Preparation Guide

EXIN Secure Programming Foundation

Edition November 2014

Content

1. Overview

Secure Programming Foundation (SPF)

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.

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.

Context
The exam Secure Programming Foundation is part of the Secure Programming qualification. The content is related to the Framework Secure Software, which can be downloaded from www.securesoftwarefoundation.org. (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.

Prerequisite(s)
A training Secure Programming Foundation and knowledge of software development is highly recommended.

Examination type
Computer-based or paper-based multiple-choice questions

Indication study load
60 hours, depends on existing knowledge

Practical assignment(s)
Not applicable

Time allotted for examination
60 minutes

Exam details

Number of questions:	40
Pass mark:	65% (26 points)
Open book/notes:	no
Electronic equipment/aides permitted:	no

Sample questions

You can download a sample exam at www.exin.com.

Training

Group size

The maximum number of participants is 15.
(This does not apply to online training courses.)

Contact hours

The minimum 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 homework, logistics for exam preparation and lunch breaks.

Training provider

You can find a list of our accredited training providers 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). The weight of the different topics in the exam is expressed as a percentage of the total.

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

Exam specifications

1. Introduction (10%)

1.1 Security Awareness (2.5%)
The candidate can:
- 1.1.1 Recognize the tension between market demands and security.

1.2 Basic Principles (2.5%)
The candidate can:
- 1.2.1 Explain security jargon and STRIDE.

1.3 Web Security (5%)
The candidate can:
- 1.3.1 Describe HTTP security issues.
- 1.3.2 Explain the Browser Security Model.

2. Authentication and Session Management (15%)

2.1 Passwords (5%)
The candidate can:
- 2.1.1 Identify problems involved in password usage.
- 2.1.2 Apply principles of password management.

2.2 Session Management (7.5%)
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 (2.5%)
The candidate can:
- 2.3.1 Recognize problems and solutions of CSRF and Clickjacking.

3. Handling User Input (22.5%)

3.1 Injection Attacks (7.5%)
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 (7.5%)
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 (2.5%)
The candidate can:
- 3.3.1 Identify where buffer overflows occur and how they impact security.

3.4 Cross-Site-Scripting (XSS) (5%)
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 (7.5%)

4.1 Authorization (5%)
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 (2.5%)
The candidate can:
- 4.2.1 Recognize session poisoning and race conditions.

5. Configuration, Error Handling and Logging (15%)

5.1 Third Party Components, Configuration and Hardening (5%)
The candidate can:
- 5.1.1 Justify the need for hardening.
- 5.1.2 Recognize methods of hardening.

5.2 Information Leaks (2.5%)
The candidate can:
- 5.2.1 Recognize different information leaks.

5.3 Error Handling and Logging (5%)
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 (2.5%)
The candidate can:
- 5.4.1 Recognize Denial of Service attacks and mitigations.

6. Cryptography (10%)

6.1 Kerckhoffs' Principle, Key Management and Randomness (2.5%)
The candidate can:
- 6.1.1 Explain the importance of Kerckhoffs' Principle, Key Management and Randomness.

6.2 Public Key Cryptography (2.5%)
The candidate can:
- 6.2.1 Describe Public Key Cryptography, Man-in-the-Middle Attacks and certificates.

6.3 HTTPS (5%)
The candidate can:
- 6.3.1 Recognize the threats to SSL/TLS/HTTPS.
- 6.3.2 Apply HTTPS correctly.

7. Secure Software Engineering (20%)

7.1 Security Requirements (5%)
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 (5%)
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 (2.5%)
The candidate can:
- 7.3.1 Recognize scope, objective and advantages of code review to development practices.

7.4 Security Testing (7.5%)
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 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.

Terms are listed in alphabetical order. If a concept is listed both with abbreviation and full name, either one can be tested. The terms labeled with an * are supposed to be familiar before preparation for the exam. If you feel you are not familiar with these terms, please familiarize yourself with them before taking the exam.

Architectural risk analysis	Code review
Asymmetric cryptography	*Core dump leaks
Attack surface	*Cracking
Authentication	Cryptography
Authorization	Cross-site Request Forgery (CSRF/XSRF)
Blacklisting	Cross-site Scripting (XSS)
*Brute force attack	Data flow diagram
Buffer overflow	Direct queries
Certificate authority	*Domain Name System (DNS)
Certificate chaining	Denial-of-Service (DoS)
Certificate revocation	Elevation of privilege
*Checksums	Exploit
*Cipher	*Framebusting
Clickjacking	*Framework Secure Software

Fuzzing

Greedy and non-greedy matching

*Hacking

Hardening

Hashing

Information disclosure

Kerckhoffs' principle

Logging

*MAC-address

*Malware

Man-in-the-middle attack

*Meta information

Mitigation

Nonce

Nonrepudiation

Parameterization

*Parsing (input validation)

Password salting

*Phishing

Private key

Privilege escalation

Public key

*Randomness

Repudiation

*Secure Development Lifecycle (S-SDLC)

Session management

*Simple Object Access Protocol (SOAP)

Spoofing

SQL injection

Stack overflow

Static analysis

STRIDE (**S**poofing identity – **T**ampering with data – **R**epudiation – **I**nformation disclosure – **Denial-of-Service** – **E**levation of privilege)

Symmetric cryptography

Tampering

Threat modeling

*Timing attack

Trust boundary

Trust zone

Whitelisting

*XML parser (input validation)

4. 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 reference

Exam requirement	Exam specification	Literature	Literature reference
1	1.1	A	Chapter 1, paragraph 1.1
1	1.2	A	Chapter 1, paragraph 1.2
1	1.3	A	Chapter 1, paragraph 1.3
2	2.1	A	Chapter 2, paragraph 2.1
2	2.2	A	Chapter 2, paragraph 2.2
2	2.3	A	Chapter 2, paragraph 2.3
3	3.1	A	Chapter 3, paragraph 3.1
3	3.2	A	Chapter 3, paragraph 3.2
3	3.3	A	Chapter 3, paragraph 3.3
3	3.4	A	Chapter 3, paragraph 3.4
4	4.1	A	Chapter 4, paragraph 4.1
4	4.2	A	Chapter 4, paragraph 4.2
5	5.1	A	Chapter 5, paragraph 5.1
5	5.2	A	Chapter 5, paragraph 5.2
5	5.3	A	Chapter 5, paragraph 5.2
5	5.4	A	Chapter 5, paragraph 5.2
6	6.1	A	Chapter 6, paragraph 6.1
6	6.2	A	Chapter 6, paragraph 6.1
6	6.3	A	Chapter 6, paragraph 6.1
7	7.1	A	Chapter 7, paragraph 7.1
7	7.2	A	Chapter 7, paragraph 7.2
7	7.3	A	Chapter 7, paragraph 7.3
7	7.4	A	Chapter 7, paragraph 7.4

Contact EXIN

www.exin.com

We turn skills into reputation