Preparation Guide

Edition 201708

Content

1. Overview 4
2. Exam Requirements 6
3. List of Basic Concepts 9
4. Literature 10

1. Overview

EXIN Secure Programming Foundation (SPF.EN)

Scope

The EXIN Secure Programming Foundation exam tests the knowledge of the candidate on the basic principles of secure programming. The subjects of this module are Authentication and Session Management; Handling User Input; Authorization; Configuration, Error Handling and Logging; Cryptography; and Secure Software Engineering.

Summary

Cybercrime, data leaks and information security get more attention than ever in the news. Governments and companies dedicate more and more resources to these areas. However, most of that attention appears to be focused on reactive measures ("How do we catch the cyber criminals?") instead of on preventive measures ("How do we make our systems secure?"). Although it is hard to measure, research reports indicate that building security in is worth the investment. Key in the software building process is education. If programmers do not understand the security of the software they are building, any additional investment in the process is useless.

Context

The EXIN Secure Programming Foundation certification is part of the EXIN Secure Programming qualification program. The content is related to the Framework Secure Software, which can be downloaded from http://securesoftwarealliance.org/framework-secure-software/. (Please note that this is not exam literature.)

Target Group

This certificate is meant for:

- programmers and software developers who have an interest in developing secure (web) applications;
- auditors who will work with the Framework Secure Software.

Requirements for Certification

- Successful completion of the EXIN Secure Programming Foundation exam.

A training Secure Programming Foundation and knowledge of software development is recommended.

Examination Details

Examination type:	Multiple-choice Questions
Number of questions:	40
Pass mark:	65% (26 / 40 questions)
Open book/notes:	No
Electronic equipment/aides permitted:	No
Exam duration:	60 minutes

The Rules and Regulations for EXIN's examinations apply to this exam.

Training

Contact Hours

The recommended number of contact hours for this training course is 15. This includes group assignments, exam preparation and short breaks. This number of hours does not include lunch breaks, homework and the exam.

Indication Study Effort

60 hours, depending on existing knowledge.

Training Organization

You can find a list of our Accredited Training Organizations at www.exin.com.

2. Exam Requirements

The exam requirements are specified in the exam specifications. The following table lists the topics of the module (exam requirements) and the subtopics (exam specifications).

Exam Requirement	Exam Specification	Weight
1. Introduction		**10%**
	1.1 Security Awareness	2.5%
	1.2 Basic Principles	2.5%
	1.3 Web Security	5%
2. Authentication and Session Management		**15%**
	2.1 Passwords	5%
	2.2 Session Management	7.5%
	2.3 Cross-Site Request Forgery (CSRF/XSRF) and Clickjacking	2.5%
3. Handling User Input		**22.5%**
	3.1 Injection Attacks	7.5%
	3.2 Input Validation	7.5%
	3.3 Buffer Overflows	2.5%
	3.4 Cross-Site-Scripting (XSS)	5%
4. Authorization		**7.5%**
	4.1 Authorization	5%
	4.2 Session Poisoning and Race Conditions	2.5%
5. Configuration, Error Handling and Logging		**15%**
	5.1 Third Party Components, Configuration and Hardening	5%
	5.2 Information Leaks	2.5%
	5.3 Error Handling and Logging	5%
	5.4 Denial of Service	2.5%
6. Cryptography		**10%**
	6.1 Kerckhoffs' Principle, Key Management and Randomness	2.5%
	6.2 Public Key Cryptography	2.5%
	6.3 HTTPS	5%
7. Secure Software Engineering		**20%**
	7.1 Security Requirements	5%
	7.2 Secure Design	5%
	7.3 Secure Coding	2.5%
	7.4 Security Testing	7.5%
	Total	**100%**

Exam Specifications

1. Introduction

1.1 Security Awareness

The candidate can:

1.1.1 Recognize the tension between market demands and security.

1.2 Basic Principles

The candidate can:

1.2.1 Explain security jargon and STRIDE.

1.3 Web Security

The candidate can:

1.3.1 Describe HTTP security issues.

1.3.2 Explain the Browser Security Model.

2. Authentication and Session Management

2.1 Passwords

The candidate can:

2.1.1 Identify problems involved in password usage.

2.1.2 Apply principles of password management.

2.2 Session Management

The candidate can:

2.2.1 Explain how Session Management works.

2.2.2 Recognize problems in Session Management.

2.2.3 Recognize best solutions for problems in Session Management.

2.3 Cross-Site Request Forgery (CSRF/XSRF) and Clickjacking

The candidate can:

2.3.1 Recognize problems and solutions of CSRF and Clickjacking.

3. Handling User Input

3.1 Injection Attacks

The candidate can:

3.1.1 Recognize the problems of injection attacks.

3.1.2 Explain the difference between direct and parameterized queries.

3.1.3 Apply solutions for SQL injection attacks.

3.2 Input Validation

The candidate can:

3.2.1 Explain the difference between whitelist and blacklist filters.

3.2.2 Apply input validation.

3.2.3 Recognize when to apply input normalization and encoding.

3.3 Buffer Overflows

The candidate can:

3.3.1 Identify where buffer overflows occur and how they impact security.

3.4 Cross-Site-Scripting (XSS)

The candidate can:

3.4.1 Recognize the difference between reflected and stored XSS attacks and the mitigations.

3.4.2 Apply solutions to XSS attacks.

4. Authorization

4.1 Authorization

The candidate can:

4.1.1 Recognize the difference between horizontal and vertical authorization.

4.1.2 Recognize the difference between direct and indirect references.

4.2 Session Poisoning and Race Conditions

The candidate can:

4.2.1 Recognize session poisoning and race conditions.

5. Configuration, Error Handling and Logging

5.1 Third Party Components, Configuration and Hardening

The candidate can:

