Guia de preparação

Edição 201710

Conteúdo

1. Visão geral

EXIN Secure Programming Foundation (SPF.PR)

Escopo

O exame Secure Programming Foundation (Fundação da Programação Segura) da EXIN testa o conhecimento do candidato sobre os princípios básicos da programação segura. Os temas deste módulo são Gerenciamento de Sessão e Autenticação; Manejo de Entrada de Usuário; Autorização; Configuração, Manejo e Registro de Erros; Criptografia; e Engenharia Segura de Software.

Resumo

Cibercrime, vazamento de dados e segurança de informações recebem mais atenção que nunca nos noticiários. Governos e empresas dedicam mais e mais recursos a essas áreas. No entanto, a maioria dessa atenção parece estar focada em medidas reativas (“Como pegar os criminosos cibernéticos?”) em vez de em medidas preventivas (“Como podemos tornar nossos sistemas seguros?”). Embora seja difícil medir, relatórios de pesquisa indicam que a construção da segurança vale o investimento. A educação é fundamental no processo de construção de software. Se os programadores não entendem a segurança do software que estão construindo, qualquer investimento adicional no processo é inútil.

Contexto

A certificação EXIN Secure Programming Foundation faz parte do programa de qualificação EXIN Secure Programming. O conteúdo está relacionado com o Framework Secure Software, que pode ser baixado em http://securesoftwarealliance.org/framework-secure-software/. (Isso não é literatura de exame.)

Pùblico-alvo

Esse certificado se destina a:
-programadores e desenvolvedores de software interessados no desenvolvimento de aplicativos (de web) seguros;
-auditores que trabalharão com o Framework Secure Software.

Requisitos para a certificação

- Conclusão do exame EXIN Secure Programming Foundation com sucesso.

Um treinamento Secure Programming Foundation e conhecimento de desenvolvimento de software é altamente recomendado.

Detalhes do exame

Tipo do exame:	Questões de múltipla escolha
Número de questões:	40
Mínimo para aprovação:	65% (26 / 40 questões)
Com consulta/anotações:	Não
Equipamentos eletrônicos permitidos:	Não
Tempo designado para o exame:	60 minutos

As Regras e Regulamentos dos exames EXIN aplicam-se a este exame.

Treinamento

Horas de contato

A carga horária mínima recomendada para este treinamento é de 15 horas. Isto inclui exercícios práticos OR trabalhos em grupo, preparação para o exame e pausas curtas. Esta carga horária não inclui pausas para almoço, trabalhos extra aula e o exame.

Indicação de tempo de estudo

60 horas, dependendo do conhecimento pré-existente.

Provedor de treinamento

Você encontrará uma lista de nossos provedores de treinamento credenciados em www.exin.com.

2. Requisitos do exame

Os requisitos do exame são definidos nas especificações do exame. A tabela a seguir lista os tópicos (requisitos do exame) e subtópicos (especificações do exame) do módulo.

Requisito do exame	Especificação do exame	Peso
1. Introdução		**10%**
	1.1 Consciência de Segurança	2.5%
	1.2 Princípios Básicos	2.5%
	1.3 Segurança da Web	5%
2. Gerenciamento de Sessão e Autenticação		**15%**
	2.1 Senhas	5%
	2.2 Gerenciamento de Sessão	7.5%
	2.3 Cross-Site Request Forgery (Falsificação de Solicitação Cruzada entre Sites – CSRF/XSRF) e Clickjacking	2.5%
3. Manejo de Entrada de Usuário		**22.5%**
	3.1 Ataques de Injeção	7.5%
	3.2 Validação de Entrada	7.5%
	3.3 Estouros de Buffer	2.5%
	3.4 Cross-Site-Scripting (Scripts Cruzados entre Sites – XSS)	5%
4. Autorização		**7.5%**
	4.1 Autorização	5%
	4.2 Envenenamento de Sessão e Condições de Corrida	2.5%
5. Configuração, Manejo e Registro de Erros		**15%**
	5.1 Componentes de Terceiros, Configuração e Endurecimento	5%
	5.2 Vazamentos de Informação	2.5%
	5.3 Manejo e Registro de Erros	5%
	5.4 Recusa de Serviço	2.5%
6. Criptografia		**10%**
	6.1 O Princípio de Kerckhoff, Manejo de Chaves e Aleatoriedade	2.5%
	6.2 Criptografia de Chave Pública	2.5%
	6.3 HTTPS	5%
7. Engenharia de Software Seguro		**20%**
	7.1 Requisitos de Segurança	5%
	7.2 Design Seguro	5%
	7.3 Codificação Segura	2.5%
	7.4 Testes de Segurança	7.5%
	Total	**100%**

