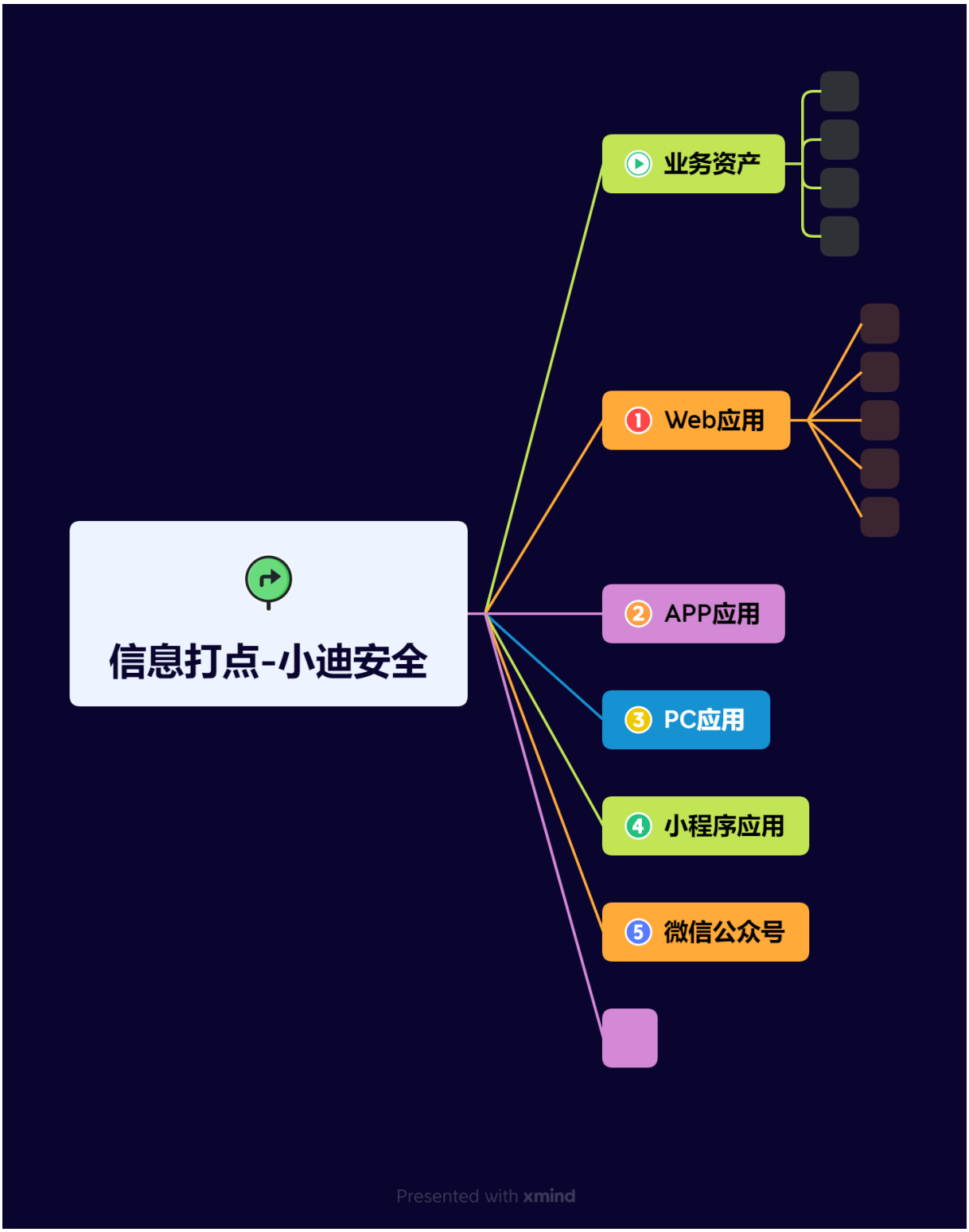
信息打点-Web 应用&企业产权&指纹识别&域名资产&网络空间&威胁情报



#知识点：

1、业务资产-应用类型分类

2、Web 单域名获取-接口查询

3、Web 子域名获取-解析枚举

4、Web 架构资产-平台指纹识别

#章节点

Web：语言/CMS/中间件/数据库/系统/WAF 等

系统：操作系统/端口服务/网络环境/防火墙等

应用：APP 对象/API 接口/微信小程序/PC 应用等

架构：CDN/前后端/云应用/站库分离/OSS 资源等

技术：JS 爬虫/敏感扫描/目录爬虫/源码获取/接口泄漏等

技术：指纹识别/端口扫描/CDN 绕过/WAF 识别/Github 监控等

演示案例：

- 应用-信息打点-某某企业
- Web-信息打点-教育 SRC
- Web-信息打点-补天 SRC

标签	名称	地址
企业信息	天眼查	https://www.tianyancha.com/
企业信息	小蓝本	https://www.xiaolanben.com/
企业信息	爱企查	https://aiqicha.baidu.com/
企业信息	企查查	https://www.qcc.com/
企业信息	国外企查	https://opencorporates.com/
企业信息	启信宝	https://www.qixin.com/
备案信息	备案信息查询	http://www.beianx.cn/

