：特征，文件等  
敏感信息：密码，文档，人员等  
监控项目：  
https://github.yhuisec.com/  
https://github.com/madneal/gshark  
https://github.com/NHPT/FireEyeGoldCrystal  
https://github.com/Explorer1092/Github-Monitor  
  
2、其他渠道（搜索引擎）  
个人信息 网盘泄漏 文档泄漏  
inurl:xxx.com filetype:xls  
inurl:xxx.com password admin  
site:xxx.com filetype:xls|doc|pdf  
  
#供应链-目标旁路-获取和拓展  
这是一种典型的迂回攻击方式。攻击者将目光聚集在目标企业的上下游供应商，比如IT供应商、安全供应商等，从这些上下游企业中找到软件或系统、管理上的漏洞，进而攻进目标企业内部。  
-商业购买系统  
-软件开发商  
-外包业务  
-代理商  
-招投标文件  
  
供应链例子edusrc挖洞思路：  
1、找供应链公司，通过演示站点或提供的ico或特征文件找到大量高校使用系统的目标，一旦测出这个应用产品系统的漏洞，形成了通杀  
2、找高校目标，通过高校系统的信息或者ico等找到供应链，再从供应链继续找使用同样的系统的高校目标，一旦测出这个应用产品系统的漏洞，形成了通杀  
  
核心：如何找到系统的漏洞  
1、尽量找到源码（源码获取途径）  
2、旁入方法（找相似目标的存在脆弱点为突破）  
  
目标供应链获取：可以企业产权或应用提示等  
供应链信息收集：ico拓展 演示站点 成功案例等  
案例文章：  
https://mp.weixin.qq.com/s/YSD6yGGlBchY61hAZdKLoA  
https://mp.weixin.qq.com/s/a8wyCeY7j29j6ITXfisOtQ  
https://mp.weixin.qq.com/s/LQ5yeVJK4yCysxArwxSYbg

涉及资源：[资源下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)