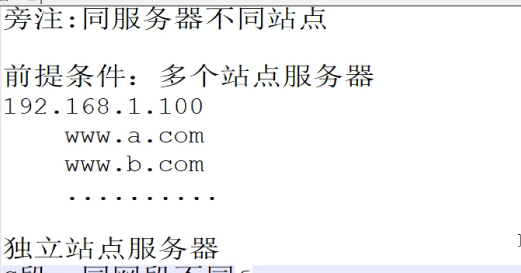
# 6.信息收集：web，app，其他

1. 有无WEB
   1. 无CDN
      1. 程序源码（转到 2.WEB源码）
         1. 内部/未知CMS
         2. 开源CMS
      2. 其他————树立简要思路
         1. 操作系统
         2. 搭建平台
         3. 数据库类型
      3. 站点搭建————目标多，机会大
         1. 目录型站点
            1. 定义：同一网站有两套或多套程序，就有多种漏洞方案
            2. 实例：[sti.blcu.edu.cn](http://sti.blcu.edu.cn/)
         2. 端口类站点
            1. 定义：不同网站放在不同端口上
            2. 实例：[web.0516jz.com](http://web.0516jz.com/)

运用端口扫描

* + - 1. 子域名站点
         1. 定义：添加子域名后网站不同，ip不同，可能在同一服务器上
         2. 实例：[goodlift.com](http://goodlift.com/)，[bbs.goodlift.com](http://bbs.goodlift.com/)
      2. 旁注，c段站点
         1. 定义：

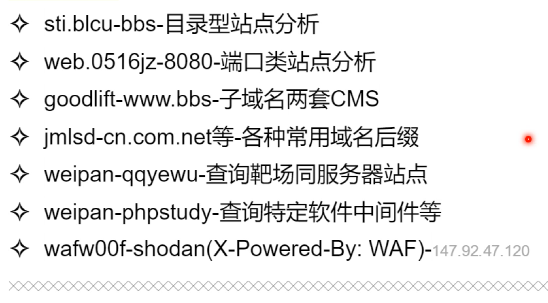
旁注：同服务器不同站点



C段：同网段不同服务器不同站点



* + - * 1. 通过拿下其他站点来得到目标站点
      1. 类似域名站点，搭建软件特征站点
         1. 定义：一个网站多个域名
         2. 实例：[www.jmlsd.cn](http://www.jmlsd.cn/)
      2. ……
    1. 防护应用WAF————防止被墙
       1. 安全狗
       2. 宝塔
       3. 云盾
       4. 安骑士
       5. 防火墙：浏览器里network里查看防火墙X-Powered-By：WAF



* 1. 有CDN————先行绕过后续接上（转到 5.信息收集：CDN绕过）
     1. 国外请求
     2. 接口查询
     3. 黑暗引擎
     4. 扫描全网
     5. 子域名
     6. ……

1. 有无APP
   1. 涉及WEB（转到 有无WEB）
   2. 非WEB协议————区分测试方法
      1. 尝试提取：apk提取工具，burp抓包
      2. 反编译逆向
      3. （若还无WEB转到 有无其他）
2. 有无其他
   1. 思路：对准ip
      1. 端口乱扫
      2. 接口乱扫
      3. 接口部分一顿测试
   2. 资产信息————侧门信息
      1. 以上各种平台信息
      2. whois备案等
      3. github等监控
         1. 便于收集整理最新exp或poc
         2. 便于发现相关测试目标的资产
   3. 第三方应用————从这些入手
      1. 数据库应用
         1. mysql
         2. mssql
         3. oracle
         4. ……
      2. 各种管理平台
         1. weblogic
         2. phpmyadmin
         3. ……
      3. 各种第三方应用
         1. vsftpd
         2. nexus
         3. git
         4. ……
   4. 各种服务接口————发现更多未知的接口尝试
      1. 存储服务
      2. 支付服务
      3. 内部服务
      4. ……
   5. 微信公众号等，找更多的应用继续————发现更多未知的应用
      1. 涉及web
      2. 涉及APP
      3. 涉及其他
   6. 内部群或内部应用等————社工或发现更多未知的应用
      1. QQ或微信群
      2. 工作群（钉钉等）
      3. 其他通讯群聊等