漏洞挖掘

- **目标确认**
  - 公告 — 收录范围
  - 友情链接 — 企业信息
  - 微信搜索 — 产品
  - ICP 备案 — 服务
  - icon 搜索 — 补充
  - 范围
    - 网站
    - 小程序
    - APP
    - 快应用
    - 公众号
- **信息收集**
  - FOFA
  - Hunter
  - OneForAll
  - 资产
    - ASN
    - 子域名
    - IP
    - 旁站
- **信息泄露**
  - ARL
  - dirsearch
  - Google
  - 网页源代码
  - Burp
    - HaE
    - FinderPrint
    - APIFinder
  - 数据包
  - 敏感信息
    - AccessKey
      - AccessKey ID
      - AccessKey Secret
    - API Key 泄露 — 地图 API
      - 谷歌地图
      - 高德地图
      - 百度地图
      - 腾讯地图
    - 身份证，学号，工号
    - 账户，密码
      - 手机号
      - 邮箱
      - VPN 配置信息
      - 数据库配置信息
      - 服务器配置信息
    - 内部资料
      - 项目说明
      - 开发设计
      - 合同
    - 源代码
      - Github
      - Sourcegraph
      - Gitee
      - CSDN
      - 开源中国
      - 博客园
      - 简书
      - ShowDoc
      - 关键词
        - 公司
          - 集团
            - 集团全称
            - 集团简称
          - 全称
          - 简称
          - 繁体
          - 英文
          - 拼音
            - 全拼
            - 简拼
        - 根域名
          - xxx.com
          - com.xxx — 关于 APP 、小程序的代码
        - APP — APP 名
        - 小程序 — 小程序名
        - 子域名的系统名称
        - 招投标信息
          - 保标招标网
          - 中国采购与招标网
          - 中国国际招标网（针对机电产品）
          - 机电产品招标投标电子交易平台
          - 全国招标信息网
          - 全民招标网
          - 中航招标网
          - 招投标网
          - 中国招标投标网
          - 蚂蚁匠人网
          - 中国采招网
        - 软件著作权
          - 软件名称
          - 软件简称
    - JWT 越权
    - .git 文件泄露
    - Token
    - 工作笔记
- **指纹识别**
  - 服务
    - 云悉
    - Wappalyzer
    - WhatWeb
    - observer_ward
    - EHole
    - Finger
    - xapp
  - WAF
    - wafw00f
    - waf-scan
- **漏洞扫描**
  - xray
  - xpoc
  - nuclei
- **交互**
  - 获取公开接口
    - FindSomthing — 将路径放到 Burp Suite 中使用 GET 和 POST 各跑一遍 — 不响应的路径则尝试在 Open Multiple URLs 中访问
    - Burp Suite — APIFinder
    - JS 文件 — 检索接口常用参数
  - 构造隐藏接口
    - 在 JS 文件中检索公开接口，得到相似的隐藏接口 — 获取请求条件
    - 在当前业务或相似业务的其它功能 — 获取请求参数
  - 请求包 — 绕过
    - 401
    - 403
    - 500
    - 访问
      - 未授权访问 — 密码爆破
      - SQL 注入
      - XSS
      - URL 跳转
- **账户**
  - 用户注册
    - 用户名枚举
    - 短信轰炸
    - 任意用户注册
  - 用户登录
    - 源代码 — 信息泄露
    - 目录扫描
    - SQL 注入
    - 未授权访问 — 构造 API
    - 页面跳转 — URL 可控 — SSRF
    - 用户名枚举
    - 弱口令
    - 密码爆破
    - 短信轰炸
    - 验证码
      - 验证码回显
      - 验证码不过期
      - 验证码 DDOS
    - 任意用户登录
      - 修改返回包
      - 修改参数
    - 并发接收手机验证码
  - 忘记密码 — 任意密码修改
  - 头像上传
  - 个人资料
    - 增加
      - 存储型 XSS
      - SQL 注入
    - 删除 — 越权删除
    - 修改
      - 存储型 XSS
      - SQL 注入
    - 查看 — 越权查看
- **社区**
  - 并发
    - 点赞
    - 签到
    - 抽奖
    - 关注
  - 评论
    - SQL 注入
    - 存储型 XSS
    - 并发
  - 文件下载
  - 文件上传 — PDF-XSS
  - 搜索框
    - SQL 注入
    - 反射型 XSS
- **商城**
  - 隐藏商品
  - 并发积分兑换
  - 收货地址
- **支付**
  - 溢出
  - 四舍五入
  - 并发支付

Presented with xmind