基础入门-概念名词

前言：简要说明下学习的整个知识点，学习计划，学习目标等，通过这次培训能学到那些安全技能，涉及那些安全方向？

域名

什么是域名？
域名在哪里注册？
什么是二级域名多级域名？
域名发现对于安全测试意义？

DNS

什么是 DNS？
本地 HOSTS 与 DNS 的关系？
CDN 是什么？与 DNS 的关系？
常见的 DNS 安全攻击有哪些？

脚本语言

常见的脚本语言类型有哪些？
asp php aspx jsp javaweb pl py cgi 等

不同脚本类型与安全漏洞的关系？
漏洞挖掘代码审计与脚本类型的关系？

后门

什么是后门？有那些后门？

后门在安全测试中的实际意义？
关于后门需要了解那些？（玩法，免杀）

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 mssql oracle sybase db2 postsql 等

架构漏洞安全测试简要介绍？
为什么要从 WEB 层面为主为首？

WEB 相关安全漏洞

WEB 源码类对应漏洞
SQL 注入，上传，XSS，代码执行，变量覆盖，逻辑漏洞，反序列化等
WEB 中间件对应漏洞
WEB 数据库对应漏洞
WEB 系统层对应漏洞
其他第三方对应漏洞
APP 或 PC 应用结合类

演示案例：

- 多级域名的枚举查找（原理，方式）
- DNS 解析修改后分析（本地或服务）
- EXE 后门功能及危害及类似 WEB 后门
- APP 类结合 WEB 协议，PC 类结合 WEB 协议

涉及资源：

http://www.xyaz.cn

http://www.downcc.com/soft/11196.html

https://github.com/quasar/QuasarRAT/releases

https://pan.baidu.com/s/13_i1ExwEaA59GfMt1Rp0Hg 提取码：0b7b
