模拟卷
高级大纲

安全性测试

GA 版本 – 2016/03

国际软件测试认证委员会

版本历史

版本	日期	备注
1.0 – Beta	2015/09/22	模拟题 Beta 版本
1.0 – GA 候选人	2016/03/04	经考试工作组评审后更新 – 18 和 29 题更新到 K3 level，确定 35 题，确定 #25 - #32 题的分数分布情况
1.0 – GA	2016/03/15	经过稍微改动后的 GA 版本。去除了学习目标的内容。

注意：该问题的学习目标被突出显示。对于某些问题，有几个学习目标可以从中得出问题。

AS-1.1.1（K2）理解风险评估在提供安全性测试计划的信息中所扮演的角色且设计和调整安全测试的业务需求
AS-1.3.1（K2）了解安全审计的目的

问题＃1（1 分）

以下哪一项是安全审计的目的？

a.防止用户使用简单的密码
b.显示供应商提供的补丁更新不足
c.阻止未经授权的入侵者访问系统
d.要求用户在预定的一组日期后更改密码

B是正确的，因为保持系统上的补丁更新是安全审计的目的之一。其他是良好的做法，但不是安全审计的目的。

AS-1.1.2（K4）识别要保护的重要资产，每种资产的价值和评估每项资产所需安全级别所需的数据
AS-1.1.3（K4）分析一个给定的情况，以确定适当的风险评估技术，以确定当前和未来的安全威胁

问题＃2（3 分）

作为风险评估的一部分，你负责确保项目外部引入的新供应商完全符合政府规定的指导方针。你应该主要关注哪些利益相关方，以确保这些外部供应商能持续遵守规定的指导方针。

a.客户，用户和供应商确保他们之间有良好的沟通
b.适用于信息来源的公共用户和供应商将遵守法律
c.中央和地方机构沟通指导方针遵循
d.内部和外部资源将使用这些信息来进一步分析风险

C 是正确的，因为这是指南的来源。准则可能会改变，所以与这些人保持沟通渠道的开放很重要。 A，B 和 D 都需要知情，但信息需要来自联邦和地方机构。

AS-1.2.1（K2）理解安全政策和程序的概念和它们是如何应用于信息系统

问题＃3（1 分）

下列哪项是将系统或设备访问最小化到可接受级别策略的结果？
a.添加更多设备以减轻影响
b.禁止对路由器等自配置设备进行适当的控制
c.不符合的设备将从无线网络中删除
d.访问 VPN 受到严格限制

C 是正确的。实施此政策后，不符合要求的设备将被删除，直至符合要求。 A 不正确，因为这不会是预期的结果。 B 是不正确的，因为这些控制将被鼓励。 D 不正确，因为访问将被控制，而不是严格限制。

AS-1.2.2（K4）分析一个给定的一组安全政策和程序以及安全性测试结果来确定有效性

问题＃4（3 分）

您作为安全管理员的角色是帮助您的组织理解整个企业安全策略和过程的有效性。分析完成后，您将向高级管理层报告您的有效性结果。以下哪项是实现此目标的最佳策略？

a.针对政策和程序独立实施静态分析评估
b.分析安全性测试的结果以验证有效性
c.评估关注当前威胁和攻击的安全性测试结果
d.评估新出现的软件威胁的静态测试结果

B 是正确的。您应该分析安全性测试的结果，看看是否遵守了政策和程序并且是有效的。 A 是不正确的，因为静态分析应该在代码上，如果有的话。 C 是不正确的，因为重点不应该只针对当前的威胁和攻击，还应该针对配置等。D 不正确，因为重点不仅仅在于新出现的威胁。

AS-2.2.1（K2）理解一个组织为什么需要引入安全性测试，以及引入之后所带来的好处，比如减少风险以及带来更高层次的信心和信任。

AS-2.3.1（K2）了解项目实际情况，业务限制，软件开发生命周期以及其他考虑因素是如何影响安全性测试团队的使命的。

问题＃5（1 分）

如果一个组织已经进行了安全性测试，那么对该组织有可能经历的安全漏洞和法律诉讼有什么帮助呢？

a.它可以表明该组织已尽职尽责，以防止发生此类事件
b.安全性测试的文档可以用来追查犯罪者
c.由于在安全性测试之前将备份任何重要信息，因此可以使用此备份来恢复任何受损信息
d.通过追踪记录的测试，安全性测试团队可以发现违规行为的可能性

答根据教学大纲是正确的。 B 不正确，因为这些信息可能没有帮助。 C 是不正确的，因为备份可能会过时，并且信息不一定被破坏，而是被盗或被查看。 D 是不正确的，因为虽然这可能有助于指出测试不足的地区，但它不会支持该组织对法律行为的辩护。

AS-2.4.1（K2）解释为什么安全性测试目标和目标必须与组织的安全策略和组织的其他测试目标相一致
AS-2.4.3（K2）理解信息保障和安全性测试之间的关系

问题＃6（1 分）

以下哪一项是正确的陈述？

a.信息保证是安全性测试的一部分
b.信息保证和安全性测试对于同样的事情是两个术语

c.安全性测试是信息保障的一部分
d.这两个术语指的是不同的安全领域

C 是正确的，安全性测试是更大的信息保证领域的一部分。

AS-2.4.2（K3）对于既定的项目场景，描述基于功能，技术特性以及已知漏洞定义安全性测试目标的能力。

问题＃7（2 分）

作为安全性测试团队的一员，您正在银行工作。在最近的安全审计中，有人指出用户的密码不够强大。从那时起，已经发布了一套新的要求来确保密码强度。考虑到这些信息，通用密码规则测试的一组合理安全目标是什么？

