

信息安全保障人员认证（CISAW）考试大纲

安全软件方向（基础级/专业级）

第一部分 考核目标

本考试大纲依据《信息安全保障人员认证准则》，确定信息安全保障人员认证（CISAW）安全软件方向的考试目标和要求。

信息安全保障人员认证（CISAW）安全软件方向的考试主要考查考生在软件安全开发中的基础知识和基本技能掌握程度与综合运用所学知识分析、解决软件安全开发问题的能力。本考试大纲适用于申请信息安全保障人员认证（CISAW）安全软件方向基础级和专业级的考生。

第二部分 考点的层次要求

本考试对考点的层次要求依次是了解、理解、综合应用三个层次，具体内容要求如下：

1. 了解：要求考生对所列知识的含义有初步的、感性的认识，知道这一知识内容是什么，按照一定的程序和步骤照样模仿，并能(或会)在有关的问题中予以识别。

2. 理解：要求考生对所列知识内容有较深刻的理性认识，知道知识间的逻辑关系，能够对所列知识做正确的描述说明并表达，能够利用所学的知识内容对有关问题进行比较、判别、讨论，具备利用所学知识解决简单问题的能力。

3. 综合应用：要求考生能够对所列的知识内容进行推导或证明，

能够利用所学知识对问题进行分析、研究、讨论，并且加以解决。

第三部分 能力要求

本考试主要考查考生在软件安全开发、项目管理及技术服务所需的沟通理解能力、数据处理能力、推理论证能力、实践操作能力和总结分析能力，具体要求如下：

1. 沟通理解能力：考生应具有针对安全软件开发的需求调研、用户及团队协调沟通的基本能力。
2. 数据处理能力：考生应具有针对安全软件开发的需求分析、安全测试、试运行过程的数据记录、分析、处理等基本能力。
3. 推理论证能力：考生应具有针对软件服务项目的研发方案开展设计，对安全策略进行制定，建立软件研发项目应急处理方案和处理项目变更的能力。
4. 实践操作能力：考生应具有针对安全软件开发过程中涉及的代码开发、软件测试和项目维护等活动的实践操作能力。
5. 总结分析能力：考生应具在安全软件开发过程中对所涉及的需求分析、概要设计、详细设计、软件开发、软件测试、项目交付、项目验收和项目维护的全软件开发生命周期进行综合分析处理能力。

第四部分 考试内容

知识内容		要求
软件安全概述	软件安全的定义	综合应用
	软件安全的范畴	综合应用
	软件生命周期中的安全问题	了解
	软件安全问题产生的原因	了解

软件安全开发模型	常用软件开发方法及安全开发模型	综合应用
	软件安全 SDL 及 McGraw 模型	理解
	NIST 安全开发生命周期模型	了解
	CISAW 软件安全开发模型	理解
	瀑布型及渐增型软件开发模型	了解
安全漏洞管理	漏洞管理	综合应用
	典型软件安全漏洞	理解
	OWASP Top 10 Web 安全漏洞	了解
软件安全功能设计	安全审计数据产生、分析及审阅	理解
	原发抗抵赖及接收抗抵赖	了解
	用户数据保护	综合应用
安全编码	安全编码概述	了解
	常见编码安全问题分类	理解
	整型数据、字符串数据及数组数据等常见安全问题	综合应用
	移动开发安全规范	了解
软件安全测试	软件安全测试过程	理解
	渗透测试	理解
	软件安全测试方法	综合应用
新技术风险	风险管理概念	了解
	软件安全组织与人员管理	了解
	软件开发中存在的新技术风险	了解

第五部分 试卷满分及考试时间

本考试为笔试试卷，满分 120 分。考试时间为 150 分钟，84 分

（含）以上为合格分。如考生有作弊行为则该考生最终笔试成绩为 0 分。

考生笔试考试成绩为“合格”的，该考生可根据《信息安全保障人员认证准则》相关要求，被授予基础级或专业级认证证书。

第六部分 试卷内容结构

知识内容	所占比例（%）
软件安全概述	10%
软件安全开发模型	10%
安全漏洞管理	20%
软件安全功能设计	15%
安全编码	20%
软件安全测试	15%
新技术风险	10%

第七部分 答题方式

笔试，闭卷独立完成。

第八部分 试卷题型结构

- 1. 单选题 50 题，每小题 1 分，共 50 分
- 2. 多选题 10 题，每小题 2 分，共 20 分
- 3. 简答题 2 题，每小题 7 分，共 14 分
- 4. 综合案例题 3 题，每小题 12 分，共 36 分

第九部分 例题

- 1. 单选题

以下关于 Linux 系统/etc/passwd 文件被篡改的危害，描述正确的是
()

- A. 攻击者可直接读取所有用户的密码明文
- B. 修改该文件对系统安全没有直接威胁
- C. 由于该文件权限为 644，普通用户永远无法修改
- D. 攻击者可通过添加 UID=0 的条目直接创建具有 root 权限的后门

账户

答案：D

解析：若/etc/passwd 对普通用户可写（权限设置错误），攻击者可直接追加 UID=0 的账户条目，创建具有 root 权限的后门账户，严重威胁系统安全。

2. 多选题

给出问题描述，要求从给出的四个答案中选择其中恰当的 2 到 4 个，多选或少选不得分。

例：在 Web 应用软件的分层测试策略中，下列哪个是测试关注的层次
()。

- A. 数据层
- B. 业务层
- C. 服务层
- D. 表示层

答案：ABD

说明：本题主要考点为软件安全测试方法，属于测试的基本问题，是综合应用的知识。从软件开发角度分析，通常使用三层架构，分为表

现层、业务层、数据层，这三层在测试时都是要重点关注的内容，因此 ABD 皆为正确选项。而 C 选项服务层一般都是采用外部接口完成，例如天气预报等服务，这种接口是测试不了的。

3. 简答题

给出问题描述，要求用简练的语言回答问题。

例：请简要论述软件安全属性有哪些。

答案：

（1）机密性。软件必须确保其特性、资源管理和内容对未授权实体隐藏。

（2）完整性。软件及其管理的资源必须能够抵御入侵并能从中恢复。

（3）可用性。软件必须对授权用户开放，即可操作和运行，而对未授权用户应该关闭，即不可操作和运行。

（4）可追溯性。所有与安全相关的软件行为都必须跟踪与记录，并进行责任归因。

（5）抗抵赖性：这一属性是指软件防止用户否认执行了某些行为的功能，以保证可追踪性不受到破坏。

说明：本题考察的是“软件安全的定义”，属于综合应用的知识。如何评判一个软件是否足够安全，著名的软件安全专家 Julia H. Allen 给出了一个安全的软件需要满足的属性，这些属性是软件安全的重要因素，主要包括：机密性、完整性、可用性、可追溯性、抗抵赖性。

4. 案例综合题

利用多个知识点解答给定实际问题。

例：小李问业务部门的需求代表：“对所定制开发的软件在安全方面

有哪些要求？”业务部门的需求代表回答：“只要能够保证安全就可以了。”结果小李对软件安全的功能需求还是不清楚。

请分析小李在需求调查中没有获取到软件安全方面的功能需求的主要原因，并给出建议。

答：需求调查过程中没有获取到软件安全方面的功能需求的主要原因如下：

- 1) 在软件系统功能调查中，从业务代表主要是获取业务功能方面的需求；
- 2) 软件安全需求是属于软件非功能性需求，不属于业务功能需求范围；
- 3) 不能要求业务代表对于软件安全方面具备相关的专业知识；
- 4) 不能要求业务代表对于软件系统的外部安全威胁具有丰富经验。

为了能够获取软件安全方面的功能需求，建议完成如下工作内容：

- 1) 与业务代表共同识别业务相关的资产及其重要性，如业务数据；
- 2) 对业务相关的资产的脆弱性进行分析；
- 3) 识别业务相关的资产可能受到威胁；
- 4) 对业务相关资产进行风险评估；
- 5) 确定对业务相关资产采取的安全措施，并识别软件系统中所需要采取的措施；
- 6) 将软件系统中所需要采取的措施转变成软件安全性功能需求。

说明：本题考察的是“常用软件开发方法及安全开发模型”，属于综合应用的知识。首先明确软件安全需求属于软件非功能性需求，然后明确软件安全需求的确认方式，进而对具体的安全需求进行确认。