# 小迪安全

## 概念名词

### 域名

多级域名的概念等同二级域名(cht.worl-xml.com)，不过比二级域名更加延伸，比如我们继续扩展该域名的主机名，设置主机名为 bbs.at,那么就可以建立一个三级域名：bbs.at.worl-xml.com，当然也可以建立四级域名bbs.at.go.worl- xml.com，五级域名bbs.at.go.home.worl-xml.com……，依次类推，可以建立无限级别的域名，我们统称这些域名为顶级域名 worl-xml.com的子域名

### DNS

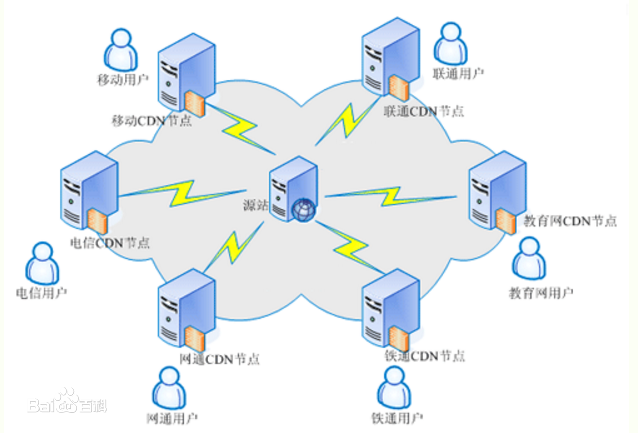
DNS: 解析域名对应的ip地址（全球有13个dns解析服务器）

Host：重定向域名对应的ip地址 路径：C:\Windows\System32\drivers\etc\hosts

CDN：内部分发网络（缓存节点技术） 访问时会找网络最快的节点

超级ping ping.chinaz.com

网站核心不在节点网站（缓存），扫描网站扫的是缓存，扫不到真实目标下面的东西，做安全检查检测的也是缓存



### 脚本语言

主流：PHP、Javaweb (少见：asp、jap、py、pl、cgo等)

不同脚本类型的框架安全系数不同

### 后门

入侵或测试后留得一个后门文件，便于下次对于这个目标进行操作（拿到权限，留下后门）

类型很多，作用：控制网站 目的：更好的控制目标

玩法：后门有各种各样的玩法

免杀：防止后门被检测到

### Web

Web的组成架构模型：

网站源码： 分脚本类型、分应用方向

操作系统：windows linux

中间件（搭建平台）：apache、iis、tomcat、nginx等

数据库：access、mysql、ms sql、oracle、sybase、db2、postsql等

不同脚本类型的框架安全系数不同

### Web相关安全漏洞

主流：PHP、Javaweb (少见：asp、jap、py、pl、cgo等)

不同脚本类型的框架安全系数不同