Exemplo de Exame - Perguntas

Conjunto de Exemplo de Exame – exame escrito
Versão Final

ISTQB ® Security Test Engineer Syllabus Specialist Level

Compatível com a versão 1.0.1 do Syllabus

International Software Testing Qualifications Board

Versão Final 2025-01-31

Aviso de direitos autorais

Responsabilidade pelo documento

O ISTQB® Examination Working Group é responsável por este documento.

Este documento é mantido por uma equipe central do ISTQB®, composta pelo Syllabus Working Group e pelo Exam Working Group.

Agradecimentos

Este documento foi produzido por uma equipe central do ISTQB®: Dr. Frank Simon (presidente), Alain Ribault, Gabriel Firmino Barjollo, Michael Pott, Beata Karpinska, Maria Kispal, Frans Dijkman

A equipe principal agradece à equipe de revisão do Exam Working Group, ao Syllabus Working Group e aos Conselhos Membros por suas sugestões e contribuições.

Histórico de revisões

Versão	Data	Observações
1.0	2024-09-10	Versão final para aprovação da GA
1.0.1	2015-01-31	Versão final após revisão EWG

Histórico da versão de tradução do BSTQB

Data	Observações
07/03/2025	Lançamento da versão na língua portuguesa

Índice

Introdução

Objetivo deste documento

Os exemplos de perguntas e respostas e as justificativas associadas neste exemplo de exame foram criados por uma equipe de especialistas no assunto e redatores de perguntas experientes com o objetivo de:

- Auxiliar os Conselhos de Membros e os Conselhos de Exames do ISTQB® em suas atividades de elaboração de perguntas.
- Fornecer aos provedores de treinamento e candidatos um exemplo de perguntas de exames.

Essas perguntas não podem ser usadas como estão em nenhum exame oficial.

Observe que os exames reais podem incluir uma grande variedade de perguntas, e este exemplo de exame ***não tem*** a intenção de incluir exemplos de todos os tipos, estilos ou durações possíveis de perguntas.

Instruções

Neste documento, você pode encontrar:

- Perguntas[1] , inclusive para cada pergunta:
  - Qualquer cenário necessário para apoiar a pergunta
  - Pontuação da questão
- Conjunto de opções de respostas
- Perguntas adicionais, inclusive para cada pergunta [não se aplica a todos os exemplos de exame]:
  - Qualquer cenário necessário para apoiar a pergunta
  - Pontuação da questão
- Conjunto de opções de resposta
- As respostas, incluindo a justificativa, estão contidas em um documento separado

[1] Neste exemplo de exame, as perguntas são classificadas pelo LO (Objetivo de Aprendizagem) a que se destinam; isso não deve ser esperado em um exame real.

Perguntas

Questão 1 (1 ponto)

Qual das opções a seguir descreve MELHOR o nível de segurança dos ativos em relação à integridade?

A) Somente usuários autenticados devem ter acesso para modificar arquivos e aplicativos.
B) Somente os proprietários de arquivos podem ter acesso para modificar dados para estabelecer a integridade adequada.
C) O histórico de registros de tentativas não autorizadas deve ser mantido por dois anos.
D) Estabeleça um processo que permita aos usuários acessar dados inalterados sempre que precisarem.

Selecione UMA opção.

Questão 2 (1 ponto)

Qual das alternativas a seguir é uma alternativa adequada para descrever como os testes de segurança podem confirmar que a confidencialidade das informações confidenciais tem as devidas proteções?

A) Verifica a existência de controles adequados para impedir o acesso não autorizado a informações confidenciais.
B) Verifica se há controles adequados que garantam que somente atualizações autorizadas possam ser feitas e que todos os dados permaneçam confiáveis.
C) Verifica os mecanismos de recuperação rápida para restaurar os serviços imediatamente após um incidente.
D) Verifica se a resposta da organização aos incidentes é eficaz, minimizando os danos e o tempo de inatividade.

Selecione UMA opção.

Questão 3 (1 ponto)

Qual das opções a seguir descreve MELHOR uma auditoria de segurança?

A) Uma avaliação sistemática dos testes de segurança e da estratégia geral de segurança em toda a organização.
B) Uma avaliação sistemática da segurança do sistema de informações, medindo o grau de conformidade com um conjunto estabelecido de critérios.
C) Uma avaliação sistemática com o objetivo de impedir o acesso de intrusos não autorizados ao sistema.
D) Uma avaliação sistemática com o objetivo de reduzir os riscos por meio da identificação de hardware e software sujeitos a vulnerabilidade.

