软件安全性测试培训考试试卷

**部门：　　　　　　　　　　　　姓名：**

1. **单选题（30分，每题2分）**
2. 信息安全系统安全保护等级分为（　　C　　　　）。

A、3级 B、4级 C、5级 D、6级

1. 从信息安全发展角度，目前主要是确保什么安全？（　　D　）。

A、通信 B、计算机 C、人 D、信息和信息系统资产

1. 防火墙的原则是什么（　B　　　　　）。

A、防攻击能力好 B、一切未被允许的就是禁止的！

C、一切未被禁止的都是允许的！ D、是否漏电

1. IDS和IPS的部署模式是（　D　　）。

A、都是旁路模式 B、都是在线模式

C、IDS在线模式、IPS旁路模式 D、IDS旁路模式、IPS在线模式

1. VPN是什么？（　D　　　　　）。

A、安全设备 B、防病毒软件 C、安全测试软件

D、虚拟专用网络

1. 下列哪个不是常见的安全设计问题（A　　　　）。

A、数据库表太多 B、密码技术使用的败笔

C、创建自己的密码技术 D、错误的处理私密信息

1. 下面哪个不是VPN分类包括的（　　A　　　　）。

A、主机对远程用户 B、主机对VPN 网关

C、VPN网关对VPN 网关 D、远程用户对VPN 网关

1. 动态测试方法不包括（　　D　　　　）。

A、手动分析技术B、安全扫描C、渗透测试D、用户测试

1. 最新的WEB系统版本是（　　D　　　　）。

A、Web7.0 B、Weblogic8.0 C、Websphere3.0 D、Web3.0

1. 渗透测试模拟什么角色进行（　　A　　　　）。

A、模拟黑客 B、模拟用户 C、模拟系统管理员 D、模拟开发

1. 信息系统安全问题产生的外因是什么（　　　B　　　）。

A、过程复杂 B、对手的威胁与破坏

C、结构复杂 D、使用复杂

1. 关于测试的思想转变，描述正确的是（　　A　　　　）。

A、所有系统不允许的事件都去想办法允许。

B、所有系统允许的事件都去想办法不允许。

C、根据用户指定内容进行测试。

D、根据开发人员指定内容进行测试。

1. 以下不属于安全测试的辅助工具的是（　　D　　）。

A、wireshark B、APPSCAN C、Zenmap D、QTP

1. 下列哪种不属于WEB系统文件上传功能安全隐患（D）。

A、未限制扩展名 B、未检查文件内容

C、未查杀病毒文件 D、未检查文件大小

1. 以下哪种说法是对的（　　B　　　　）。
2. 关系数据库不需要进行安全测试。
3. 通过软件安全测试能够降低安全隐患。
4. 通过软件安全测试能够杜绝安全隐患。
5. 一个应用系统只需要一种测试工具测试。
6. **多选题（30分，每题3分，少选给2分，多选无分）**
7. 以下属于软件安全产品的是（　CD　　　）。

A、交换机 B、路由器 C、防火墙 D、IDS/IPS

1. 主机IDS监测的资源主要包括（ABCD　）。

A、网络 B、文件 C、进程 D、系统日志

1. 关于软件安全开发周期正确的说法是（　　AD　　）。

A、软件安全生命周期纳入到软件生命周期。

B、软件生命周期贯穿软件安全生命周期中的每个阶段。

C、软件生命周期纳入到软件安全生命周期。

D、软件安全生命周期贯穿软件生命周期中的每个阶段。

1. 测试实施阶段的工作包括（　ABC　　　）。

A、白盒测试 B、黑盒测试 C、灰盒测试 D、蓝盒测试

1. 安全测试七个接触点包括（　　ABCD　　　　）。

A、代码审核 B、滥用案例 C、安全操作 D、渗透测试

1. 根据渗透目标分类，渗透测试包括（ABCD）。

A、主机操作系统渗透 B、数据库系统渗透

C、应用系统渗透 D、网络设备渗透

1. 下面哪种是跨站脚本的攻击形式（　　ABCD　　）。

A、盗取Cookie B、钓鱼

C、操纵受害者的浏览器 D、蠕虫攻击

1. WEB系统动态安全测试手段包括（　　ABC　　　）。

A、手动检查/配置检查 B、渗透测试

C、安全扫描 D、用户测试

1. Web应用系统十大漏洞包括（　ABCD　　　）。

A、反射型跨站 B、存储型跨站C、DOM跨站D、跨站脚本

1. 软件安全开发周期包括（　ABC　　　　）。

A、安全需求‐攻击用例 B、架构和设计评审/威胁建模

C、安全编码原则 D、软件版本更新

1. **填空题（30分，每空3分）**
2. 信息系统安全由　物理安全　　、网络安全、系统安全、应用安全、安全管理等五部分组成。
3. 信息系统安全等级中，第一级是　　用户自主保护　。
4. 等级保护评估手段包括管理评估、　　技术评估　　。
5. 防火墙的类型包括　包过滤防火墙　　、应用网关(应用代理)防火墙、状态检测包过滤防火墙等。
6. IDS中文名称是　　入侵检测系统　　　　　　　　　。
7. 软件安全测试应该像　　攻击者　　　　　　一样思考。
8. 隔离网闸由　外部系统　、内部系统和数据交换系统（开关系统）组成。
9. 根据渗透方法分类，渗透测试包括：黑箱测试、　白盒测试、隐秘测试。
10. 安全测试法包括　静态测试　　　　和动态测试。
11. 隐藏在软件中的漏洞包括　设计漏洞　　　　与实现漏洞。
12. 问答题（10分）

1、软件安全测试的常规方法是什么？（5分）

* 猜错法测试
* 模糊测试
* 语法测试
* 故障注入

3、关于在实际工作中开展软件安全测试，谈谈你的想法（5）