模拟卷-问题
高级大纲

安全性测试

GA 版本 - 2016/03

国际软件测试资质认证委员会

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 - 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	经过稍微的改动后，发布了 GA 版本去除了学习目标的内容.

问题# 1（1 分）

以下哪些是安全审计的目的?
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. 阻止非法入侵者访问系统
d .要求用户在预设天数后更改密码

问题# 2（3 分）

你负责确保为项目从外部引入的新供应商完全符合政府规定的指导方针，作为您的风险评估的一部分。为确保这些外部供应商持续符合要求，你应该主要关注哪些利益相关方
a. 客户、用户和供应商，确保他们之间有良好的沟通
b .公众用户和遵守法律的供应商，因其适用于信息源
c .传达要遵守的指导方针的联邦和地方机构
d .将使用这些信息来进一步分析风险的内外部源

问题# 3（1 分）

将系统或设备的访问最大程度地降至可接受水平，下列哪些是该方针的后果？
a. 添加更多的设备以减轻影响
b .禁止对路由器等自配置设备进行适当的控制
c .从无线网络中删除不符合的设备
d .访问 VPN 受到严格限制

问题# 4（3 分）

作为安全管理员，你的角色是帮助您的组织了解整个企业安全策略和过程的有效性。你将在完成分析后向高级管理层报告关于有效性的结果。下面哪个是实现这一目标的最佳策略?
a. 针对策略和过程独立实施静态分析评估
b. 分析安全性测试结果以验证有效性
c. 针对当前威胁和攻击，评估安全性测试结果
d. 评估新的和正在出现的软件威胁的静态测试结果

问题# 5（1 分）

如果一个组织遇到安全漏洞和法律行动的结果,它是如何帮助组织完成安全性测试的?
a. 它可以表明该组织已实施尽职调查，以防止发生此类事件
b.安全性测试的文档可以用来追踪犯罪者
c.由于在安全性测试之前会备份所有重要的信息，可以使用该备份恢复任何受损信息
d. 通过追踪测试记录，安全性测试团队可以发现违规行为的可能性

问题# 6（1 分）
下面哪项是正确的陈述?
a. 信息安全是安全性测试的一部分
b.信息安全和安全性测试是同一事物的两个术语
c.安全性测试是信息安全的一部分
d. 这两个术语指的是安全的不同领域。

问题# 7（2 分）

您作为安全性测试团队的一员在银行工作。在最近的安全审计中，有人指出用户的密码强度不够。自那时起，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．确认密码长度满足要求
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时间内重新使用
5．确认密码每三个月必须重置
6．确认用户可以通过邮件获取他们的密码
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

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。虽然您同意需要采取措施，但您担心这种方法可能过度反应，并且可能无法带来所需的测试。

根据教学大纲，如果实施这些举措，合理的关切点是什么？

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，可能会忽略之前要避免产生的相同问题

问题#9（3 分）

您刚刚接受了一项工作，为某公司创建安全性测试团队，该公司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会导致意外暴露。以前做你工作的人带来过一些顾问来做测试，但是这些发现没有记录在案，也没有做任何改变。事实上，你甚至不知道测试的覆盖范围。您已将您的发现报告给执行管理团队。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了解需要完成的工作？

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，并演示这些策略如何符合您提出的测试方法

#10（2 分）

您刚刚参加了一个会议，会上讨论了组织的安全方法。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了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工作带来的好处？

a. 高级管理层
b. 合规性人员
c. 商业客户
d. 监管人员

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. 创造安全性测试条件和目标
b. 安全性测试实施
c. 安全性测试整体评估和报告
d. 安全性测试分析和设计

问题#12（3 分）

您一直在为系统制定安全性测试计划，该系统将存储患者医疗信息，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（范围内和范围外）
- 角色和任务
- 责任（供应商与内部）
- 概要时间表
- 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. 列出将要进行测试的人员所需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. 该系统必须满足的监管标准副本
d. 发生安全漏洞时将进行测试的个人及其联系信息的列表

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。退出后使用新创建的密码重新登录。
b. 您多次尝试登录后收到锁定消息。您致电 IT 支持以获取新密码。您使用临时密码登录，随后退出，然后再次登录并输入新密码。
c. 多次尝试后，您被锁定在系统外。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. 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。您尝试列表上的另一个密码，它是有效的。

问题#14（1 分）

以下哪一项是有效安全性测试环境的主要特征？
a. 与生产系统紧密联系以提高各方面的安全性
b. 隔离不同旧版本的操作系统以供在环境中使用
c. 在访问权限方面模拟生产环境
d. 纳入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

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.一些国家禁止使用某些安全性测试工具
b.确保恶意事件正在发生的情况下，安全性测试工具的审批流程可以以例外情况绕过
c.在采购工具之前，很少了解工具的风险，在使用工具时更容易发现
d.由于安全性测试工具的风险通常是已知的，因此不需要缓解策略