Selecione UMA opção.

Questão 4 (1 ponto)

Qual das opções a seguir descreve o Zero Trust?

A) Qualquer usuário precisa de verificação contínua de identidade, independentemente de sua localização.
B) Qualquer dispositivo e usuário com acesso ao sistema é confiável por padrão.
C) Somente os dispositivos da rede confiável têm acesso aos sistemas.
D) Todos os usuários recebem o nível de acesso de que precisam.

Selecione UMA opção.

Questão 5 (1 ponto)

Quais dos itens a seguir você incluiria para verificar se o conceito de Zero Trust foi implementado corretamente?

A) Implemente controles que verifiquem cada solicitação de acesso individual a qualquer recurso confidencial.
B) As solicitações de acesso iniciadas por contas de serviço não humanas são sempre confiáveis.
C) Verifique se os registros de acesso produzidos pelo sistema fornecem um registro permanente e com carimbo de data e hora de todas as atividades.
D) Implemente conjuntos de permissões padrão com base nas funções e responsabilidades dos usuários.
E) Concentre-se em controles de acesso à rede externa em vez de controles a aplicativos, recursos, dados e ativos específicos.

Selecione DUAS opções.

Questão 6 (1 ponto)

Ao usar software de código aberto, qual dos fatores a seguir NÃO é um fator crítico a ser considerado ao tratar de questões de segurança?

A) Alinhamento com o OWASP e auditorias de segurança ativas pelos colaboradores.
B) Frequência e disponibilidade de patches e atualizações de segurança.
C) A capacidade da sua equipe de gerenciar e personalizar a ferramenta para o seu ambiente.
D) Requisitos de licenciamento e conformidade com as diretrizes de segurança de código aberto.

Selecione UMA opção.

Questão 7 (1 ponto)

Um banco subcontratou o desenvolvimento de novos recursos para seu portal de clientes, a fim de melhorar a experiência do usuário. O desenvolvimento dos recursos está concluído e foi entregue ao banco. O banco solicita que você planeje e execute testes de segurança em um ambiente de pré-produção antes da implementação.

Qual das opções a seguir descreve melhor como você abordaria essa tarefa?

A) Executar testes caixa-branca para cobrir todo o código-fonte e ter certeza de que não há mais defeitos antes da implementação.
B) Executar a varredura de vulnerabilidade de caixa-cinza para garantir que todas as vulnerabilidades conhecidas no escopo do projeto, potencialmente exploráveis por um invasor, sejam ou venham a ser identificadas.
C) Executar testes de injeção de falhas em caixa-preta para encontrar possíveis pontos de entrada vulneráveis.
D) Verificar se as regras de codificação de segurança foram aplicadas usando uma ferramenta de teste de segurança estática de aplicativos.
E) Verificar se as vulnerabilidades detectadas pelo teste de caixa-branca podem ser exploradas.

Selecione DUAS opções.

Questão 8 (1 ponto)

Como engenheiro de teste de segurança do projeto, você tem a tarefa de definir as técnicas de teste de segurança que devem ser aplicadas como teste de segurança estático.

Qual seria sua abordagem?

A) Verificar se as regras de codificação de segurança são aplicadas pelos desenvolvedores, verificar se o projeto seguiu as práticas recomendadas de "segurança por projeto" e, em seguida, verificar se os requisitos de segurança estão completos.
B) Verificar se as regras de codificação são aplicadas pelos desenvolvedores e, em seguida, criar o aplicativo e executar algumas injeções de SQL para verificar se os campos de entrada estão corretamente protegidos contra injeção de SQL.
C) Verificar se os requisitos de segurança estão completos, verificar se o design seguiu as práticas recomendadas de "segurança por design" e, em seguida, verificar se os desenvolvedores aplicam as regras de codificação de segurança.
D) Verificar se o conjunto de requisitos de segurança é pertinente e completo e, em seguida, executar o teste de valor limite no aplicativo criado para verificar se os estouros de buffer são evitados com a aplicação de regras de codificação de segurança dedicadas.

Selecione UMA opção.