5.1.1 Justify the need for hardening.

5.1.2 Recognize methods of hardening.

5.2 Information Leaks

The candidate can:

5.2.1 Recognize different information leaks.

5.3 Error Handling and Logging

The candidate can:

5.3.1 Explain the importance of logging for security.

5.3.2 Explain the principle of 'Fail Securely'.

5.4 Denial of Service

The candidate can:

5.4.1 Recognize Denial of Service attacks and mitigations.

6. Cryptography

6.1 Kerckhoffs' Principle, Key Management and Randomness

The candidate can:

6.1.1 Explain the importance of Kerckhoffs' Principle, Key Management and Randomness.

6.2 Public Key Cryptography

The candidate can:

6.2.1 Describe Public Key Cryptography, Man-in-the-Middle Attacks and certificates.

6.3 HTTPS

The candidate can:

6.3.1 Recognize the threats to SSL/TLS/HTTPS.

6.3.2 Apply HTTPS correctly.

7. Secure Software Engineering

7.1 Security Requirements

The candidate can:

7.1.1 Identify missing security requirements.

7.1.2 Recognize hidden assumptions and ambiguities in given requirements and contexts.

7.2 Secure Design

The candidate can:

7.2.1 Recognize threats that are inherent to a specific architecture.

7.2.2 Recognize appropriate solutions for threats and the imperfections in these solutions.

7.3 Secure Coding

The candidate can:

7.3.1 Recognize scope, objective and advantages of code review to development practices.

7.4 Security Testing

The candidate can:

7.4.1 Remember different methods for security testing.

7.4.2 Recognize the best test for a given scenario.

7.4.3 Identify ways to improve software development and testing processes by incorporating findings from testing.

3. List of Basic Concepts

This chapter contains the terms and abbreviations with which candidates should be familiar.

Please note that knowledge of these terms alone does not suffice for the exam; the candidate must understand the concepts and be able to provide examples.

Architectural risk analysis	Kerckhoffs' principle
Asymmetric cryptography	Logging
Attack surface	*MAC-address
Authentication	*Malware
Authorization	Man-in-the-middle attack
Blacklisting	*Meta information
*Brute force attack	Mitigation
Buffer overflow	Nonce
Certificate authority	Nonrepudiation
Certificate chaining	Parameterization
Certificate revocation	*Parsing (input validation)
*Checksums	Password salting
*Cipher	*Phishing
Clickjacking	Private key
Code review	Privilege escalation
*Core dump leaks	Public key
*Cracking	*Randomness
Cryptography	Repudiation
Cross-site Request Forgery (CSRF/XSRF)	*Secure Development Lifecycle (S-SDLC)
Cross-site Scripting (XSS)	Session management
Data flow diagram	*Simple Object Access Protocol (SOAP)
Direct queries	Spoofing
*Domain Name System (DNS)	SQL injection
Denial-of-Service (DoS)	Stack overflow
Elevation of privilege	Static analysis
Exploit	STRIDE (Spoofing identity – Tampering with data – Repudiation – Information disclosure – Denial-of-Service – Elevation of privilege)
*Framebusting	Symmetric cryptography
*Framework Secure Software	Tampering
Fuzzing	Threat modeling
Greedy and non-greedy matching	*Timing attack
*Hacking	Trust boundary
Hardening	Trust zone
Hashing	Whitelisting
Information disclosure	*XML parser (input validation)

4. Literature

Exam Literature

The knowledge required for the exam is covered in the following literature:

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

Literature Matrix

Exam Requirement	Exam Specification	Reference
1. Introduction		
	1.1 Security Awareness	A: Chapter 1, paragraph 1.1
	1.2 Basic Principles	A: Chapter 1, paragraph 1.2
	1.3 Web Security	A: Chapter 1, paragraph 1.3
2. Authentication and Session Management		
	2.1 Passwords	A: Chapter 2, paragraph 2.1
	2.2 Session Management	A: Chapter 2, paragraph 2.2
	2.3 Cross-Site Request Forgery (CSRF/XSRF) and Clickjacking	A: Chapter 2, paragraph 2.3
3. Handling User Input		
	3.1 Injection Attacks	A: Chapter 3, paragraph 3.1
	3.2 Input Validation	A: Chapter 3, paragraph 3.2
	3.3 Buffer Overflows	A: Chapter 3, paragraph 3.3
	3.4 Cross-Site-Scripting (XSS)	A: Chapter 3, paragraph 3.4
4. Authorization		
	4.1 Authorization	A: Chapter 4, paragraph 4.1
	4.2 Session Poisoning and Race Conditions	A: Chapter 4, paragraph 4.2
5. Configuration, Error Handling and Logging		
	5.1 Third Party Components, Configuration and Hardening	A: Chapter 5, paragraph 5.1
	5.2 Information Leaks	A: Chapter 5, paragraph 5.2
	5.3 Error Handling and Logging	A: Chapter 5, paragraph 5.2
	5.4 Denial of Service	A: Chapter 5, paragraph 5.2
6. Cryptography		
	6.1 Kerckhoffs' Principle, Key Management and Randomness	A: Chapter 6, paragraph 6.1
	6.2 Public Key Cryptography	A: Chapter 6, paragraph 6.1
	6.3 HTTPS	A: Chapter 6, paragraph 6.1
7. Secure Software Engineering		
	7.1 Security Requirements	A: Chapter 7, paragraph 7.1
	7.2 Secure Design	A: Chapter 7, paragraph 7.2
	7.3 Secure Coding	A: Chapter 7, paragraph 7.3
	7.4 Security Testing	A: Chapter 7, paragraph 7.4

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER