1. 为什么asp容易入手？
   1. 已知漏洞多，方便入门
   2. 多部署在service2003上，系统老
   3. web服务器本身有漏洞
2. 案例步骤分析
   1. google hack寻找测试目标
      1. 搜索：公司 inurl:asp?id=
   2. 一个asp站点的sql注入
      1. 测试数字型注入点
         1. 常见数字型测试方法
            1. 加个’
            2. 加 and 1=1 然后再 and 1=2
      2. sqlmap拆解数据库和表名
         1. sqlmap -u http://........ --dbs --current-user
      3. dump表数据
      4. 登录后台