问题#16（3 分）

您正在审查某产品进行的一系列安全性测试结果，该产品正在进行其发布生产前的最终测试。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.向开发人员报告问题，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.通过对计划的发布进行进一步测试并特别关注其他XSS问题来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利益相关方报告的状态报告中，继续测试其他安全缺陷以确定安全问题的程度

问题#17（1 分）

在SDLC中的哪些环节应该进行检查，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

问题#18（2 分）

业务分析人员要求你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？记录的详细程度应如何？

a.需要保护来自外部的代码的安全实施，因此不应正式记录
b.在需求阶段，他们应该在需求文档中以详细和明确的方式记录
c.应该在代码方法已知的设计阶段记录，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上，并在需求阶段记录

问题#19 (3 分)

生产中发现缺陷。如果未经授权的用户复制授权用户的会话的URL，则未经授权的用户可以将URL粘贴到其会话中，并继续以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。为了修补这个漏洞，在URL被使用时，开发人员会检查会话ID和用户ID。

这个修复有什么现实意义？

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

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. 因为这些表明将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

问题#21 (2 分)

你在测试一个包含了 20 个已定义组件的系统，每个组件均已经过了全面的安全性测试，系统已经可以开始进入组件集成安全性测试阶段，你应该如何开展这项测试？

a. 由于组件集成测试涉及到各个组件中的漏洞，对集成的组件实施同样的测试是最好的方法。
b. 现在主要的风险在于各组件自身的集成，所以测试应覆盖每一个接口并验证接口不存在漏洞，各组件也应该被重新测试。
c. 很有可能新的漏洞存在于集成组件以及更大的系统和基础设施中，这些系统和基础设施现在是可测试的，因此测试应该扩展到包括这些新领域。
d. 由于组件现在已经集成，所以安全风险将会降低，因为可能的交互受到了限制。因此只有集成点应被测试，而组件无需重新测试。

问题 #22 (3 分)

您正在创建安全性测试用例，以检查输入域中的 SQL 注入，该字段最多允许输入 5 个字母数字字符，你计划应用等价类划分来减少需要执行的测试用例数，鉴于这些信息，以下哪一个是你需要用来测试该字段的最小输入集？

a. bbbbb, 12345, ‘
b. %, ‘, @, ab123
c. ‘, ab123
d. ‘

问题#23 (2 分)

你得到了如下的安全性测试需求。

允许用户申请获取他们的密码，如果他们提出此请求，他们必须正确回答三个安全问题中的两个。如果回答正确，一个链接将被发至他们的邮箱，通过此链接可到达重置密码的页面。一旦重置，他们就可以使用新密码登录。这个链接必须在发送后一小时后被禁用，用户在成功重置密码前只允许请求两次，此后他们必须联系服务台。对于任何其他错误，用户 ID 将被锁定且必须由服务台进行解锁。

以下哪项是最低限度测试条件清单，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；两个正确的答案；两个不正确的答案；正确的邮箱；不正确的邮箱；使用有效的密码重置；使用无效的密码重置；有效的重置链接；过期的重置链接；未重置前请求两次；未重置前请求三次。
b. 有效的用户；两个正确的答案；正确的邮箱；使用有效的密码重置；有效的重置链接；未重置前请求两次。
c. 无效的用户；两个不正确的答案；不正确的邮箱；使用无效的密码重置；过期的重置链接；未重置前请求三次。
d. 每个输入字段的缓冲区溢出；每个输入字段的 SQL 注入；登录页面和重置密码页面上的跨站脚本；无效的用户；有效的用户；两个正确的答案；两个不正确的答案；正确的邮箱；不正确的邮箱；使用有效的密码重置；使用无效的密码重置；有效的重置链接；过期的重置链接；未重置前请求两次；未重置前请求三次。

问题#24（2 分）

允许用户申请获取他们的密码，如果他们提出此请求，他们必须正确回答三个安全问题中的两个。如果回答正确，一个链接将被发至他们的邮箱，通过此链接可到达重置密码的页面。一旦重置，他们就可以使用新密码登录。这个链接必须在发送后一小时被禁用，用户在成功重置密码前只允许请求两次，此后他们必须联系服务台。对于任何其他错误，用户 ID 将被锁定且必须由服务台进行解锁。

以下哪项是该需求的有效验收标准？

1. 如果自上次重置以来请求次数少于三次且正确回答两个安全问题，则用户可以重置密码，使用重置链接来重置密码并在提示时输入有效密码。
2. 超过两次请求将锁定用户 ID。
3. 未重置前请求两次将锁定用户 ID。
4. 超过两个安全问题回答失败将导致错误。
5. 超过两个安全问题回答失败将导致用户 ID 锁定。
6. 如果系统收到邮箱错误，用户 ID 将被锁定。
7. 如果重置时用户输入了无效的密码，将得到合适的密码规则的提示。
8. 重置后的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