一般使用小蓝本和爱企查，其中小蓝本免费，爱企查收费，可在拼DD购买低价会员

备案信息	备案管理系统	https://beian.miit.gov.cn/
公众号信息	搜狗微信搜索	https://weixin.sogou.com/
注册域名	域名注册查询	https://buy.cloud.tencent.com/domain
IP 反查	IP 反查域名	https://x.threatbook.cn/
IP 反查	IP 反查域名	http://dns.bugscaner.com/

标签	名称	地址
DNS 数据	dnsdumpster	https://dnsdumpster.com/
证书查询	CertificateSearch	https://crt.sh/
网络空间	FOFA	https://fofa.info/
网络空间	全球鹰	http://hunter.qianxin.com/
网络空间	360	https://quake.360.cn/quake/
威胁情报	微步在线 情报社区	https://x.threatbook.cn/
威胁情报	奇安信 威胁情报中心	https://ti.qianxin.com/
威胁情报	360 威胁情报中心	https://ti.360.cn/#/homepage
枚举解析	在线子域名查询	http://tools.bugscaner.com/subdomain/
枚举解析	DNSGrep 子域名查询	https://www.dnsgrep.cn/subdomain
枚举解析	工具强大的子域名收集器	https://github.com/shmilylty/OneForAll

标签	名称	地址

指纹识别	在线 cms 指纹识别	http://whatweb.bugscaner.com/look/
指纹识别	Wappalyzer	https://github.com/AliasIO/wappalyzer
指纹识别	TideFinger 潮汐	http://finger.tidesec.net/ 潮汐和云悉用的最多，还有Wappalyzer插件
指纹识别	云悉指纹	https://www.yunsee.cn/
指纹识别	WhatWeb	https://github.com/urbanadventurer/WhatWeb
指纹识别	数字观星 Finger-P	https://fp.shuziguanxing.com/#/

标签	名称	地址
网络空间	钟馗之眼	https://www.zoomeye.org/
网络空间	零零信安	https://0.zone/
网络空间	Shodan	https://www.shodan.io/
网络空间	Censys	https://censys.io/
网络空间	ONYPHE	https://www.onyphe.io/
网络空间	FullHunt	https://fullhunt.io/
网络空间	Soall Search Engine	https://soall.org/
网络空间	Netlas	https://app.netlas.io/responses/
网络空间	Leakix	https://leakix.net/
网络空间	DorkSearch	https://dorksearch.com/
威胁情报	VirusTotal 在线查杀平台	https://www.virustotal.com/gui/
威胁情报	VenusEye 威胁情报中心	https://www.venuseye.com.cn/

威胁情报	绿盟科技 威胁情报云	https://ti.nsfocus.com/
威胁情报	IBM 情报中心	https://exchange.xforce.ibmcloud.com/
威胁情报	天际友盟安全智能平台	https://redqueen.tj-un.com
威胁情报	华为安全中心平台	https://isecurity.huawei.com/sec
威胁情报	安恒威胁情报中心	https://ti.dbappsecurity.com.cn/
威胁情报	AlienVault	https://otx.alienvault.com/
威胁情报	深信服	https://sec.sangfor.com.cn/
威胁情报	丁爸情报分析师的工具箱	http://dingba.top/
威胁情报	听风者情报源 start.me	https://start.me/p/X20Apn
威胁情报	GreyNoise Visualizer	https://viz.greynoise.io/
威胁情报	URLhaus 数据库	https://urlhaus.abuse.ch/browse/
威胁情报	Pithus	https://beta.pithus.org/

#业务资产：

1、WEB 应用

2、APP 应用

3、PC 端应用

4、小程序应用

5、微信公众号

6、其他产品等

#WEB 单域名：

1、备案信息

2、企业产权　就是上述的企业信息

3、注册域名　例如登陆腾讯云，在其注册域名一栏搜索qquan，显示出已被注册的域名可能也是资产

4、反查解析　打开命令窗口，ping qquan.site得到IP地址，再利用上述IP反查工具，可能查出其他资产

#WEB 子域名：

1、DNS 数据

2、证书查询

3、网络空间

4、威胁情报

5、枚举解析　暴力破解，比如ping qquan.xxx，看是否能够ping通

#Web 架构资产：

1、程序语言

2、框架源码

3、搭建平台　指纹识别

4、数据库类

5、操作系统

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址
