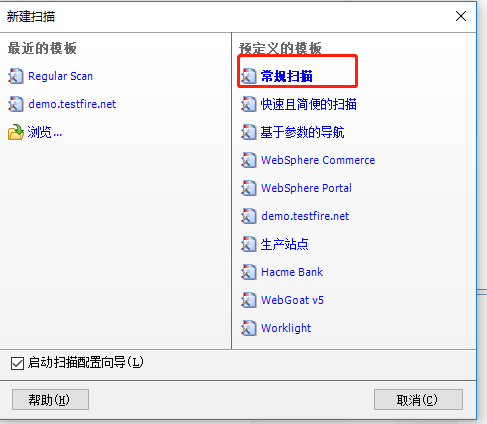
**Web漏洞评估**

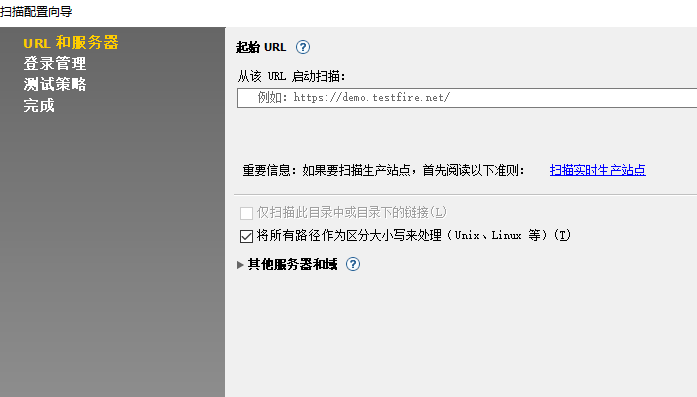
Appscan是由IBM公司开发的一款在web应用程序渗透测试舞台上使用最广泛的工具，有助于专业人员进行web应用程序自动化脆弱性评估