问题 25（2 分）

你正在执行评估系统强化情况的流程，以测试系统的安全有效性，若要确保所采用的强化机制按预期工作,以下哪个选项是你应当执行的流程?

a. 密切监视各种安全的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. 经常审计强认证以确保始终保持高水平的入侵防护
c. 评估进行了强化的硬件组件，并将其与进行了强化的软件组件进行比较以确保实现均衡
d. 由知名的黑客对强化效果进行独立评估

问题 26（1 分）

对于一个中等复杂的 IT 系统，以下哪个选项是其安全认证的关键属性？

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. 它使用了用户之间的通用凭证来获得进入系统的权限

问题 27（2 分）

典型的加密机制易受威胁，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. 评估秘钥以确保它们的大小至少是 256 位
b. 在可能的情况下，确保你使用了随机算法来生成随机数
c. 进行测试，以确保对称加密以正确的模式运用
d. 删除所有 WEP 协议以查看系统的性能

问题 #28 （1 分）

关于防火墙和网络区域的关系，以下哪个说法是正确的？

a. 网络区域和防火墙都关注所传输的数据大小
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. 一个子网络可被视为是网络区域，防火墙是可以监控流量的软件
d. 网络区域阻止了来自非信任区域且未经防火墙过滤的恶意流量

问题 29（2 分）

以下哪种方法能最有效地测试入侵检测工具的能力？

a. 基于过去的经验开发一系列场景
b. 使用生成恶意流量的测试，以增加新的入侵规范
c. 将其应用于已知的恶意流量的情境中
d. 可能的情况下，结合其他 IDS 产品使用

问题 30（1 分）

以下哪项是恶意软件扫描工具的主要缺点？

a. 它们仅检测某些级别的恶意软件
b. 它们仅检测工具已知的恶意软件
c. 过度复杂，不易运行
d. 没有更新和报告能力

问题 31（2 分）

你需要从遗留系统中删除个人识别号码以降低测试中的风险。你的数据混淆计划包括了验证数据掩蔽的有效程度。以下哪项是最有效的方法？

a. 在数据库中进行手工验证，以证明要混淆的目标数据对于人类的逻辑解释来说不可理解
b. 设计对混淆数据的强力攻击
c. 使用不同字符串长度的随机数据来替换敏感数据
d. 由开发团队开发一个程序，对数据库施以压力以暴露其漏洞

问题 32 （1 分）

下面哪个选项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，以便跟上持续发展的安全威胁
c. 人类的行为
d. 恶意技术的不断进步

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 上发布一个对同事的生日祝福
c. 在公司内网上公布公司电话目录
d.在 Linked In 的个人资料中公布工作经验

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，他并发现您在其中一台服务器上运行了过时且脆弱的操作系统。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，看看忽视了什么
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

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.攻击者可能会感到工作无聊，并继续黑客攻击系统进行娱乐
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

问题#36（3 分）

您正在一个对服务器的系统管理访问进行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“来自您最喜欢的服务器（From your favorite server）”。这个程序被封杀了，没有人能够找出它的来源。第二个问题是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的名字。

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.验证主管系统管理员的狗的名字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

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.万一被探测到，立即通知管理人员，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.检查生产系统以查看该漏洞是否也在生产代码中

问题#38 （1 分）

为什么频繁地重新评估安全风险预期是重要的？

a.利益相关者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.用户必须手动制定风险缓解计划
d.用户和利益相关者对安全性的期望应该保持不变

问题#39 （1 分）

以下哪项是安全性测试结果的一个重要方面？

a.它们发布给用户和利益相关方，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.越少人知道越好
d.结果应始终按照危急程度分类

问题#40 （3 分）

您正在为准备好部署到生产环境的项目确定最终的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。总结中描述的风险影响，稍后详细描述具体的漏洞
d。风险影响不是报告摘要的一部分

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诸如内存泄漏之类的问题
d.安全工具需要根据所实施的应用程序的语言来定制

问题#42 （3 分）

你被赋予测试组织防火墙的工作。您已经检查了实施计划和步骤，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，特别是当他们使用旧防火墙时发生过一次这样的攻击以后。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，发送畸形的网络数据包或模糊数据，查看它们是否被防火墙检测到并拒绝
b.实施自动化测试，对服务器施加测试以验证其故障切换能力
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.执行软件组件强化，以确保尽可能减少攻击面

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.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

问题#44 （1 分）

以下哪一项是符合安全性测试标准的好处？

a.由于他们与项目目标和目的是分开的和独立的，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.由于威胁总是动态变化，因此允许在安全实践中保持自由度

问题#45 （1分）

在合同中实施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.提供一个双方谈判起点
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