# 2.10-目录扫描收集信息（无涯）

- 什么是目录扫描
  - 部署的网站有一些敏感文件
    - 配置文件 — xxx.cfg
    - 数据文件
      - xxx.sql
      - .tar.gz
    - 目录
      - /backup
      - /conf
      - /admin
  - 会泄露哪些信息
    - 数据库用户名和密码
    - 服务器的用户名和密码
    - 网站源码
    - 数据库的文件
    - .....
  - 为什么会泄露？
    - 配置不当的问题
    - 本地文件包含
      - local file inclusion（LFI）
      - PHP
        - header.php
        - common.php
        - footer.php
        - function.php
      - include("路径/文件") — include("../../..")
      - require();
      - dvwa靶场
        - http://localhost/dvwa/vulnerabilities/fi/?page=../../phpinfo.php
        - http://localhost/dvwa/vulnerabilities/fi/?page=../../../../../../in.txt
- 常见的敏感目录和文件
  - robots.txt
  - sitemap.xml
  - 网站的备份文件/数据
    - 在线压缩
      - 路径
      - 文件名
      - wwwroot — 20210819.zip
    - 帝国备份王 — 1.sql — 1.zip
  - 后台登录的目录
    - /admin
    - /manage
  - 安装包（源码）
    - 非开源，商用
    - 1.zip
  - 上传的目录
    - 文件上传漏洞 — webshell
    - /upload
    - /upload.php
  - mysql的管理界面
    - MySQL
    - web页面去管理
    - phpadmin — 密码爆破 — webshell
  - 程序的安装路径 — /install
  - php的探针
    - phpinfo
    - 雅黑探针
  - 文本编辑器
    - Ueditor — https://github.com/fex-team/ueditor
    - kindeditor
    - CKeditor
    - 文件上传漏洞、命令注入
  - Linux
    - /etc/passwd
    - /etc/shadow — SHA512
    - /etc/sudoers — sudo
  - MacOS — .DS_Store
  - 编辑器的临时文件.swp
  - 目录穿越
    - Windows IIS
    - Apache
    - pikachu靶场
      - http://localhost/pikachu/vul/dir/dir_list.php?title=jarheads.php
      - http://localhost/pikachu/vul/dir/dir_list.php?title=../../../../Windows/win.ini
  - tomcat WEB-INF
    - WEB-INF/web.xml : Web应用程序配置文件，描述了servlet和其他的应用组件配置及命名规则.
    - WEB-INF/database.properties : 数据库配置文件
    - WEB-INF/classes/ : 一般用来存放Java类文件(.class)
    - WEB-INF/lib/ : 用来存放打包好的库(.jar)
    - WEB-INF/src/ : 用来放源代码(.asp和.php等)
  - 其他非常规文件
    - secret.txt
    - password.txt
- 文件扫描思路
  - 做法 — 直接在域名后面拼接路径/文件名，如果返回200，就是存在
  - 扫描方法？
    - 递归 — dir xxx — dir xxx
    - 字典 — dict
    - 暴力破解
      - 1位
        - a-z
        - 0-9
      - 2位
        - aa
        - 00
        - a0
        - 9z
    - 爬虫
      - robots.txt
      - sitemap.xlml
      - 网页中的其他链接
    - fuzz（模糊测试） — 字典
      - /word
      - /index.php?word=
- 文件扫描的字典
  - kali — wordlists
  - dirb — /usr/share/wordlists/dirb/common.txt
- 工具
  - dirb
  - dirbuster
  - 御剑
  - Burp Suite
    - Intruder — payload
    - www.baidu.com/SbbsS
  - DirBrute
  - Dirsearch
  - Dirmap
  - wfuzz
- 注意事项 — WAF、IDS
  - 代理
  - 网络空间搜索引擎
- 防御
  - 权限
  - 删除敏感文件
  - WAF、IDS