1.确认密码符合长度要求
2.确认密码符合使用字符，数字，字母和大写的要求
3.确认密码可以重试三次
4.确认密码不能在一年内重新使用
5.确认密码必须每三个月重置一次
6.确认用户可以请求将他们的密码通过电子邮件发送给他们
7.确认系统管理员可以重置锁定的密码

a. 1，2，3，4
b.1，2，4，5
C. 3，4，6，7
d. 4，5，6，7

B 是正确的，因为所有这些都是有效的安全目标。 A 是不正确的，因为 3 是功能性的而不是安全性相关的（除非它将它们锁定，但我们不知道这个说明）。 C 不正确，因为 6 和 7 都是功能性的而不是特定的安全性要求。由于与 C 相同的原因，D 不正确。

AS-2.5.1（K3）对于既定的项目，描述定义安全性测试目标以及加强敏感数据与物理资产完整性的需求之间的联系的能力。

问题＃8（2 分）

安全漏洞导致客户机密信息被盗后，贵公司最近成为头条新闻。管理层已经作出反应，指出安全性测试目标的范围需要立即扩大。虽然您同意需要做某些事情，但您担心这种方法可能过于具有反应性，并且可能无法实现所需的测试。

根据教学大纲，如果这些举措得到实施，什么是合理的关切？

a.测试仍然会漏掉问题，因为它不会很专注
b.测试将被外包，以便更有效地完成测试
c.测试范围可能太大，可能没有足够的资源来完成它
d.测试目标没有明确定义，可能会错过之前转入生产的相同问题

根据教学大纲 C 是正确的，因为当目标被广泛定义时，这是一个常见问题。 A 和 D 是合理的关注点，但我们不知道何时或如何定义测试目标，因此这可能是可控的。在这种情况下，B 始终是可能的并且可能是正确的做法，但目前还没有迹象表明外包将会发生。

AS-2.6.1（K4）分析一个给定的情况并确定哪些安全性测试方法最有可能成功
AS-2.6.2（K4）分析一个安全性测试方法失败的场景，并确定失败的原因。
AS-2.7.1（K4）分析关键绩效指标（关键绩效指标），以确定需要改进的安全性测试实践和不需要改进的因素

问题＃9（3 分）

您刚刚接受了一项工作，为公司创建安全性测试团队，公司主要是处理医生和医院之间共享的敏感医疗信息。您已经注意到，这些信息的安全性不足以防止黑客甚至意外暴露。你的前任曾经带来了一些顾问来做测试，但是这些测试结果没有文档化，也没有实施任何改变。事实上，你甚至不知道测试的覆盖范围。您已将您的发现呈现给执行管理团队。虽然他们原则上同意他们需要安全性测试，但他们没有为项目分配必要的预算或时间。看起来，虽然他们认为安全是一个好主意，但他们对于应该做什么或应该如何完成并不了解。你应该首先采取什么措施让高级管理人员与需要完成的工作保持一致？

a.创建所有可能的安全漏洞的详细列表，并将其提供给高管
b.提供您提出的测试方法的总结，并举例说明如何进行测试
c.引入法律团队来解释安全漏洞可能会给组织造成什么损失
d.创建安全策略和安全性测试策略，并演示如何与您提出的测试方法保持一致

D 是正确的。在这一点上，组织需要一个高层次的政策和计划来推进。如果没有这个政策，测试可能会继续是零碎的，将很难获得高层的支持和资金支撑。 A 和 C 在这一时间点上是不正确的，尽管如果您在实施该政策时遇到资金困难，它们可能会有用。 B 不正确，因为在定义方法之前，您需要一个总体策略。

AS-2.6.3（K3）对于既定场景，描述能够确定负责人以及将安全性测试的好处介绍给每个负责小组的能力。

问题＃10（2 分）

您刚刚从一次会议中来了解有关该组织安全方法的大量讨论。其中一个重点是测试的重要性，以确保数据免受欺诈性访问，尤其是信用卡信息。你被要求准备一套测试目标来帮助解决这个风险领域。你的任务之一是确保你覆盖利益相关者的所有关切。哪个利益主体组织最可能看到您的努力带来的好处？

a.经营管理层
b.合规官员
c.商业客户
d.监管官员

C是正确的。企业客户最关心的是防止欺诈访问，因为它们的数据是脆弱的。我们希望A，B和D也会参与其中，但这通常不是他们的主要好处。

AS-3.1.1（K3）对于某个项目，具有定义有效的安全性测试流程及其要素的能力。

问题＃11（2 分）

作为安全管理员，您负责安全过程的各个方面，包括测试。对于这个特定的过程，您将使用概念测试作为手动测试的基础，并从外部供应商的角度执行这些测试。哪种安全性测试流程最具有并行性？

a.安全性测试创造条件和目标
b.安全性测试实施
c.整体评估和报告安全性测试
d.安全性测试分析和设计

B是正确的。使用概念测试来创建手动测试并执行执行是安全性测试实施的一部分。 A和D是不正确的，因为这已经通过创建概念测试完成了。 C将在测试执行后发生。

AS-3.2.1（K4）分析安全性测试计划并对其优缺点提供反馈。

问题＃12（3 分）

您一直在为系统开发安全性测试计划，该系统将为患者存储医疗信息，并将该数据传输给专科医生。您已经在计划中涵盖了以下几个方面：
•范围（包括哪些在范围内以及哪些在范围之外）
•角色和任务
•责任（包括供应商责任与内部责任）
•高水平的时间表
•环境要求和设置
•必要的授权和批准清单