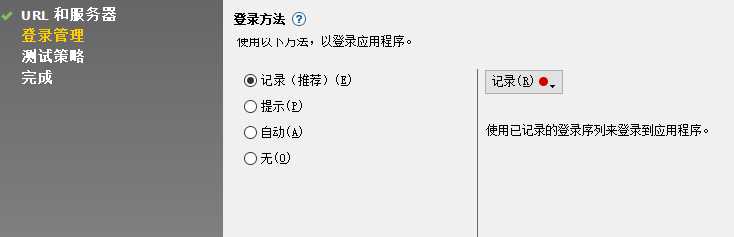
新建扫描



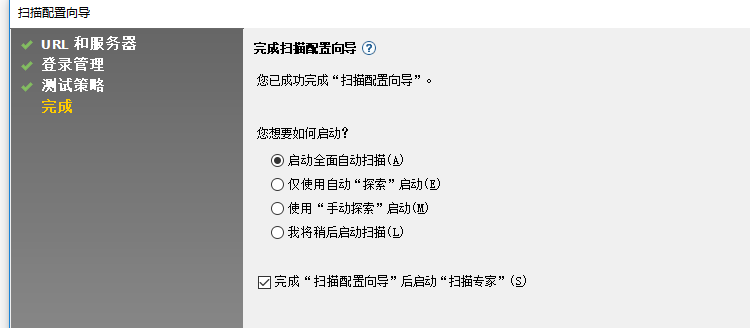


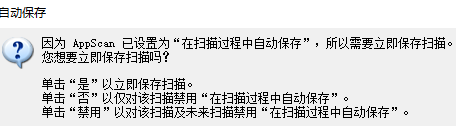
下一步





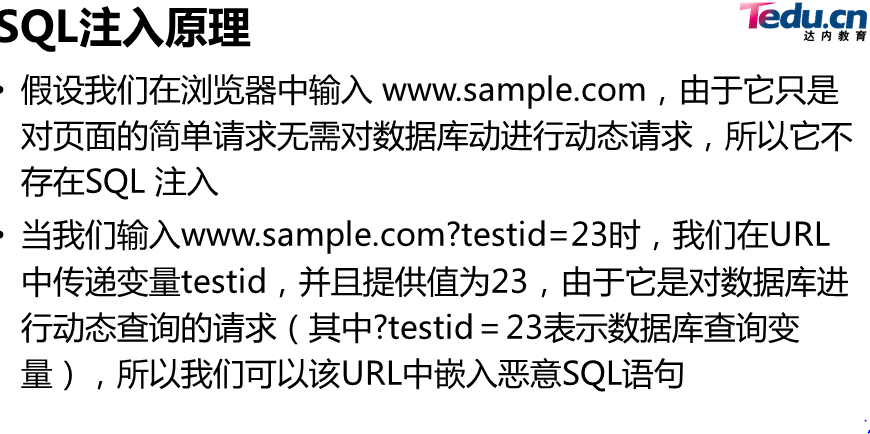


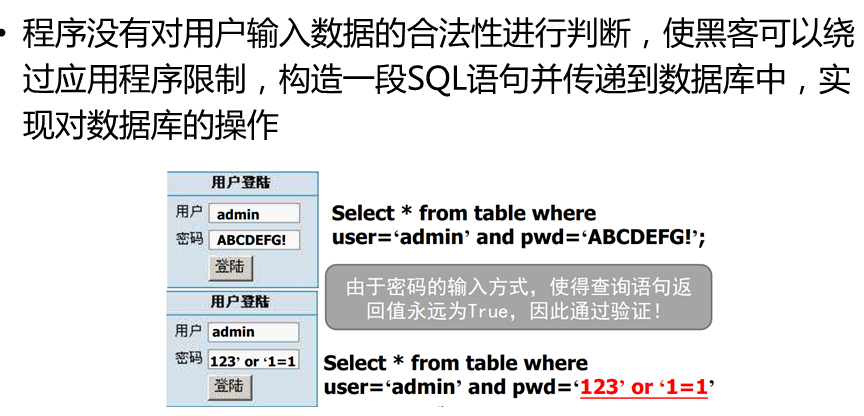




**SQL入注**

原理：用户对数据库进行动态查询请求，所以可以在URL中嵌入恶意SQL语句。程序没有对用户输入数据的合法性进行判断，构造一段SQL语句并传递到数据库中，实现对数据库的操作