Questão 9 (1 ponto)

Você recebeu o seguinte requisito para o teste de segurança:

O usuário poderá solicitar a redefinição da senha. Se ele fizer essa solicitação, deverá responder corretamente a duas de suas três perguntas de segurança. Se a resposta for correta, um link será enviado ao e-mail do usuário. O link o levará a uma página na qual ele poderá redefinir sua senha. Depois de redefinida, o usuário poderá fazer login com a nova senha. Esse link deve se tornar inválido uma hora após ter sido enviado ou se o usuário emitir outra solicitação de redefinição de senha. Se o usuário enviar mais de duas solicitações de redefinição de senha sem concluir a redefinição, a ID de usuário será bloqueada. Para desbloquear a ID, o usuário deve entrar em contato com o helpdesk.

Qual das opções a seguir é a lista mínima de condições de teste para testar adequadamente a segurança funcional coberta por esse requisito?

A) Usuário inválido; usuário válido; 2 respostas corretas; 2 respostas incorretas; redefinição completa da senha; link válido; link expirado; duas solicitações sem redefinição; 3 solicitações sem redefinição.
B) Usuário válido; usuário válido; 2 respostas corretas; 3 respostas corretas; redefinição completa da senha; link válido; duas solicitações sem redefinição.
C) Usuário inválido; usuário inválido; 2 respostas incorretas; link expirado; 3 solicitações sem redefinição; caracteres inválidos.
D) Usuário inválido; usuário válido; usuário inválido; usuário válido; 2 respostas corretas; 2 respostas incorretas; estouro de buffer em cada campo de entrada; injeções de SQL.

Selecione UMA opção.

Questão 10 (1 ponto)

Em sua organização, você é responsável pelo Gerenciamento de Identificação e Acesso para gerenciar e manter as contas e os direitos dos usuários. Nos últimos dois meses, houve dois recém-chegados e uma pessoa da empresa mudou de departamento. Seus perfis foram atribuídos a suas novas funções e direitos. Que técnicas de teste de segurança você deve planejar com base na sua responsabilidade?

A) Nenhum teste é necessário porque as contas e os direitos foram gerenciados.
B) Revise as permissões de funções da pessoa que mudou o departamento.
C) Teste as funções e os privilégios atribuídos aos recém-chegados para garantir que estejam configurados corretamente.
D) Nenhum teste é necessário porque os recém-chegados têm funções e privilégios básicos e a pessoa que mudou de departamento tem menos privilégios do que antes.
E) Depois de aplicar as alterações, verifique se o acesso a novos aplicativos está funcionando.

Selecione DUAS opções.

Questão 11 (1 ponto)

Qual das opções a seguir descreve CORRETAMENTE as técnicas de teste de segurança para o mecanismo de autenticação?

A) Examinar se os usuários podem gerenciar os recursos do sistema com base em suas funções.
B) Verificação dos detalhes de login definidos na fábrica e avaliação dos requisitos de força da senha.
C) Verificação dos níveis de permissão do usuário por meio da análise de perfil.
D) Monitoramento dos registros de atividades do usuário durante o processo de login.

Selecione UMA opção.

Questão 12 (1 ponto)

Qual das seguintes afirmações descreve MELHOR como testar os controles de proteção de dados?

A) Os testes devem avaliar as medidas de segurança verificando a conformidade da criptografia, dos controles de acesso e dos recursos de mascaramento de dados.
B) Os testes devem medir exclusivamente a rapidez e a eficiência com que as medidas de proteção operam no sistema.
C) Os testes devem examinar como os usuários interagem com os recursos de segurança por meio dos elementos e controles da tela.
D) Os testes devem analisar o desempenho dos sistemas de armazenamento de dados quando os recursos de segurança estão ativos.

Selecione UMA opção.

Questão 13 (1 ponto)

Pedimos que você explique os procedimentos para avaliar a proteção do sistema como um exemplo típico de tecnologia de proteção. Que procedimento você poderia seguir para garantir que os mecanismos de proteção implementados estejam funcionando conforme o esperado?

A) Monitorar de perto vários relatórios e métricas de desempenho de segurança para determinar se o nível correto de acesso e autenticação foi alcançado, ou seja, se não é muito restritivo nem muito amplo.
B) Auditar com frequência a autenticação forte para garantir que um alto nível de proteção contra intrusões seja mantido o tempo todo.
C) Avaliar os componentes de hardware que foram protegidos e compará-los com outros componentes de software protegidos para garantir que um equilíbrio esteja sendo alcançado.
D) Contratar um hacker conhecido para realizar uma avaliação independente da eficácia da proteção.

Selecione UMA opção.

Questão 14 (1 ponto)

Você é responsável por todos os aspectos do processo de segurança, inclusive os testes. Para essa tarefa específica, você deve usar testes de alto nível como base para testes manuais e executá-los a partir da perspectiva de um fornecedor externo. Que tarefa de teste de segurança pode ser realizada paralelamente a essa?

A) Criação de condições e objetivos de teste para o teste de segurança.
B) Implementação de testes de segurança.
C) Avaliação geral e relatórios de testes de segurança.
D) Análise e projeto de testes de segurança.

Selecione UMA opção.

Questão 15 (1 ponto)

Qual das características a seguir é a principal de um ambiente de teste de segurança eficaz?

A) Estreitamente ligado aos sistemas de produção para aumentar a segurança em todos os pontos.
B) Isola diferentes versões antigas dos sistemas operacionais para uso no ambiente.
C) Imita o ambiente de produção em termos de direitos de acesso.
D) Inclui todos os plug-ins do ambiente de produção, bem como outros plug-ins que não estão no ambiente de produção, para garantir a configuração mais abrangente.

Selecione UMA opção.

Questão 16 (1 ponto)

Durante o teste de componentes, qual aviso do compilador mais acionaria o testador de segurança?

A) Aqueles que indicam problemas de segurança que devem ser corrigidos
B) Aqueles que indicam possíveis problemas que devem ser investigados
C) Aqueles que indicam problemas de codificação que causarão defeitos de adequação funcional
D) Aqueles que indicam práticas de programação ruins que aumentarão a capacidade de manutenção

Selecione UMA opção.

Questão 17 (1 ponto)

Dada a seguinte especificação de design: O componente A e o componente B se comunicam por meio de uma API REST. Qual das opções a seguir é um exemplo de teste de segurança realizado no nível de integração do componente?

A) Testar a criptografia de dados durante as chamadas de API entre os componentes A e B
B) Testar se o componente A pode chamar a API do componente B
C) Testar se os componentes externos são de fornecedores confiáveis.
D) Testar o tempo de resposta entre os componentes A e B.

Selecionar UMA opção

Questão 18 (1 ponto)

Qual das alternativas a seguir descreve MELHOR o procedimento correto para a implementação de testes de segurança de ponta a ponta para testar o tratamento do sistema de tentativas de login malsucedidas?

A) Antes da execução do teste, prepare um gerador de gerenciador de senhas para alterar a senha ao fazer o login. Você faz logout e, em seguida, faz login usando a senha recém-criada. Três tentativas de login sem sucesso gerarão uma mensagem de bloqueio.
B) Após várias tentativas de login, você recebe uma mensagem de bloqueio e liga para o Service Desk para obter uma senha temporária pelo correio. Você faz login com a senha temporária, faz logout, faz login novamente e digita uma nova senha.
C) Depois de tentar fazer login várias vezes sem sucesso, você pressiona o botão para obter um link para alterar a senha. Depois de obter o link, você reutiliza a senha antiga. O sistema aceita a senha.
D) Após a primeira tentativa de usar uma senha inválida, você abre uma lista de senhas no bloco de notas do PC para garantir que está usando a senha correta. Você tenta outra senha da lista e ela funciona.

Selecione UMA opção.

Questão 19 (1 ponto)

Você está trabalhando como gerente de testes em um banco que está desenvolvendo um novo aplicativo bancário on-line. O aplicativo manipulará dados confidenciais de clientes e transações financeiras. Você foi solicitado a realizar testes de segurança para esse novo aplicativo. Não há requisitos explícitos, portanto, você seleciona seus próprios casos de teste a partir de padrões e práticas recomendadas.

Quais são as três (3) afirmações a seguir que melhor o orientam na seleção de casos de teste?

i. As normas são entradas válidas, pois são aprovadas por um órgão de conhecimento reconhecido
ii. Os padrões podem ser classificados em padrões do setor, padrões de fato e padrões específicos do fabricante. Os padrões do setor e os de fato são entradas válidas, mas os padrões do fabricante podem não se adequar a um contexto específico
iii. Como os padrões são obrigatórios, elas são entradas válidas, pois devem ser aplicados em todos os ambientes
iv. As práticas recomendadas não são uma entrada válida, pois geralmente são de nível muito alto
v. Os padrões de fato são bons insumos, pois geralmente têm suas raízes nos padrões do setor

A) i, ii e v
B) i, ii e iii
C) ii, iii e v
D) iii, iv e v

Selecione UMA opção.