在这个测试计划中你还需要提供哪些信息来满足教学大纲中提到的最低要求？

a.对将要进行测试的人员进行必要的证书和培训的清单
b.一个时间表，显示设计，运行和评估安全性测试所需的时间
c.一份该系统必须满足的监管标准
d.在发生安全漏洞时，将进行测试的个人及其联系信息的列表

B根据教学大纲是正确的。可能需要A，但这不是最低要求之一，可能已在角色和责任部分中已经理解。C是不正确的，因为标准可能被引用但未包含在计划中。 D是不正确的，因为这个级别的细节不属于该计划，并且在违规期间不应该联系单个测试人员。

AS-3.3.1（K3）对于某个项目，基于特定的安全性测试方法以及已识别的功能和结构的安全风险，实现概念（抽象）安全性测试模型

AS-3.3.2（K3）实施测试用例来验证安全策略和过程。

问题＃13（2 分）

以下哪个测试用例最适合测试系统的安全程序？

a.三次不成功的登录尝试将生成锁定消息。请联系您的经理或系统管理员，以便他们通过电话提供临时密码。您必须在登录后更改临时密码。注销后使用新创建的密码重新登录。

b.几次尝试登录后，您会收到锁定消息。您可以致电 IT 支持以获取新密码。您使用临时密码登录，然后重新登录，然后再次登录并输入新密码。
C.经过几次尝试，您被锁定在系统之外。您使用之前有效的密码。但是，它不再有效。您尝试创建一个新密码，但您现在被锁定。完成机器的重新启动是下一步，让您进入提示重新输入密码。
d.在第一次尝试使用无效密码后，您立即在您的 PC 上的记事本上拉出一个密码列表，以确保您使用的密码正确。您尝试从列表中另一个密码，它的作品。

A 是正确的。由于“几次”这个词，B 和 C 不正确。 D 是不正确的，因为这肯定不是一个好的安全措施。

AS-3.4.1（K2）理解一个有效安全性测试环境的要素和特性
AS-3.6.1（K2）考虑到技术和威胁的演变性质，了解维护安全性测试过程的重要性

问题＃14（1 分）

以下哪一项是有效的安全性测试环境的主要特征？

a.与生产系统密切联系以提高所有点的安全性
b.隔离不同的旧版本的操作系统以供在环境中使用
c.根据访问权限模仿生产环境
d.包括所有生产环境插件以及不在生产环境中的其他插件，以确保最全面的设置

C 是正确的，因为测试环境越接近模拟生产，测试就越有效。在涉及访问权限和委派设置时尤其如此。 A 不正确，因为系统不需要，可能不应该连接。 B 可能是有用的，但不是主要特征。 D 是不正确的，因为它包含了不在生产中的插件，这可能会导致测试中的误报和漏报。

AS-3.4.2（K2）理解在执行任何安全性测试之前计划并获得批准的重要性

问题＃15（1 分）

寻求安全性测试工具的批准时，什么是重要的关注点？

a.有些国家禁止使用某些安全性测试工具
b.确保安全性测试工具的审批流程在恶意事件正在进行时可以有旁路绕过
c.在采购工具之前，工具的风险很少被发现，并且在工具被使用时更容易被发现
d.由于安全性测试工具风险通常是已知的，因此不需要缓解策略

A是正确的。虽然有些工具对测试非常有效且有效，但它们可能会被一些国家和一些组织所禁止。 B是不正确的，因为总是有部署次优工具来应对危机的危险。快速审批流程是有道理的，但完整的旁路是有风险的。 C和D是不正确的，因为工具可能存在未知风险，最好在工具选择中进行尽职调查，而不是处理选择不当的工具的后果。

AS-3.5.1（K4）分析安全性测试结果以确定以下内容：
•安全漏洞的性质
•安全漏洞的程度
•安全漏洞的潜在影响

•建议的补救措施
•最佳测试报告方法

问题＃16（3 分）

您正在审查一系列安全性测试结果，这些结果在发布到产品之前正在进行最终测试的产品上运行。这是当前正在生产的版本的更新。刚刚测试的应用程序是您的电子商务网站，它有一个允许跨站点脚本的缺陷。以下哪一项是您应该采取的适当步骤？

a.将问题报告给开发人员，将其添加到利益相关方报告中，并继续测试其他类型的缺陷
b.测试当前生产版本是否存在问题，在安全系统中记录缺陷，通知开发人员，继续测试其他XSS缺陷
c.通过对计划版本进行进一步测试并特别关注其他XSS版本，调查问题的严重程度，对代码进行静态分析
d.通知管理层，记录缺陷并将其包含在每周向状态报告的利益相关方报告中，继续测试其他安全缺陷以确定安全问题的程度

B是正确的。首要任务是查看生产版本中是否存在问题。由于问题可能存在于生产环境中，因此缺陷应仅记录在安全缺陷跟踪系统中。由于发现了一个XSS问题，因此可能有其他问题，因此需要继续进行测试。A不正确，因为缺陷不应在利益相关方报告中公布。 C不正确，因为在需要进一步测试时，通知至关重要。由于利益相关者报告，D不正确。

