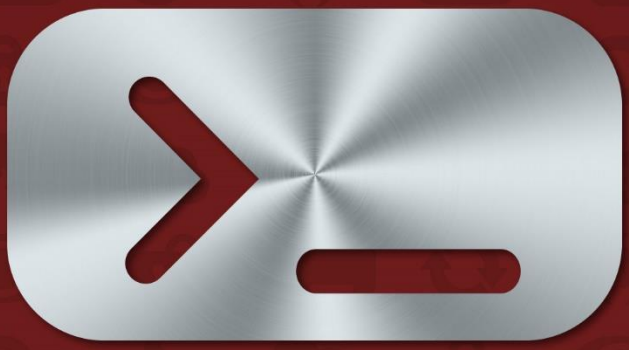

SECURE PROGRAMMING

FOUNDATION

Exam Syllabus

SECO INSTITUTE

Table of contents

Disclaimer

Although SECO-Institute has made every effort to ensure that the information in this exam syllabusbook was correct at publication time, SECO-institute does not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

Copyright notice

Exam Syllabus Secure Programming Foundation

Economic globalisation is leading to an ever-increasing exchange of information between organisations (including employees, customers and suppliers) and, consequently, an explosion of cybercrime. The dramatic rise in cyber-attacks, in turn, results in a growing demand for certified security specialists:

***"By 2017, there will be a shortage of 2 million cyber security jobs worldwide"* — UK House of Lords, Digital Skills Committee**

As cyber attackers are shifting focus to software, improving software security is becoming indispensable. The Secure Programming certificate demonstrates your ability to understand the logic behind security principles and apply security principles in design and code. The certificate enables you to exhibit your knowledge about web application vulnerabilities and the most effective ways to discover, prevent and eradicate these vulnerabilities.

With a Secure Programming certificate, you will be internationally recognised as a secure software developer.

Context

Secure Programming Foundation is part of SECO-Institute's Secure Software Certification Track.

Target audience

The Secure Programming Foundation certification program (S-SPF) is suitable for every programmer or software developer responsible for developing (web) applications. The course is suitable for both novice and experienced developers who wish to acquire a solid grounding in secure software development.

Prerequisites

None. Because the exam subject is of a technical nature we would like to recommend the following:

- Experience with one or more programming languages;
- Familiarity with web technology;
- Attending an accredited Secure Programming Foundation course.

Exam information

SECO-Institute provides the official Secure Programming Foundation courseware to accredited training centres where candidates are trained by accredited instructors. Candidates can take their exams at an accredited exam centre or directly with the SECO-Institute.

Examination details

- Computer-based
- Multiple choice with 40 questions
- Time allotted: 60 minutes
- Pass mark: 60% (out of 100)

The Rules and Regulations for SECO-Institute examinations apply to this exam.

Exam requirements

The following tables list the exam requirements and exam specifications.

Secure Programming Foundation										
Requirements	**1.** Introduction to software security **2.** Secure software engineering **3.** Authentication, Session management, and Authorisation **4.** Input handling **5.** Cryptography **6.** Configuration, error logging and handling									
Required prior knowledge	Recommended: experience with one or more programming languages, familiarity with web technology, and attending an accredited Secure Programming Foundation course.									
Learning-levels	x	Know	x	Understand		Apply		Analyse, Synthesize		Create

Exam specifications

Requirements, specifications, testing levels				Bloom level
1.	**Introduction to software security**			
	1.1	The candidate can describe the economic context of software security.		2
		The candidate is able to:		
		1.1.1	Describe the concept of information asymmetry in relation to software security.	2
		1.1.2	Recall the dilemmas of security investment by software producers.	1
Exam topics and terms			Information asymmetry, adverse selection, security investment.	
	1.2	The candidate can describe the basic concepts of security		2
		The candidate is able to:		
		1.2.1	Recall the definition of security	1
		1.2.2	Recall Microsoft's STRIDE Threat Model	1
		1.2.3	Describe the concepts of attack surface and trust zone	2
		1.2.4	Describe the basic terms of security	2
		1.2.5	Explain how the HTTP protocol works and can be misused	2
Exam topics and terms			Attack, exploit, mitigation, patch, risk, threat, vulnerability, weakness, STRIDE-model, attack surface, trust zone, man-in-the-middle proxy, HTTP Requests, HTTP responses, HTTP header injection.	

Requirements, specifications, testing levels				Bloom level
2.	**Secure software engineering**			
	2.1	The candidate can explain secure software engineering techniques		2
		The candidate is able to:		
		2.1.1	Explain how architecture analysis works	2
		2.1.2	Describe secure software engineering techniques	2
Exam topics and terms			Secure software engineering, architecture analysis, secure coding, code review, secure testing, attack and penetration test, vulnerability scan, unit test, acceptance test, regression test, automated tests, fuzzing, safety nets.	

Requirements, specifications, testing levels				Bloom level
3.	**Authentication, Session management, and Authorisation**			
	3.1	The candidate can explain authentication		2
		The candidate is able to:		
		3.1.1	Describe the concept of authentication	2
		3.1.2	Explain how lost passwords can be managed	2
		3.1.3	Describe the purpose of HTTP sessions	2
Exam topics and terms		Authentication, password strength, username/password authentication, username enumeration, password storage, lost password management.		
	3.2	The candidate can explain session management		2
		The candidate is able to:		
		3.2.1	Describe the concept of session management and related terms	2
		3.2.2	Examine session data like cookies	3
		3.2.3	Recall how a session can be made secure	1
		3.2.4	Explain session vulnerabilities and countermeasures	2
Exam topics and terms		HTTP sessions, session cookies, session data, session-ID, Cross-site request forgery (CSRF), clickjacking.		
	3.3	The candidate can explain Authorisation		2
		The candidate is able to:		
		3.3.1	Describe the key concepts of authorisation	2
		3.3.2	Explain the concept of session poisoning	2
Exam topics and terms		Authorisation, privilege escalation, unauthorised object access, authorisation checks, session poisoning, race conditions.		

Requirements, specifications, testing levels				Bloom level
4.	**Input handling**			
	4.1	The candidate can explain Input Handling		2
		The candidate is able to:		
		4.1.1	Recall the origin of the name 'cross-site-scripting'	1
		4.1.2	Recall data types that can contain instructions	1
		4.1.3	Explain the core concepts of input handling	2
		4.1.4	Describe SQL injection and the solutions to SQL injection	2
		4.1.5	Describe the concept of input validation	2
		4.1.6	Explain the concept of buffer overflows	2
Exam topics and terms		Cross-site-scripting, data types, injection attack, sub-system, instructions, user input and trust, SQL injection, direct queries, escape, prepared statements, parameterised queries, Object Relation Mappers (ORM), input validation, NUL bytes, buffer overflows, XSS, file uploads, encoding, character sets, second order injection.		

Requirements, specifications, testing levels				Bloom level
5.	**Cryptography**			
	5.1	The candidate can describe the field of cryptography		2
		The candidate is able to:		
		5.1.1	Recall Kerkhoffs principle	1
		5.1.2	Describe the key concepts of cryptography	2
		5.1.3	Explain the different types of cryptography	2
		5.1.4	Recall general cryptographic guidelines	1
Exam topics and terms		Cryptography, Kerckhoffs principle, confidentiality (encryption), integrity (checksums and hashing), authentication (signing), non-repudiation (signing), symmetric cryptography, asymmetric cryptography, Public key cryptography, man-in-the-middle attack, trusted third party, SSL/TLS.		

Requirements, specifications, testing levels				Bloom level
6.	**Configuration, error logging and handling**			
	6.1	The candidate can explain configuration, error handling and logging		2
		The candidate is able to:		
		6.1.1	Describe how third party components can be hardened.	1
		6.1.2	Describe the core concepts of configuration	2
		6.1.3	Explain how countermeasures can be configured	2
		6.1.4	Describe the concept of error handling	2
Exam topics and terms		Configuring, hardening, information leaks, reduce attack surface, side channel attacks, error handling, denial of service (DoS), logging.		

Literature

A	S-SPF -Secure Programming Foundation ‘course materials’
Optional	

Exam-literature matrix

Exam requirement	Exam specification	Literature	Chapter reference(s)
1	1.1	**A**	01_awareness_notes
	1.2	**A**	02_introduction_notes
2	2.1	**A**	09_securesoftwareengineering_notes
3	3.1	**A**	03_authsm_notes
	3.2	**A**	03_authsm_notes
	3.3	**A**	05_authorization_notes
4	4.1	**A**	04_inputhandling_notes
5	5.1	**A**	07_crypto_notes
6	6.1	**A**	06_configerrorlogging_notes

How to book your exam

All our exams are delivered through an online examination system called ProcterU. To enrol for an exam, go to: https://go.proctoru.com/
Make sure you are fully prepared. Use the ProctorU Preparation checklist to assess whether you are ready to take the exam.

If you are a new user, select Test Taker. Select "SECO-Institute" as the institution and fill in all the necessary information. See the instructions for more information. Once you have scheduled your exam, you will be asked to pay the exam fee. If you have an exam voucher, please fill in the access code.

Our online examination system allows you to book your exam and take it at any place convenient to you. Do you prefer your kitchen table, your home desk or your office? Would you rather take a test in the day or at night? It is up to you!

System requirements

To ensure the quality and security of the examination, you will have to meet specific requirements regarding your computer configuration, your exam environment and your behaviour during the exam. Click here to see the requirements.

The exam will be taken with special proctor software. To enable webcam and audio recording during the exam, you have to install software that monitors your activities.

Your exam will be recorded through your webcam and microphone. The recordings will be reviewed by multiple proctors after you have completed the exam. The proctors will check if you comply with all the requirements for the examination.

Results

If no non-conformities are detected by the proctors, you will receive the final result by email one month after you complete the test. The email will also contain information on how to claim your certificate and digital badge as well as how to use your title.

Digital badges

SECO-Institute and digital badge provider Acclaim have partnered to provide certification holders with a digital badge of their SECO-Institute certification. Digital badges can be used in email signatures as well as on personal websites, social media sites such as LinkedIn and Twitter, and electronic copies of resumes. Digital badges help certification holders convey employers, potential employers and interested parties the skills they have acquired to earn and maintain a specialised certification.

Claim your title at: https://www.seco-institute.org/claim-your-title

SPF-EN-2018-01a