危害：数据信息的搜集

操作数据库

增加数据

删除数据

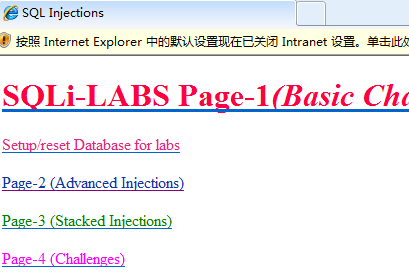
更改数据

操作系统

借助数据库的内置功能操作系统

演示：

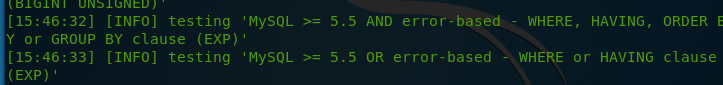
建网站：



Sqlmap命令（kali）

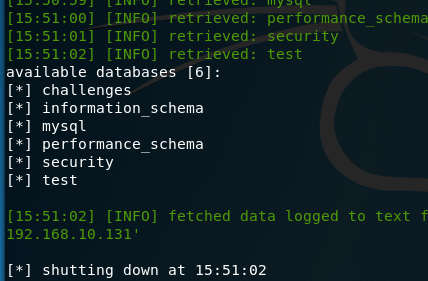
进入漏洞





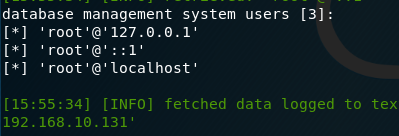
获取数据库信息





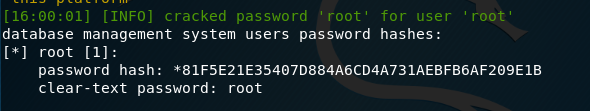
获取用户名





获取密码





**社会工程学**

概述：

黑客米特尼克在《欺骗的艺术》中所提出的

利用人性弱点（本能反应、贪婪、易于信任等）进行欺骗获取利益的攻击方法

社会工程学的危害：

永远有效的攻击方法

人是最不可控的因素

**安全管理体系标准**

ISO 27001概述

信息安全管理使用规则ISO 27001的前身为英国的BS7799标准，该标准由英国标准协会（BSI）于1995年2月提出

它提供了一套综合的、有信息安全最佳惯例组成的实施规则，其目的是作为确定工商业信息系统在大多数情况所需控制范围的唯一参考基准，并且适用于大中小组织

ISO 27001认证

信息安全管理体系标准（ISO 27001）可有效保护信息资源，保护信息化进程健康、有序、可持续发展

ISO 27001是信息安全领域的管理体系标准，类似于质量体系认真的ISO 9000标准

当组织通过了ISO 27001的认证，就相当于通过了ISO 9000的质量认证一般，表示组织信息安全管理已经建立了一套科学有效的管理体系作为保障

总体来说，建立信息安全管理体系一般要经过下列四个基本步骤

信息安全管理体系成都策划与准备

信息安全管理体系文件的编制

信息安全管理体系的运行

信息安全体系的审核与评审

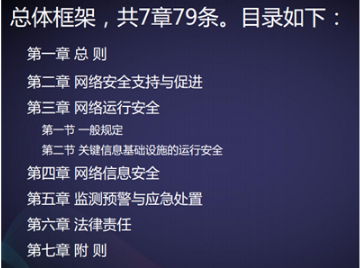
**等级保护**

等级保护编年史



网络安全法

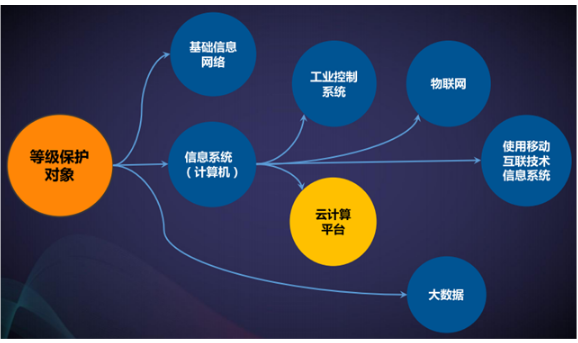


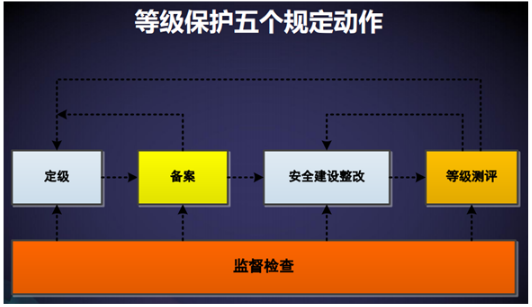




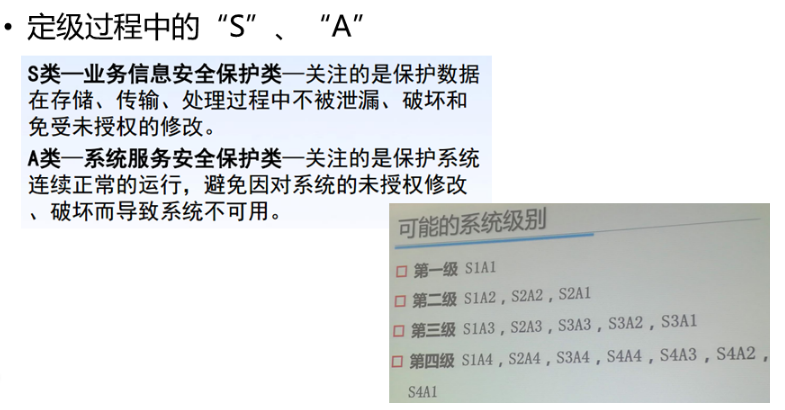
等级保护概述

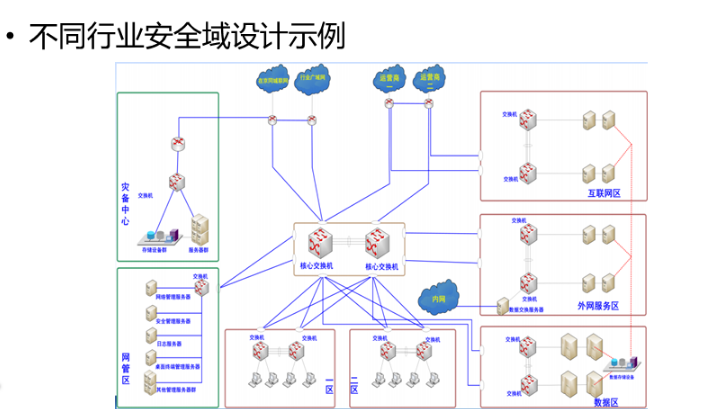








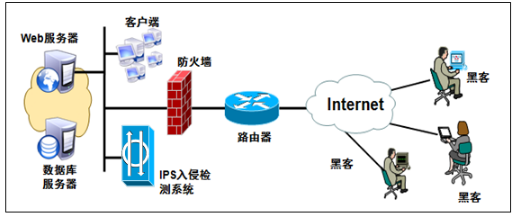




**网络安全解决方案**

企业网络安全应用

从网络安全防护的角度来看，应当认真制定有针对性的策略。明确安全对象，设置强有力的安全保障体系，有的放矢，在网络中层层设防，让攻击者无计可施



三分技术，七分管理

首先不仅是网络管理员，企业管理者和企业中的任何一名员工都应该建立起信息安全的意识，只有有了这样的安全意识后，网络安全才能够实现

其次才是安全防范手段

网络安全解决方案将从网络设备、操作系统、应用服务，加装防火墙和入侵检测系统等几个层面对企业网络的安全提供全面的保护

加固系统，不论是windows还是linux的操作系统，都难面会存在漏洞或缺陷

安装防火墙软件，注意病毒库的定期更新

部署防火墙、入侵检测/防御系统等安全设备。