AS-4.1.1（K2）解释为何在生命周期过程中最能实现软件的安全性

问题＃17（1 分）

SDLC中的哪些地方应该进行检查，以确保遵循适当的安全编码实践？

a.组件测试
b.集成测试
c.系统测试
d.安全验收测试

A是正确的。代码写入后应尽快进行检查。

AS-4.1.2（K3）为给定的软件生命周期（例如，迭代、连续）实施适当的安全相关的活动

问题＃18（2 分）

业务分析师已经问过你，以帮助定义系统安全方面的要求。这是一个安全关键系统，可存储患者的医疗信息，并将这些信息提供给医院，医生办公室和救护车中的医疗专业人员。在生命周期的哪个阶段应该记录安全需求以及详细程度？

a.由于需要保护外部人员的代码中的安全实施，因此不应将其正式记录在案
b.在需求阶段，他们应该在需求文档中以详细且明确的方式记录
c.在代码方法已知的设计阶段，应该记录它们，而不是在方法未知的需求阶段
d.从用户的角度来看，它们应该仅限于功能访问和可用性要求，并且应在需求阶段记录

B是正确的。 A是不正确的，但重要的是要保护记录的要求免受不需要知道的人的保护。 C是不正确的，

因为尽管它们可以在设计层面进行细化，但它们应该在需求定义阶段初始捕获。 D是不正确的，因为安全需求还需要包含安全编码实践等。

AS-4.2.1（K4）从安全的角度分析一组给定的需求以识别它们的不足
AS-4.3.1（K4）从安全角度分析给定的设计文件，找出缺陷

问题＃19（3 分）

生产中发现缺陷。如果未经授权的用户复制来自授权用户的会话的URL，未经授权的用户可以将URL粘贴到自己的会话，并继续与授权用户的权限来处理。在报告的情况下，未经授权的用户可以使用授权用户的URL更改系统管理密码。为了弥补这种差距，开发人员将在任何时候使用URL来检查会话ID和用户ID。

以下哪项关于这个修复的表述是正确的？

a.它不会解决问题，会话劫持仍然是可能的
b.它会解决问题，但可用性可能受到不利影响
c.它会解决问题，但性能可能会受到不利影响
d.它不会解决问题，并会暴露一个会话ID的新漏洞

C是正确的。这种检查级别可能会降低系统速度，因为它必须检查每个屏幕更改。 A和D不正确，因为修复程序应该解决问题。 B不正确，因为不应该影响可用性（除非你是黑客！）。

AS-4.4.1（K2）了解在组件测试过程中安全性测试的作用。
AS-4.4.4（K2）了解组件集成测试期间安全性测试的作用。

问题＃20（1 分）

在组件级别测试期间，安全性测试人员为什么应该检查编译器警告？
a.因为这些表明必须解决的安全问题
b.因为这些表明应该调查的潜在问题
C.因为这些表明会导致功能缺陷的编码问题
d.因为这些表明不良的编程习惯会增加可维护性

B是正确的。从安全性测试的角度来看，编译器警告指出可能导致安全漏洞的潜在问题。A不正确，因为警告不一定需要修复。 C和D可能是真实的，但与安全性测试无关。

AS-4.4.2（K3）根据给定的代码规范实施组件级别的安全性测试（概要）
AS-4.4.5（K3）根据给定的系统规范实施组件集成的安全性测试（概要）

问题＃21（2 分）

您一直在测试有 20 个定义组件的系统。您已对每个组件进行了广泛的安全性测试。系统现在已准备好进入组件集成安全性测试。你应该如何处理这个测试？

a.由于组件集成测试涉及单个组件的漏洞总和，所以对集成组件进行相同的测试是最好的方法。
b.主要风险在于组件本身的集成，因此测试应覆盖每个接口并验证接口中没有漏洞，并且组件也应该重新测试。
C.集成组件以及现在可测试的更大的系统和基础架构可能存在新的漏洞，因此测试应该扩展到包含这些新的领域。
d.由于这些组件现在已经集成，所以安全风险将会降低，因为可能的交互作用现在受到限制，因此只需要测试集成点，并且不需要重新测试组件。

C是正确的。集成组件可能会出现新的漏洞，并且新的测试区域很可能会出现。A不正确，因为组件集成测试不是各个组件的总和。B不正确，因为测试不应仅限于接口和原始组件。D是不正确的，因为安全风险可能会增加，而不是减少。

AS-4.4.3（K4）对给定的组件级别的测试结果进行分析，从而从安全的角度判断代码的充分性。

问题＃22（3 分）

您正在创建安全性测试用例来检查输入字段上的 SQL 注入，该输入字段最多允许 5 个字母数字字符。您计划应用等价分区来减少您需要执行的测试用例的数量。鉴于这些信息，以下哪一项是您需要用来测试该字段的最小输入集合？

a.bbbbb，12345，'
b.%，'，@，ab123
C.'，ab123
d。“

C 是正确的，因为这有一个 SQL 注入测试，一个用于有效输入。这是最少的测试次数。 A 和 B 的最小数量多于 D，并且 D 没有足够的测试，因为它没有测试有效的输入。建议对可以支持 SQL 注入的各种角色进行更多测试，但这个问题是要求申请 EP 并获得最少数量的测试用例。

AS-4.5.1（K3）为安全性测试搭建一个端到端的测试场景，以验证一个或多个指定的安全需求以及测试一个已描述的功能过程。

AS-4.6.1（K3）基于指定的场景，实施端对端的安全再测试/回归测试方法。

问题＃23（2 分）

您已获得以下安全性测试要求。

用户将被允许请求他们的密码。如果他们提出这个请求，他们必须正确回答三个安全问题中的两个。如果他们回答正确，链接将被发送到他们的电子邮件。该链接将把他们带到可以重置密码的页面。重置后，他们可以使用新密码登录。链接必须在发送后 1 小时内禁用。用户只允许两个密码请求而不需要重置，之后他们将不得不打电话给服务台。对于任何其他错误，用户标识被锁定，必须由帮助台解锁。

