Web系统测试

4.1 渗透测试概述



目录

- 〉渗透测试基础概念
- ▶Web服务器可能存在的漏洞
- >怎样做渗透测试



渗透测试基础概念



一什么是渗透测试

- ●通过模拟真实黑客的技术手段对目标进行漏洞检测,突破系统的安全防护手段,深入评估漏洞所可能造成的实际影响
- ▶渗透测试与安全测试的区别
 - ●渗透测试侧重于几个点的穿透攻击
 - ●安全测试是侧重于对安全威胁的建模,系统的对来自各个方面,各个层面威胁的全面考量。安全测试可以告诉您,您的系统可能会来自哪个方面的威胁,正在遭受哪些威胁,以及您的系统已经可抵御什么样的威胁

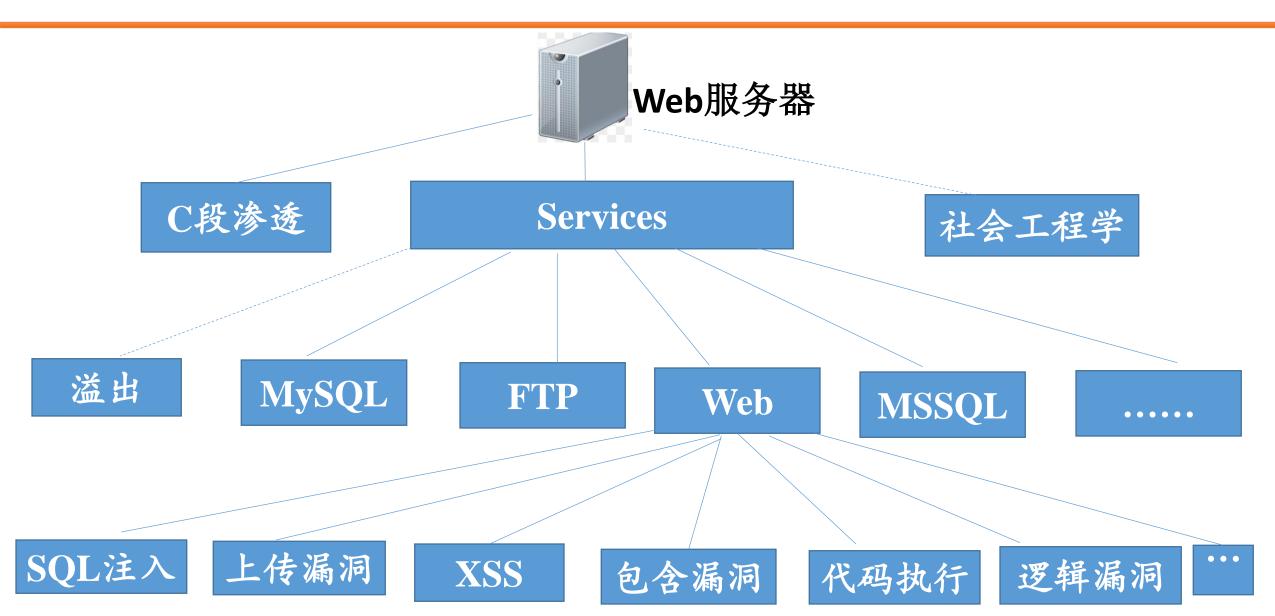
渗透测试基础概念



- ▶为什么要进行渗透测试
 - ●保障Web服务器端的安全
- ▶Web服务器是怎样被入侵的
 - ●直接针对目标进行攻击,比如端口扫描、密码爆破、缓冲区溢出攻击等方式直接获取目标权限

可能存在的漏洞





怎样做渗透测试



〉渗透测试

●通过实际的攻击进行安全测试与评估的方法就是渗透测试

(Penetration Testing, Pentest)

渗透测试流程



- ▶明确目标
- ▶信息收集
- >漏洞探测
- ▶漏洞验证
- ▶编写报告
- ▶信息整理与分析

渗透测试流程



▶信息收集

- ●Web页面爬取
- ●网站结构进行爆破扫描
- ●目标服务器端口扫描

>探测漏洞

- ●SQL注入漏洞
- ●XSS跨站脚本攻击
- ●文件上传漏洞

总结



- >渗透测试基础概念
- ▶Web服务器可能存在的漏洞
- >怎样做渗透测试
 - ●渗透测试流程

Question