Especificações do exame

1. Introdução

1.1 Consciência de Segurança

O candidato pode:

1.1.1 Reconhecer a tensão entre as exigências do mercado e a segurança.

1.2 Princípios Básicos

O candidato pode:

1.2.1 Explicar o jargão de segurança e STRIDE.

1.3 Segurança da Web

O candidato pode:

1.3.1 Descrever questões de segurança HTTP.

1.3.2 Explicar o modelo de segurança do navegador.

2. Gerenciamento de Sessão e Autenticação

2.1 Senhas

O candidato pode:

2.1.1 Identificar problemas envolvidos no uso de senha.

2.1.2 Aplicar princípios de gerenciamento de senhas.

2.2 Gerenciamento de Sessão

O candidato pode:

2.2.1 Explicar como funciona o gerenciamento de sessão.

2.2.2 Reconhecer problemas em gerenciamento de sessão.

2.2.3 Reconhecer as melhores soluções para problemas em gerenciamento de sessão.

2.3 Cross-Site Request Forgery (Falsificação de Solicitação Cruzada entre Sites – CSRF/XSRF) e Clickjacking

O candidato pode:

2.3.1 Reconhecer problemas e soluções de CSRF e Clickjacking.

3. Manejo de Entrada de Usuário

3.1 Ataques de Injeção

O candidato pode:

3.1.1 Reconhecer os problemas de ataques de injeção.

3.1.2 Explicar a diferença entre consultas diretas e parametrizadas.

3.1.3 Aplicar soluções para ataques de injeção SQL.

3.2 Validação de Entrada

O candidato pode:

3.2.1 Explicar a diferença entre filtros de lista branca (whitelist) e lista negra (blacklist).

3.2.2 Aplicar validação de entrada.

3.2.3 Reconhecer quando aplicar normalização de entrada e codificação.

3.3 Estouros de Buffer

O candidato pode:

3.3.1 Identificar onde ocorrem estouros de buffer e como eles impactam a segurança.

3.4 Cross-Site-Scripting (Scripts Cruzados entre Sites – XSS)

O candidato pode:

3.4.1 Reconhecer a diferença entre ataques XSS refletidos e armazenados e as mitigações.

3.4.2 Aplicar soluções para ataques XSS.

4. Autorização

4.1 Autorização

O candidato pode:

4.1.1 Reconhecer a diferença entre autorização horizontal e vertical.

4.1.2 Reconhecer a diferença entre referências diretas e indiretas.

4.2 Envenenamento de Sessão e Condições de Corrida
O candidato pode:
4.2.1 Reconhecer envenenamento de sessão e condições de corrida.

5. Configuração, Manejo e Registro de Erros
5.1 Componentes de Terceiros, Configuração e Endurecimento
O candidato pode:
5.1.1 Justificar a necessidade de endurecimento.
5.1.2 Reconhecer métodos de endurecimento.
5.2 Vazamentos de Informação
O candidato pode:
5.2.1 Reconhecer diferentes vazamentos de informação.
5.3 Manejo e Registro de Erros
O candidato pode:
5.3.1 Explicar a importância do registro para a segurança.
5.3.2 Explicar o princípio de 'Falhar com Segurança'.
5.4 Recusa de Serviço
O candidato pode:
5.4.1 Reconhecer ataques por recusa de serviço e mitigações.