以下哪项是测试条件的最低限度清单，以充分测试此要求涵盖的功能安全性？

a.无效的用户;有效的用户; 2 个正确答案; 2 个不正确答案;好电子邮件;坏的电子邮件用好的密码重置;用错误的密码重置;链接良好;链接过期;两个请求没有重置;三个请求没有重置

b.有效的用户; 2 个正确答案;好电子邮件;用好的密码重置;链接良好;两个请求没有重置
C.无效的用户; 2 个不正确答案;坏的电子邮件用错误的密码重置;链接过期;三个请求没有重置
d. 每个输入字段上的缓冲区溢出;每个输入字段上的 SQL 注入; XXS 登录页面并重置密码页面，无效的用户;有效的用户; 2 个正确答案; 2 个不正确答案;好电子邮件;坏的电子邮件用好的密码重置;用错误的密码重置;链接良好;链接过期;两个请求没有重置;三个请求没有重置

A 是正确的，因为它涵盖了需求中指定的功能安全性的主要方案。B 只在有效的测试中测试。C 只测试错误情况。D 扩展到攻击测试以及功能测试。

AS-4.5.2（K3）展示为一个指定的验收测试在安全性方面定义验收标准集的能力。

问题＃24（2 分）

用户将被允许请求他们的密码。如果他们提出这个请求，他们必须正确回答三个安全问题中的两个。如果他们回答正确，链接将被发送到他们的电子邮件地址。该链接将把他们带到可以重置密码的页面。重置后，他们可以使用新密码登录。该链接必须在发送后一小时内禁用。用户只允许两个密码请求而不需要重置，之后他将不得不打电话给服务台。对于任何其他错误，用户标识被锁定，必须由帮助台解锁。

以下哪一项是该要求的有效验收标准？

1.如果自上次重置后发出的请求少于三次，用户可以重置密码，并且两个安全问题得到正确回答，并且该链接用于重置，并在重置提示时输入有效密码。
2.超过两个请求会导致用户标识锁定。
3.没有重置的两个以上请求会导致用户标识锁定。
4.超过两个安全问题错过了结果。
5.错过了两个以上安全问题，用户 ID 被锁定。
6.如果系统收到电子邮件错误，用户 ID 将被锁定。
7.如果在重置时输入无效密码，则会提示用户使用适当的规则。
8.重置密码可用于登录系统。

a. 1，2，4，6，7，8
b.1，2，3，4，5，6，7，8
c. 3，5，6，7，8
d. 1，3，5，6，8

D 是正确的，因为它提供了基于需求的验收标准。 7 是诱人的，并且是合乎逻辑的，但在要求中没有规定。其他人不正确，因为他们不包含适当的标准。 2 不正确，其中 3 是正确的。 4 是不正确的，其中 5 是正确的。

AS-5.1.1（K2）理解系统加固的概念以及在增强安全性方面的作用
AS-5.1.2（K3）演示如何测试通用系统加固机制的有效性

问题＃25（2 分）

您正在实施评估系统加固的程序，以测试系统的安全有效性。你可以采取什么程序来确保实施的加固机

制按预期工作？

a.密切监视各种安全性能报告和指标，以确定是否实现了正确的访问和认证级别
b.经常审核强认证，以确保始终保持高水平的入侵保护
c.评估已经加固的硬件组件，并将其与其他加固软件组件进行比较，以确保实现均衡
d. 让一个已知的黑客进行加固效果的独立评估

A 是正确的。有可用的安全性能报告和指标可用于确定您是否已达到适当的加固级别。 B 不正确，因为强认证只是加固的一个方面。 C 不正确，因为不需要平衡。更重要的领域可能需要更好的加固。 D 是不正确的，因为黑客不会告诉你发现了什么。

AS-5.2.1（K2）理解身份验证与授权之间的关系，以及这两种技术在安全信息系统中是如何应用的。
AS-5.2.2（K3）演示如何测试通用身份验证和授权机制有效性

问题＃26（1 分）

中等复杂性 IT 系统的安全认证的关键属性是什么？

a. 它验证用户具有正确的配置文件和相应的权限来访问系统的有限部分
b. 确定用户可以使用的系统资源的数量是关键
c. 它验证进入系统的用户是否合法
d. 它使用用户之间的通用凭证来获得进入系统的权限

C 是正确的。它验证用户是否合法并经过授权。 A 不正确，因为它没有查看访问权限。 B 不正确，因为系统资源利用率不是一个考虑因素。 D 不正确，因为不应使用通用凭证验证 - 每个人都应拥有唯一的凭证。

AS-5.3.1（K2）理解加密的概念以及如何在安全信息系统中使用加密技术
AS-5.3.2（K3）演示如何测试通用加密机制的有效性

问题＃27（2 分）

典型的加密机制容易受到威胁，这使得在任何特定时间了解其有效性都很重要。确定您应该执行以下哪项措施以获得对加密机制的信心？

a.评估加密密钥以确保它们的大小至少为 256 位
b.确保您正在应用随机算法来尽可能生成随机数
c.开发确保在正确模式下使用对称加密的测试
d. 删除所有 WEP 协议以查看系统的性能