Questão 20 (1 ponto)

Uma nova empresa iniciante do setor bancário desenvolveu um novo sistema central. Até o momento, a equipe de desenvolvimento concentrou-se na boa usabilidade e no excelente desempenho. Antes de entrar em operação, a diretoria executiva deseja obter uma visão independente sobre o nível de segurança. Eles estão pedindo que você, como testador de segurança, faça um teste de caixa-preta. A tarefa é testar as vulnerabilidades mais críticas que poderiam ser exploradas pelo novo aplicativo bancário.

Se você deseja realizar esse trabalho, como pode aproveitar os padrões para sua tarefa?

A) Você seleciona os pontos fracos relevantes no padrão CWEs e executa os casos de teste listados.
B) Você seleciona os pontos fracos relevantes no CWE, escolhe os exploits disponíveis para os CWEs selecionados e os aplica
C) Você seleciona os pontos fracos relevantes no CWE, prioriza os CWEs selecionados com base no padrão CWSS e seleciona os CVEs relevantes que abrangem o CWE priorizado
D) Você seleciona os pontos fracos relevantes no CWE, prioriza os CWEs selecionados com base no padrão CVSS e deriva casos de teste individuais relacionados ao CVSS
E) Para cada CVE selecionado, você deriva casos de teste para o aplicativo bancário e os executa

Selecione DUAS opções

Questão 21 (1 ponto)

Quando você usa oráculos de teste para um aplicativo de padrões e práticas recomendadas, o que deve considerar?

A) Esses oráculos de teste são válidos independentemente de quaisquer parâmetros do aplicativo
B) Esses oráculos de teste só podem ser usados como dicas difusas para testes de segurança
C) Esses oráculos de teste não podem ser usados para testes de segurança
D) Quanto menos específico for um aplicativo e seu contexto, mais eficiente será a reutilização desse teste

Escolha UMA opção.

Questão 22 (1 ponto)

As práticas recomendadas e os padrões fornecem muitos artefatos, que podem ser usados de forma eficaz para testes de segurança. Quais combinações de artefatos e mapas de atividades estão corretas?

1. Nomenclatura consistente
2. Conhecimento especializado
3. Benchmarking
4. Visão geral da segurança holística

que pode ser usado para:

A. comunicação mais fácil
B. reutilização do conhecimento de especialistas em segurança para testes de segurança
C. verificar novamente a integridade das atividades de teste de segurança
D. Demonstrar facilmente a eficácia das atividades de teste de segurança aplicadas

A) 1-A, 2-B, 3-D, 4-C
B) 1-A, 2-B, 3-C, 4-D
C) 1-D, 2-A, 3-B, 4-C
D) 1-B, 2-D, 3-A, 4-C

Escolha UMA opção.

Questão 23 (1 ponto)

Você foi contratado como testador de segurança pela gerência de uma empresa de engenharia de médio porte que produz diferentes peças para automóveis e depende muito de seus fornecedores, pois o preço das matérias-primas afeta diretamente o lucro. A empresa tem apenas um site público e um domínio de e-mail conhecido, mas não oferece outros serviços da Web. Sua tarefa é obter acesso ao ambiente de produção interno, que consiste em várias instalações industriais modernas, e comprometer pelo menos um sistema.

Quais são as DUAS opções que melhor apresentam como você poderia aproveitar o contexto organizacional?

A) Infiltrar-se em um dos fornecedores mais usados para se aproximar da empresa-alvo real
B) Realizar um ataque de engenharia social fingindo ser um fornecedor existente ou um novo fornecedor em potencial e tentar saber mais sobre o alvo, por exemplo, visitando-o e solicitando uma breve visualização
C) Identificar o endereço de e-mail do departamento de contabilidade e enviar faturas falsas com conteúdo malicioso, por exemplo, para obter acesso remoto por meio de um shell reverso
D) Espalhe pen drives USB pelo prédio da empresa e espere até que alguém pegue um pen drive e o conecte.
E) Faça uma força bruta contra o login SSH do servidor da Web

Escolha DUAS opções.

Questão 24 (1 ponto)

Sua empresa desenvolve diferentes produtos para o setor de aviação. No início do ano, foi anunciado um novo produto. Pela primeira vez, ele será um dispositivo de comunicação. Seu trabalho é realizar testes de segurança do novo produto antes que ele seja lançado no mercado.

Qual dos aspectos a seguir descreve MELHOR o que você deve considerar?

A) O setor de aviação é um setor regulamentado; portanto, o novo produto e todo o processo de desenvolvimento devem estar em conformidade com as normas vigentes
B) Alguns países têm seus próprios regulamentos sobre antenas de rádio e padrões usados. O produto deve funcionar corretamente, mesmo que algumas frequências possam interferir com as frequências usadas pelo produto
C) Os testes de segurança precisam ser executados muito rapidamente, pois o produto deve ser lançado o mais rápido possível
D) Os funcionários precisam comprovar seu conhecimento sobre radiocomunicação por meio de certificações pessoais

Escolha UMA opção.

Questão 25 (2 pontos)

Durante o teste de segurança de um sistema principal, você encontra vários arquivos suspeitos que não foram criados por você ou por outros testadores durante o teste nem usados pelos aplicativos em execução nesse sistema.

Escolha a opção MELHOR que descreve como você procederia

A) Continue o teste de segurança e relate suas descobertas depois de concluir todas as atividades de teste
B) Pause o teste de segurança e escreva um e-mail global informativo pelo menos para todos os colegas que têm acesso ao sistema. Continue, se ninguém tiver uma contestação.
C) Interrompa o teste de segurança e desligue o sistema imediatamente, pois houve um acesso não autorizado e é necessário evitar outros possíveis danos
D) Interrompa o teste de segurança e siga as etapas definidas pela política de segurança da empresa para relatar um incidente. Se não houver uma política para a comunicação de incidentes, informe à pessoa responsável (por exemplo, diretor de segurança de TI, CISO...)
E) Interromper o teste de segurança e iniciar as investigações e seguir as etapas definidas pela política de segurança da empresa para investigação

Escolha UMA opção

Questão 26 (2 pontos)

Cada ataque é diferente. No entanto, algumas etapas são comuns a quase todos os ataques. Essas etapas podem ser definidas como

A) Etapa de coleta de informações, seguida de exploração/ganho de acesso e, no final, persistência/manutenção do acesso.
B) Engenharia social, seguida de ataque de força bruta e, no final, persistência/manutenção do acesso
C) Exploração/ganho de acesso seguido de engenharia social para entender os resultados e, no final, limpar os rastros
D) Coleta de informações, seguida de limpeza de rastros e, no final, engenharia social para obter uma melhor linha de base.

Escolha UMA opção

Questão 27 (1 ponto)

Qual das seguintes afirmações descreve MELHOR como os testes de segurança devem ser implementados no ciclo de vida do desenvolvimento?

A) Cada atividade de desenvolvimento deve ter uma atividade de teste de segurança correspondente
B) Com a realização de uma análise de ameaças e um projeto de segurança adequados, a maioria das vulnerabilidades pode ser encontrada
C) O SAST e o DAST devem ser executados em todas as fases do ciclo de vida do desenvolvimento de software
D) Os testes de segurança devem ser realizados durante todas as fases do ciclo de vida do desenvolvimento do software para manter a sincronia com os testes funcionais manuais

Escolha UMA opção.

Questão 28 (2 pontos)

Qual das DUAS afirmações a seguir descreve MELHOR o impacto de um modelo de desenvolvimento de software nos testes de segurança?

A) A equipe pode envolver uma equipe de habilitação de segurança para realizar o teste de segurança em cada modelo
B) O modelo em cascata é o que melhor suporta testes de segurança durante o ciclo de vida de desenvolvimento de software
C) O DevOps pode oferecer um suporte melhor para que os testes de segurança sejam realizados durante as operações
D) É mais fácil realizar testes de segurança usando o Kanban em comparação com o Scrum
E) Os testes de segurança podem ser mais bem planejados usando os modelos de desenvolvimento de software Agile em comparação com o modelo Waterfall

Escolha DUAS opções.

Questão 29 (1 ponto)

Qual das quatro afirmações a seguir é verdadeira para os testes de segurança no contexto dos testes de manutenção?

A) Concentrar-se em confirmar a satisfação de todos os requisitos de segurança após a mudança
B) Executar o conjunto de regressão existente em relação a funções individuais para verificar se a alteração funciona
C) Teste de novas vulnerabilidades que possam ter sido introduzidas pela alteração.
D) Execução de testes de segurança de confirmação e regressão após a realização de uma alteração

Escolha UMA opção.

Questão 30 (1 ponto)

Qual das opções a seguir descreve MELHOR por que você deve analisar os resultados dos testes de segurança?

A) Compreender ameaças e riscos de segurança específicos com base em avaliações de segurança, auditorias e fontes padrão de vulnerabilidades conhecidas
B) Traduzir testes conceituais em testes que possam ser executados manualmente ou com ferramentas
C) Definir um escopo apropriado de testes que corresponda aos riscos de segurança.
D) Levar as atividades de teste de segurança a um ponto de encerramento, de modo que os testes possam ser mantidos e realizados regularmente para dar suporte a quaisquer novos requisitos de segurança e/ou detectar novas ameaças

Escolha UMA opção.

Questão 31 (1 ponto)

Você é responsável pela segurança do sistema. Alguém da sua equipe está interessado em testes de segurança e faz um teste de penetração no seu sistema, que inclui as 10 principais vulnerabilidades do OWASP. O relatório de teste correspondente consiste apenas em casos de teste bem-sucedidos e com falha que abrangem essas vulnerabilidades. Qual raciocínio sobre a aceitação ou rejeição do relatório de teste está correto?

A) Aceitar, pois o teste de penetração foi feito por um colega interno que conhece os guias de estilo de segurança específicos.
B) Rejeitar, pois seus critérios de aceitação de segurança não foram comunicados e não são considerados no relatório de teste. Portanto, não está claro se as técnicas de teste correspondentes foram usadas e se os resultados do teste são relevantes para sua verificação anual de conformidade com o guia de estilo de segurança.
C) Aceitar, pois a OWASP é uma prática recomendada e define uma lista geral de critérios de aceitação
D) Rejeitar, porque um guia de estilo de código de segurança deve ser testado por abordagens de teste de caixa-branca, não por pentests dinâmicos de caixa-preta.
E) Aceitar, pois a OWASP reflete seu guia de estilo de código de segurança.

Escolha DUAS opções.

Questão 32 (1 ponto)

Para aproveitar os testes de segurança no mais alto nível de eficiência e eficácia, é necessário:

A) Integrá-lo a um processo geral de segurança, que tenta minimizar os riscos e garantir a continuidade dos negócios.
B) Aplicá-lo anualmente a todos os sistemas de TI usados
C) Usá-lo para limitar proativamente o impacto de uma violação de segurança
D) Considerar as vulnerabilidades comunicadas no dia a dia.
E) Garantir que todas as vulnerabilidades identificadas sejam corrigidas dentro de um prazo apropriado menor que 6 meses

Escolha DUAS opções.

Questão 33 (1 ponto)

As dimensões típicas que um engenheiro de testes de segurança pode usar para aprimorar o escopo do ISMS são:

1) Adição de objetos de teste adicionais ao do teste
2) Acrescentar técnicas de teste adicionais ao seu projeto de teste
3) Aprimorar a cobertura de testes, mantendo-se fiel a determinados objetos e abordagens de teste
4) Aumentar a automação da execução de testes de segurança

Que pode ser usado para

a) trazer insights adicionais sobre um determinado sistema que pode ser usado para aprimorar um ISMS existente
b) Identificar pontos fracos adicionais para componentes conhecidos para aprimorar um SGSI existente
c) identificar pontos fracos adicionais para componentes que ainda não fazem parte do ISMS geral.
d) tornar o sistema de TI existente mais seguro.

Qual das alternativas a seguir apresenta o emparelhamento correto das ações e metas do engenheiro de testes de segurança?

A) 1-c, 2-a, 3-b
B) 1-b, 2-d, 3-b
C) 1-c, 2-a, 4-b
D) 2-d, 2-c, 4-a

Escolha UMA opção.

Questão 34 (1 ponto)

Como os testes de segurança podem melhorar a mensurabilidade em um ISMS?

A) Os testes de segurança podem ser usados como análise objetiva na etapa de verificação do ciclo PDCA para medir a eficácia de um ciclo PDCA.
B) Todos os testes de segurança geram percepções quantificáveis sobre a segurança de um sistema que podem ser usadas para medir a eficácia do ISMS.
C) Quanto mais testes de segurança forem aprovados em um SUT, melhor e mais eficaz será o ISMS.
D) A eficácia de um ISMS é maior quanto mais técnicas de teste de segurança forem usadas.

Escolha UMA opção

Questão 35 (1 ponto)

Os relatórios de testes de segurança devem ser tratados com um alto nível de confidencialidade. Que tipo de dados que fazem parte da maioria dos relatórios de testes de segurança motiva essa classificação?

A) Nome do testador de segurança, prazo para execução do teste, resultados do teste (casos de teste aprovados e reprovados)
B) Ambiente de teste usado, pré-condições predefinidas dos testes executados, dados de teste usados, procedimento de execução do teste, comportamento detectado
C) Lista de vulnerabilidades CVE testadas, lista de desenvolvedores nomeados, método de desenvolvimento de software identificado, ferramentas de desenvolvimento de software identificadas
D) Usou convenções de codificação de segurança, identificou cobertura de teste funcional, aplicou varreduras de vulnerabilidade

Escolha UMA opção.

Questão 36 (1 ponto)

Imagine que você executou alguns casos de teste de segurança como parte de um teste de penetração para um sistema crítico para os negócios. Um deles falhou e parece que você identificou uma possível vulnerabilidade, que pode ter um impacto dramático nos negócios. O que fazer antes de motivar diretamente sua atenuação?

A) Demarcação de vulnerabilidade, ou seja, executar casos de teste semelhantes para identificar a demarcação da vulnerabilidade identificada.
B) Estimativa de esforço para a ação de mitigação, ou seja, para fazer uma estrutura de decomposição da mitigação pretendida
C) Projeto de atenuação, ou seja, projetar a solução que atenua a vulnerabilidade identificada
D) Ajuste de risco 1, ou seja, para verificar novamente se a vulnerabilidade identificada pode ser explorada na produção
E) Você começa imediatamente a mitigar a vulnerabilidade identificada.

Escolha DUAS opções.

Questão 37 (1 ponto)

Imagine que você identificou uma vulnerabilidade no nível 9.8 do CVSS. Você verificou duas vezes se essa vulnerabilidade pode mesmo ser explorada na produção, e a empresa confirmou que essa vulnerabilidade pode ter um impacto negativo muito forte. Por outro lado, o aplicativo é essencial para os negócios, portanto, decidiu-se mitigar o risco identificado associado à vulnerabilidade identificada: Qual é a sua recomendação?

A) Se a vulnerabilidade afetar um conjunto específico de recursos, deve-se analisar se é possível desativar o recurso específico que contém a vulnerabilidade.
B) Na maioria dos casos, é mais fácil bloquear o tráfego específico na camada de rede, portanto, a tarefa é bloquear o tráfego vulnerável específico dentro do firewall.
C) Se você tiver um firewall de aplicativo da Web moderno, as vulnerabilidades serão automaticamente identificadas e atenuadas.
D) Se for possível adicionar um controle de segurança adicional à lista de usuários (por exemplo, filtragem de IP ou adição de MFA), pode-se considerar que essa técnica reduz a probabilidade de risco.
E) Na maioria dos casos, a ação de atenuação mais rápida e barata é evitá-la completamente, reparando a vulnerabilidade dos sistemas afetados.

Escolha DUAS opções.

Questão 38 (1 ponto)

Em um ambiente de CI/CD, um novo pipeline está sendo criado para o próximo projeto em que você está trabalhando. Qual das seguintes opções você recomendaria que fosse a primeira etapa acionada como parte do pipeline?

A) SCA
B) SAST
C) DAST
D) IAST

Escolha UMA opção.

Questão 39 (1 ponto)

Quais dos seguintes scanners e métodos de teste estão verificando o aplicativo em teste durante o tempo de execução?

A) DAST
B) Análise estática
C) SCA
D) SAST

Escolha UMA opção

Questão 40 (1 ponto)

Quais objetos de teste podem ser verificados por ferramentas de teste estático?

A) Arquivos de configuração
B) Design de segurança
C) Pontos de extremidade da API
D) Processos na RAM

Escolha UMA opção.