模拟卷 – 答案
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

修订历史

版本	日期	备注
1.0 - Beta	2015/09/22	模拟题 Beta 版本
1.0 - GA 候选	2016/03/04	经考试工作组评审后更新 - 确定 #25 - #32 题的分数分布情况
1.0 - GA	2016/03/15	GA 版本

问题#1（1 分）

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。

问题#2（3 分）

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。

问题＃3（1 分）

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。

问题＃4（3 分）

B 是正确的。您应该分析安全性测试的结果，看看采取的安全策略和过程是否有效的。 A 是不正确的，因为如果有静态分析的话，分析应该在代码上。 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正在发生的威胁。

问题＃5（1 分）

根据教学大纲 A 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区域，但它不会支持该组织对法律行为的辩护。

问题＃6（1 分）

C 是正确的，安全性测试是更大的信息安全保证领域的一部分。

问题＃7（2 分）

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，而不是安全相关的（除非它将它们锁定，但我们从这个描述中无法得知）。 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。

问题#8 （2 分）

C 是正确的，在教学大纲里，目标被广泛的定义是一个常见的问题。A 和 D 是合理的关注点，但你不知道何时或如何定义测试目标，所以这可能是可控的。B 总是可能的，在这种情况下可能是正确的，但是还没有迹象表明会发生外包。

问题#9 （3 分）

D 是正确的。此时，组织需要一个向前发展的高水平的政策和计划。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。此时 A 和 C 不正确，但如果您在实施策略时难以获得资金，它们可能会有用。B 是不对的，因为在定义方法前你需要一个总体方针。

问题#10 （2 分）

C 是正确的。业务客户最关心的是防止欺诈访问他们易受攻击的数据。你希望 A，B 和 D 也会参与其中,但通常这不是他们的主要利益。

问题# 11（2 分）

B是正确的。使用概念测试创建手动测试和执行是实现安全性测试的一部分。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在测试执行后发生。

问题# 12（3 分）

B选项根据教学大纲是正确的。可能是必要的，但这并不是一个最低要求。这些内容在角色和职责章节可能已经理解。C是不正确的，因为可能引用不包括在这个计划里的标准。D是不正确的，因为这种级别的细节不在计划中，同时不应在违规期间联系单个测试人员。。

问题# 13（2 分）

A 是正确的。B 和 C 是不正确的，因为这个词“多次”。D 是不正确的，因为这绝对不会是一个好的安全实践。

问题＃14（1 分）

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。

问题＃15（1 分）

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，因为部署次优工具来应对危机总是危险的。快速审批流程是有意义的，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，而不是去处理由工具选择不当引起的后果。

问题＃16（3 分）

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。

问题＃17（1 分）

A 是正确的。代码写入后应尽快进行检查。

问题＃18（2 分）

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这些信息人的访问。 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。

问题＃19（3 分）

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的变更。 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！）。

问题＃20（1 分）

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。

问题＃21（2 分）

C是正确的。集成组件可能会出现新的漏洞，并且很可能会出现新的测试区域。 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。

问题＃22（3 分）

C是正确的，因为这有一个SQL注入测试，一个用于有效输入。这是测试次数的最小值。 A和B大于最小值，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注入的各种字符进行更多测试，但这个问题是要求申请EP并获得最少数量的测试用例。

问题＃23（2 分）

A是正确的，因为它涵盖了需求中描述的功能安全性的主要场景。 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。

问题＃24（2 分）

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。其他是不正确的，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。

问题＃25（2 分）

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

问题＃26（1 分）

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。

问题＃27（2 分）

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。

问题＃28（1 分）

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。

问题＃29（2 分）

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的侵入规范。 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。

问题＃30（1 分）

B是正确的。恶意软件工具只能检测到它已知的恶意软件。 B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。

问题＃31（2 分）

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。

问题＃32（1 分）

C 是正确的。这是人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。

问题＃33（1 分）

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。 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。

问题＃34（2 分）

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。

问题＃35（1 分）

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。

问题＃36（3 分）

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踪路径，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一些线索。 B可能会被追踪，但只要问系统管理员谁会知道狗的名字会更容易。

问题＃37（2 分）

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。

问题＃38（1 分）

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。

问题＃39（1 分）

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。这是因为测试结果经常识别出当前被测系统的弱点，并且通常与生产系统存在相同的问题。 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。

问题＃40（3 分）

C是正确的。风险影响应在总结中进行描述，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总结中。 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。

问题＃41（1 分）

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。

问题＃42（3 分）

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，因为软件组件强化将帮助单个软件组件，而不是防火墙及其实施。

问题＃43（1 分）

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。

问题＃44（1 分）

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。

问题＃45（1 分）

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，因为合同通常不会以这种方式变化。