根据教学大纲 C 是正确的。 A 是不正确的，因为应该使用最少 768 位。 B 是不正确的，因为随机算法很容易破解。 D 是不正确的，因为 WEP 协议应该保留在原位而不是删除。

AS-5.4.1（K2）理解防火墙的定义以及网络区的使用，理解他们在安全信息系统中的应用
AS-5.4.2（K3）演示如何测试现有防火墙实施和网络区域的有效性

问题＃28（1 分）

防火墙和网络区域之间的关系如何？

a.网络区域和防火墙都关注正在传递的数据大小
b.网络区域通过安全协议选项进行通信，而防火墙确保这些协议安全
c.子网络可以被认为是网络区域，而防火墙可以是流量监控软件
d.网络区域阻止来自防火墙不过滤的不受信任区域的恶意流量

根据教学大纲 C 是正确的。 A 不正确，因为网络区域不关注数据的大小。 B 不正确。网络区域是防火墙配置的一部分，并定义网络之间授权的数据流。 D 不正确，因为防火墙阻止了流量，而不是网络区域。

AS-5.5.1（K2）理解入侵检测工具的概念以及它们如何应用于保护信息系统
AS-5.5.2（K3）演示如何测试已有的入侵检测工具实现的有效性

问题＃29（2 分）

您正在部署入侵检测工具的组织中工作。您担心流量正在流失，应被视为未经授权。您应该采用以下哪一项来最有效地测试入侵检测工具的功能，并提供更新入侵规范的输入？

a.根据过去的经验开发一系列场景
b.使用生成恶意流量的测试来添加新的入侵规范
c.将其应用于已知恶意流量的情况
d.尽可能将其与其他 IDS 产品结合使用

B 是正确的，因为这些测试可以用来添加以前被认为是授权流量的新入侵规范。 A 和 C 可能是有用的，但不会像 B 那样有效地确保该工具在未来以及现在都能发挥作用。 D 的用法是正确的，但不适用于测试。

AS-5.6.1（K2）理解恶意软件扫描工具的定义，以及他们如何在安全信息系统中应用的。
AS-5.6.2（K3）演示如何测试现有恶意软件扫描工具实施的有效性。

问题＃30（1 分）

以下哪项是恶意软件扫描工具的主要缺点？

a.他们只检测某些级别的恶意软件
b.他们只能检测该工具已知的恶意软件
C.他们往往过于复杂的运行
d. 他们不提供更新和报告功能

B是正确的。恶意软件工具只能检测到它已知的恶意软件。A可能是正确的取决于工具的特定焦点，但不是主要缺点。 C通常是不正确的 - 这些工具通常很容易运行。 D是不正确的，因为这些工具提供了用新发现来更新自己并产生报告的能力。

AS-5.7.1（K2）理解数据混淆工具的概念以及它们如何应用于保护信息系统
AS-5.7.2（K3）演示如何测试数据混淆方法的有效性

问题＃31（2 分）

您需要从遗留系统中删除个人识别号码，以降低测试过程中的风险。部分数据混淆计划包括验证数据如何被有效屏蔽。以下哪一项是最有效的使用方法？

a.在数据库中手动验证针对混淆的数据对于逻辑人类解释不再可以理解
b.设计对混淆数据的强力攻击
c.用不同字符串长度的随机数据替换敏感数据
d. 让开发团队创建一个程序来强调数据库的漏洞

B根据教学大纲是正确的。暴力或字典攻击可以用来查看个人信息是否仍然可以访问。 A是不正确的，因为它通常不可行，因为它会花费大量的数据和时间。 C是不正确的，因为这更像是一个匿名练习。此外，字段长度可能会受到限制，因此可能会破坏数据。 D是不正确的，因为我们没有试图强调测试数据库本身。

AS-5.8.1（K2）理解安全性培训作为软件生命周期一项活动的概念，以及为何在安全信息系统中需要安全性培训
AS-5.8.2（K3）演示如何测试安全培训的有效性

问题＃32（1 分）

什么通常被认为是软件安全中最薄弱的环节？

a.缺乏一致和全面的安全培训计划
b.维护文档和程序更新所需的努力，以跟上持续的安全威胁
c.人类的行为
d. 恶意技术的不断进步

C 是正确的。人类和他们的行为是最薄弱的环节。 A，B 和 D 是担忧，但 C 是安全链中最薄弱的环节。

AS-6.1.1（K2）解释人类行为如何导致安全风险，以及它如何影响安全性测试的有效性
AS-6.3.1（K2）了解安全意识对于整个组织的重要性

问题＃33（1 分）

以下哪项是潜在的安全风险？

a.在公司网站上发布会计部门的组织结构图
b.在 Facebook 上发布一位同事的生日祝福
C.在公司内部网上发布公司电话号码簿
d. 在 Linked In 配置文件中发布专业经验

A 是正确的。此信息可用于确定发票审批的审批链，如果会计系统可能被黑客入侵，则可用该审批链创建

和审批虚假发票。 B 不正确，因为出生日期不应用于任何员工信息，例如密码（我们希望！）。 C 不正确，因为公司内部网应该在防火墙后面加上其他受保护的信息。D 是不正确的，因为这个信息不可能对黑客有用。

AS-6.1.2（K3）在给定场景中，展示攻击者可用来发现特定目标的关键信息的方法以及可采取的环境防护措施

问题＃34（2 分）

您负责安全性测试贵公司的财务应用程序。您最近收到了一位声称已经使用 Shodan 入侵系统的人的电子邮件，并发现您在其中一台服务器上运行了过时且易受攻击的操作系统。你已经检查过并且黑客是正确的。您已确保服务器已更新。您的初步检查没有显示黑客如何进入您的系统。你应该担心吗？

a.不，这是一个“白帽子”的黑客，对你的公司没有任何坏处
b. 不，你已经修复了这个漏洞，所以系统现在是安全的
c.是的，你的安全性测试是不够的，你需要重新运行你的测试，看看错过了什么
d. 是的，因为黑客不承认他是如何进入系统的，他仍然可以访问它，并可能决定下次利用该漏洞

D 是正确的，那是你最关心的问题。A 不正确，可能是一个危险的假设。B 是不正确的，因为黑客仍然可以访问系统。 C 可能是真的，但重新运行相同的测试不会对这个问题有所帮助。

AS-6.1.3（K2）解释针对计算机系统的攻击的常见动机和来源
AS-6.2.1（K2）解释安全措施如何受到社会工程学的影响

问题＃35（1 分）

为什么来自组织内部的攻击特别令人担忧？

a. 攻击者很可能被好奇心所驱使，而且会毫不留情
b. 攻击者可能无聊工作，并会继续黑客娱乐系统
c. 攻击者已经在防火墙内并且是授权系统用户
d. 攻击者很可能会发起 DOS 攻击，从而使服务器瘫痪

C 是正确的。这里最大的威胁是外部保护是无用的，因为攻击者已经进入了系统。 A 和 B 更可能与外部攻击者发生。 D 不是最可能的攻击 - 通常内部用户是在他们可以出售或可以用来使公司无法获得的信息之后。

AS-6.1.4（K4）分析攻击场景（已发生和发现的攻击）并识别可能的来源和攻击

问题＃36（3 分）

您正在一个对服务器的系统管理访问受到高度限制的组织中工作。只有三位长期和值得信赖的员工知道 root 密码。但最近出现了一些奇怪的现象。发现一个名为“IKnowYourBirthday”的未知程序正在运行，并正在向工作人员发送生日祝福。出生日期是正确的，并且问候全部签名为“From your favorite server”。这个程序被中止了，没有人能够找出它的来源。第二个问题发生在公司电话列表被黑掉，所有电话号码被

更改为 867-5309（显然取自歌曲的同名）。虽然新文件是由“root”创建的，但正确的列表已被恢复，并且再次没有人能够弄清楚它是如何完成的。您刚刚收到主管系统管理员的电话，告诉您根密码已更改。已确定密码已设置为主管系统管理员的狗名。

进一步调查发现，在发现一系列受病毒感染的电子邮件后不久，问题就开始了。当发现第一个病毒时，立即采取保护措施以阻止病毒进一步传播，但现在您想知道是否有人设法通过病毒引入系统的代码进入系统。

作为下一步调查，你现在应该做什么？

a. 查看是否从系统外部访问 HR 出生日期信息，如果是，则跟踪 IP 地址
b. 验证领先系统管理员的狗名是否在社交媒体中发布
c. 检查发送的可疑电子邮件并尝试追踪 IP 地址
d. 检查另外两个系统管理员的人事档案，看看是否有迹象表明他们不满意

C 是正确的。这是最好的开始，因为看起来这可能是问题的起源。如果 C 没有找到任何东西，那么 A 和 D 将成为下一个可能的追求路径，因为这可能是内部攻击（D）或者攻击是分开的，并且生日信息可能提供关于谁已经靠近它。B 可能会被追求，但只要问系统管理员谁会知道狗的名字会更容易。

AS-6.3.2（K3）对特定的测试结果采取适当措施来提升安全意识

问题＃37（2 分）

在升级测试期间，您发现可能会创建一个中间人攻击，这可能会改变您在电子商务网站上向客户收取的金额。您的测试人员成功更改了金额，以便客户都可以享受 10％的折扣。你应该先做什么？

a. 应该阻止测试人员创建这些类型的攻击，因为它们在生产环境中不现实
b. 立即通知管理人员，如果发现攻击是由测试团队创建的，则作为测试的一部分
c. 与开发人员一起实施诸如SSL-trip之类的检查以确保证书是有效的而不是自签名的
d. 检查生产以查看该漏洞是否也在生产代码中

D是正确的。首要任务是查看是否存在漏洞，并立即解决问题。C应该是下一步，以确保开发人员编码正确，并使用所有可用的工具来检查此类问题。 A是不正确的，因为这正是安全性测试人员应该做的。B不正确，因为管理权限应始终在测试之前获得，而不是之后。

AS-7.1.1（K2）了解当项目的范围和目标发展时，需要修改安全预期和验收标准

问题＃38（1 分）

为什么重要的是频繁地重新评估安全风险预期？

a. 必须始终接受所有安全风险方面的教育
b. 利益相关者将基于相关的安全风险水平做出商业决策
c. 用户必须制定基于手动的风险缓解计划
d. 用户和利益相关者对安全性的期望应该保持不变

B是正确的。利益相关者通常必须就可接受的安全风险级别和任何必要的缓解计划做出商业决策。A不正

确，因为每个人都不需要知道一切。 C是不正确的，因为基于手动的风险缓解计划是不可行的，用户可能不会实现这一点。D是不正确的，因为期望值应该改变。

AS-7.2.1（K2）理解保证安全性测试结果保密和安全的重要性

AS-7.2.2（K2）了解是否需要创建适当的控制和数据收集机制，以及时，准确和精确地提供安全性测试状态报告的源数据（例如安全性测试仪表板）

问题＃39（1 分）

以下哪项是安全性测试结果的重要方面？

a. 它们被发布供用户和利益相关者访问，以帮助他们更好地理解风险
b. 他们应该与整个企业的开发人员共享，以减轻未来开发项目的风险
c. 知道更好的人越少
d. 结果应始终按照关键性分类

C是正确的。安全性测试的结果应该保密，并且应该严格控制对结果的访问。这是因为测试的结果经常识别当前被测系统中的弱点，并且通常与生产系统有相同的问题。 A是不正确的，因为需要严格控制对结果的访问。 B是不正确的，因为只有报告的有限部分应该被提供给开发者以改进他们的编码。同样，基础设施人员也应该使用有限的部件来解决可能发现的任何基础设施问题。D是真实的，但不是最重要的方面。

AS-7.2.3（K4）可以通过分析给定的中期安全性测试状态报告，从而决定准确性、可理解性和干系人适宜度的级别

问题＃40（3 分）

您正在为可准备部署到生产环境的项目最终确定安全性测试状态报告。由于系统的性质，这个项目存在高度的风险。因此，您要特别强调风险。基于此，在报告中阐述风险的最佳方式是什么？

a. 摘要中包含描述性风险评估
b. 报告最后部分包含整体风险
c. 风险影响在摘要中描述，稍后在具体漏洞方面进行详细描述
d. 风险影响不是报告摘要的一部分

C是正确的。风险影响应在摘要中进行描述，并在后面的报告中详细讨论具体的漏洞。 A不正确，因为细节不应包含在摘要中。 B不正确，因为这些信息不应只记录在报告末尾。 D不正确，因为这是报告的重要部分。

8.1.1（K2）解释静态和动态分析工具在安全性测试中的作用

问题＃41（1 分）

动态安全分析工具与通用动态分析工具有什么不同？

a. 安全工具探测系统而不仅仅是被测试的应用程序
b. 安全工具在动态或静态模式下工作相同
c. 安全工具更适合检测内存泄漏等问题
d. 安全工具需要根据应用程序实施的语言来定制

A是正确的。 B不正确，因为有动态和静态分析安全工具。 C不正确，因为通用动态分析工具检测到内存泄漏，而不是安全特定的内存泄漏。 D不正确，因为所有静态分析工具都是如此。

8.2.1（K4）分析和记录安全性测试需要通过一个或多个工具来解决

问题＃42（3 分）

你被赋予测试组织防火墙的工作。您已经查看了实施计划和步骤，确认已按照防火墙供应商的指示设置了配置并进行了端口扫描。你的组织特别担心拒绝服务（DOS）攻击，特别是当旧防火墙到位时他们曾遇到一次攻击。你应该进行哪种类型的测试来帮助检测可能被DOS攻击利用的意外行为？

a. 创建测试将发送畸形的网络数据包或模糊数据，并查看它们是否被防火墙检测到并拒绝
b. 实施自动化测试来压力测试服务器以测试故障转移功能
c. 测试加密和解密算法以确定它们是否足够快以处理DOS攻击的负载
d. 进行软件组件加固以确保尽可能减少攻击面

A是正确的，因为这两种技术都用于测试防火墙。B和C不正确，因为目标是防止攻击而不是让它通过防火墙。 D是不正确的，因为软件组件加固将帮助单个软件组件，而不是防火墙及其实施。

8.2.2（K2）理解开源工具的问题
8.2.3（K2）了解是否需要评估供应商频繁更新工具的能力，以便及时了解安全威胁

问题＃43（1 分）

如果您已经获得了GNU通用公共许可证下使用的工具，以下哪一项是工具维护的重要考虑因素？

a. 供应商的可靠性和提供支持的能力
b. 来自供应商的更新频率和可用性
c. 您团队的技术能力，以支持和定制适用于您的环境的工具
d. 许可成本和支持合同成本

C是正确的。 GNU许可证是免费的，它是一个开源社区，因此没有供应商。A和B不正确，因为没有供应商。D是不正确的，因为该工具是免费的，尽管您可能在为您的需求定制该工具时有开发成本。

9.1.1（K2）了解使用安全性测试标准的好处以及在哪里可以找到它们
9.3.1（K2）了解在哪里学习信息安全行业趋势

问题＃44（1 分）

以下哪一项符合安全性测试标准的好处？

a. 由于他们与项目目标和目标是分开的和独立的，因此他们一致且易于遵循
b. 它们是未来安全性测试的基石，无需从头开始
c. 他们概述了在进入系统之前应对威胁的有效进攻
d. 它们允许在安全实践中保持自由度，因为威胁总是动态变化的

B是正确的。
A是不正确的，因为项目目标可能会提到安全标准。 C不正确，因为它们本质上是防御性的。 D是不正确的，因为它们定义了一些有助于定义实践的标准 - 标准应该对威胁的变化作出响应。

9.1.2（K2）了解标准在监管与合同情况下的适用性差异
9.2.1（K2）理解任何标准中强制性（规范性）和可选（信息性）条款之间的区别

问题＃45（1 分）

在合同中施加安全标准有什么好处？

a. 当不可预见的安全问题对产品造成不利影响时，它向每一方提供合法退出
b. 提供一个起点双方开始谈判
c. 它们是公开各方之间协议的便捷方式
d. 即使合同最终确定，他们也可以随着标准的变化而改变

B 是正确的。通过定义安全标准，各方可以确定需要什么并进一步指定这些要求。 A 不正确，因为太晚了！ C 不正确，因为安全协议可能会保密。D 不正确，因为契约通常不会以这种方式变化。