6. Criptografia
6.1 O Princípio de Kerckhoff, Manejo de Chaves e Aleatoriedade
O candidato pode:
6.1.1 Explicar a importância do Princípio de Kerckhoff, Manejo de Chaves e Aleatoriedade.
6.2 Criptografia de Chave Pública
O candidato pode:
6.2.1 Descrever a criptografia de chave pública, ataques de homem do meio e certificados.
6.3 HTTPS (5%)
O candidato pode:
6.3.1 Reconhecer as ameaças a SSL/TLS/HTTPS.
6.3.2 Aplicar HTTPS corretamente.

7. Engenharia de Software Seguro
7.1 Requisitos de Segurança
O candidato pode:
7.1.1 Identificar requisitos de segurança em falta.
7.1.2 Reconhecer ambiguidades e pressupostos ocultos em determinadas condições e contextos.
7.2 Design Seguro
O candidato pode:
7.2.1 Reconhecer ameaças que são inerentes a uma arquitetura específica.
7.2.2 Reconhecer soluções adequadas a ameaças e as imperfeições nessas soluções.
7.3 Codificação Segura
O candidato pode:
7.3.1 Reconhecer o escopo, objetivo e vantagens da revisão de código para as práticas de desenvolvimento.
7.4 Testes de Segurança
O candidato pode:
7.4.1 Lembrar diferentes métodos para testes de segurança.
7.4.2 Reconhecer o melhor teste para um determinado cenário.
7.4.3 Identificar formas de melhorar o desenvolvimento de software e processos de testes, incorporando resultados de testes.

3. Lista de conceitos básicos

Este capítulo contém os termos e abreviaturas com que os candidatos devem se familiarizar.

Por favor, note que o conhecimento destes termos de maneira independente não é suficiente para o exame; O candidato deve compreender os conceitos e estar apto a fornecer exemplos.

Inglês	Português
Architectural risk analysis	Análise de risco de arquitetura
Asymmetric cryptography	Criptografia assimétrica
Attack surface	Superfície de ataque
Authentication	Autenticação
Authorization	Autorização
Blacklisting	Lista negra
*Brute force attack	*Ataque de força bruta
Buffer overflow	Transbordamento de buffer
Certificate authority	Autoridade de certificados
Certificate chaining	Encadeamento de certificados
Certificate revocation	Revogação de certificados
*Checksums	*Checksums (Verificações de somatório)
*Cipher	*Cifra
Clickjacking	Clickjacking
Code review	Revisão de código
*Core dump leaks	*Vazamentos de core dump
*Cracking	*Cracking (Quebra de códigos)
Cryptography	Criptografia
Cross-site Request Forgery (CSRF/XSRF)	Cross-Site Request Forgery (Falsificação de Solicitação Cruzada entre Sites – CSRF/XSRF)
Cross-site Scripting (XSS)	Scripts Cruzados entre Sites (XSS)
Data flow diagram	Diagrama de fluxo de dados
Direct queries	Consultas diretas
*Domain Name System (DNS)	*Sistema de Nomes de Domínio (DNS)
Denial-of-Service (DoS)	Recusa de Serviço (DoS)
Elevation of privilege	Elevação de privilégio
Exploit	Explorar
*Framebusting	*Framebusting (Falha de estrutura)
*Framework Secure Software	*Framework Secure Software
Fuzzing	Fuzzing
Greedy and non-greedy matching	Greedy matching e non-greedy matching
*Hacking	*Hacking
Hardening	Endurecimento

Hashing	Hashing
Information disclosure	Divulgação de informações
Kerckhoffs' principle	Princípio de Kerckhoff
Logging	Registro
*MAC-address	*Endereço MAC
*Malware	*Malware
Man-in-the-middle attack	Ataque de homem do meio
*Meta information	*Meta informações
Mitigation	Mitigação
Nonce	Nonce
Nonrepudiation	Não rejeição
Parameterization	Parametrização
*Parsing (input validation)	*Parsing (validação de entrada)
Password salting	Falsificação de senha
*Phishing	*Phishing
Private key	Chave privada
Privilege escalation	Escalonamento de privilégios
Public key	Chave pública
*Randomness	*Aleatoriedade
Repudiation	Rejeição
*Secure Development Lifecycle (S-SDLC)	*Ciclo de Vida de Desenvolvimento (S-SDLC)
Session management	Gerenciamento de sessão
*Simple Object Access Protocol (SOAP)	*Protocolo Simple de Acesso a Objetos (SOAP)
Spoofing	Forjamento
SQL injection	Injeção SQL
Stack overflow	Transbordamento de pilha
Static analysis	Análise estática
STRIDE (Spoofing identity – Tampering with data – Repudiation – Information disclosure – Denial-of-Service – Elevation of privilege)	STRIDE (Spoofing identity – Tampering with data – Repudiation – Information disclosure – Denial-of-Service – Elevation of privilege, ou seja, Forjamento de Identidade – Adulteração de dados – Rejeição – Divulgação de informações – Recusa de Serviço – Elevação de privilégio)
Symmetric cryptography	Criptografia simétrica
Tampering	Adulteração
Threat modeling	Modelagem de ameaça
*Timing attack	*Ataque temporizado
Trust boundary	Limite de confiança
Trust zone	Zona de confiança
Whitelisting	Lista branca
*XML parser (input validation)	*Analista XML (validação de entrada)

4. Literatura

Literatura do exame

O conhecimento necessário para o exame é coberto na seguinte literatura:

A Hemel, T., & Witmond, G.
EXIN Secure Programming Foundation – Workbook
(R. Pisaturo, M. Hubregtse, & E. Kleijer, Eds.)
Utrecht, The Netherlands: EXIN Holding B.V., 2014 (1st ed.)
ISBN: 978-90-820388-6-6

Matriz da literatura

Requisito do exame	Especificação do exame	Referência
1. Introdução		
	1.1 Consciência de Segurança	A: Capítulo 1, § 1.1
	1.2 Princípios Básicos	A: Capítulo 1, § 1.2
	1.3 Segurança da Web	A: Capítulo 1, § 1.3
2. Gerenciamento de Sessão e Autenticação		
	2.1 Senhas	A: Capítulo 2, § 2.1
	2.2 Gerenciamento de Sessão	A: Capítulo 2, § 2.2
	2.3 Cross-Site Request Forgery (Falsificação de Solicitação Cruzada entre Sites – CSRF/XSRF) e Clickjacking	A: Capítulo 2, § 2.3
3. Manejo de Entrada de Usuário		
	3.1 Ataques de Injeção	A: Capítulo 3, § 3.1
	3.2 Validação de Entrada	A: Capítulo 3, § 3.2
	3.3 Estouros de Buffer	A: Capítulo 3, § 3.3
	3.4 Cross-Site-Scripting (Scripts Cruzados entre Sites – XSS)	A: Capítulo 3, § 3.4
4. Autorização		
	4.1 Autorização	A: Capítulo 4, § 4.1
	4.2 Envenenamento de Sessão e Condições de Corrida	A: Capítulo 4, § 4.2
5. Configuração, Manejo e Registro de Erros		
	5.1 Componentes de Terceiros, Configuração e Endurecimento	A: Capítulo 5, § 5.1
	5.2 Vazamentos de Informação	A: Capítulo 5, § 5.2
	5.3 Manejo e Registro de Erros	A: Capítulo 5, § 5.2
	5.4 Recusa de Serviço	A: Capítulo 5, § 5.2
6. Criptografia		
	6.1 O Princípio de Kerckhoff, Manejo de Chaves e Aleatoriedade	A: Capítulo 6, § 6.1
	6.2 Criptografia de Chave Pública	A: Capítulo 6, § 6.1
	6.3 HTTPS	A: Capítulo 6, § 6.1
7. Engenharia de Software Seguro		
	7.1 Requisitos de Segurança	A: Capítulo 7, § 7.1
	7.2 Design Seguro	A: Capítulo 7, § 7.2
	7.3 Codificação Segura	A: Capítulo 7, § 7.3
	7.4 Testes de Segurança	A: Capítulo 7, § 7.4

Contato EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER