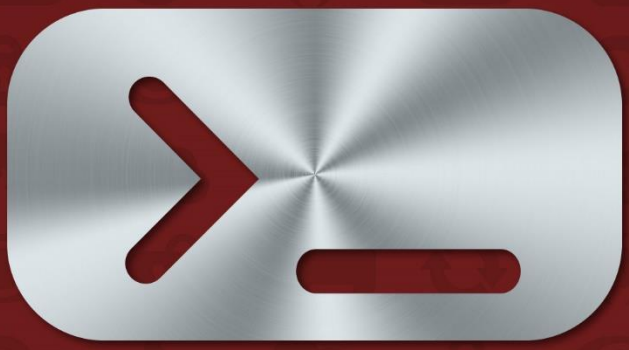

SECURE PROGRAMMING

FOUNDATION

Sample Exam

SECO INSTITUTE

Sample Exam Secure Programming Foundation

SECO-Institute issues the official Secure Software courseware to accredited training centres where students are trained by accredited instructors. Students can take their exams at an accredited exam centre or directly at the SECO-Institute. Attending an official certification course is not a prerequisite for taking an exam. Upon successful completion of a foundation exam (with a passing score of 60%), students can claim their digital badge at the SECO-Institute.

This document provides a sample exam for you to familiarise yourself with the structure and topic areas of the current Secure Programming Foundation examination. We strongly recommend you to test your knowledge before taking the actual assessment. The results of this test do not count towards your certification assessment.

Examination type

- Computer-based
- 40 Multiple choice: 2,5 points per question

Time allotted for examination

- 60 minutes

Examination details

- Pass mark: 60% (out of 100)
- Open book/notes: no
- Electronic equipment permitted: no
- The Rules and Regulations for SECO-Institute examinations apply to this exam

Questions

Question 1

What is the best answer to the question: why do we have insecure software?

A. Consumers cannot objectively assess the quality and security of available software
B. The software industry can sell more software if they offer more features for a lower price and faster delivery than their competition
C. We are bad at estimating risks. Consequently, we are unable to estimate the odds that the software built for us is vulnerable and we are unable to predict the resulting damage if those vulnerabilities are exploited
D. Consumers focus on price and features and software vendors are not liable for insecure products

Question 2

The following words are in alphabetical order: Exploit, Patch, Threat, Vulnerability.
What is the best chronological order?

A. Threat, Patch, Vulnerability, Exploit
B. Vulnerability, Threat, Exploit, Patch
C. Exploit, Vulnerability, Patch, Threat
D. Patch, Vulnerability, Threat, Exploit

Question 3

What does the abbreviation STRIDE mean, as related to exploiting system vulnerabilities?

A. Survey the system, Testing applications, Identify security objectives, Decompose it, Evaluate compliancy
B. Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
C. Security architecture, Threat evaluation, Identify vulnerabilities, Data asset matching, Evaluate compliancy
D. Safe standards, Target hardening, Identify threats, Detection of intrusions, Elevation of privilege

Question 4

To ascertain the trust boundary and improve security, it helps if a web application can be divided in clear and modular components. Which answer explains the best why this is difficult?

A. In today's web applications, JavaScript and applets are called within the browser but these components directly communicate with the web server
B. Most users score web applications only on performance and this contradicts modular design, in which the code amount is limited by building multi-purpose routines
C. The clear communication line between web client and web server can be blurred by a so-called man in the middle (MITM) proxy
D. Modern applications can contain millions of lines of code, and the resulting complexity of the code impedes modular design

Question 5

Which statement on GET requests is closest to the truth?

A. It is one of the three original HTTP Request types distinguished in the CGI standard: GET, POST and CONNECT
B. The original semantics of the CGI standard require that a GET request modifies the application state
C. GET parameters are visible in URL and therefore in the Browser address bar and in various logs
D. The original semantics were forgotten and today both GET and POST requests are equally secure

Question 6

Which of the following HTTP verbs are marked as custom in RFC 2616, section 9?

A. TRACE
B. CONNECT
C. DELETE (modify state)
D. LOCK

Question 7

Which statement about HTTP Requests in code is true?

A. .NET offers the HttpServletRequest class, which has no GET/POST difference
B. Java offers the HttpServletRequest class which implements a clear GET/POST difference
C. To avoid implementations variations, Standards provide clear details like multiple occurrences of parameters, cookies and headers
D. PHP offers the associative arrays like $_GET, $_POST, $_COOKIE, $_REQUEST to access the HTTP requests

Question 8

Which authentication method is the most secure?

A. Combine a password with an SMS token
B. Lock account after input of 10 false user-ID & password combinations
C. Delay next logins after input of 10 false user-ID & password combinations
D. Combine a password with a PIN

Question 9

A user can send his session identifier to the web server to resume a previous session. What is the best way to send a session identifier?

A. as a login parameter
B. as a cookie
C. as a POST parameter
D. as a GET parameter

Question 10

Which of the following statements on Clickjacking attacks is true?

A. A JavaScript which verifies that the top page is equal to the web site page breaks Clickjacking attacks
B. Break Clickjacking attacks by including an X-Frame-Options header with value "deny", which page can only be loaded in a frame from the specified URI
C. The user is misled to perform actions on a transparent page overlaying the visible web site page
D. Break Clickjacking attacks by including an X-Frame-Options header with value "allow-from" so pages can only be loaded in a frame from the same web site

Question 11

What will the (PCRE) regular expression '<name>.*</name>' match in the following string:
<members><name>Alice</name><name>Bob</name><name>Eve</name></members>

A. <name>Alice</name><name>Bob</name><name>Eve</name>
B. <name>Alice</name><name>Bob</name>
C. <name>Alice</name>
D. <members><name>Alice</name><name>Bob</name><name>Eve</name></members>

Question 12

Injection attacks are possible if a system passes user input unfiltered to a subsystem, which allows instructions. Which is most likely NOT a source of untrusted input data?

A. A system file
B. e-mail
C. A pointer to XML document
D. HTTP headers

Question 13

Which of the following commands is an example of a parameterized query (not vulnerable for SQL injection)?

A. [C#] SqlCommand cmd = new SqlCommand("SELECT * FROM people WHERE LastName =" +LastName.Text+"')", conn);
B. [PHP] $query = "SELECT * FROM people WHERE LastName =".$_POST['LastName'];
C. [Python] cmd = "SELECT * FROM people WHERE LastName ='%s'" % (LastName)
D. [JDBC] PreparedStatement statement = connection.prepareStatement("SELECT * FROM people WHERE LastName = ?"); statement.setString(1, LastName);

Question 14

To avoid SQL injection, what is the MAIN difficulty for a programmer to neutralize metacharacters?

A. Routines that are provided by the system may be buggy
B. Because there are many metacharacters, it is easy to miss a few
C. It is not a good idea to write your own escaping routines
D. OWASP's ESAPI library only links to a few database dialects and was not yet properly reviewed

Question 15

Which of the following statements on Stored procedures is true?

A. Stored procedures are an effective countermeasure against SQL injection
B. Stored procedures are defined in the database itself and hide the internals of SQL queries from application programmers
C. With Stored procedures it becomes impossible to construct a direct query
D. With a Stored procedure, a programmer cannot create a dynamic SQL query

Question 16

What is the best regular expression to validate a phone number in a pattern like '+31 70 1234567'

A. \+[0-9]{2}\s*[0-9]{2}\s*[0-9]{7}
B. ^\+[0-9\s]{13}$
C. [+ 0123456789]{14}
D. \n[^A-Za-z]{13}

Question 17

What is NOT a security risk linked to memory access errors?

A. Corruption of data/execution flow
B. Core dumps leak (sensitive) program information
C. Arbitrary code execution (e.g. buffer overflow)
D. Self-modifying code

Question 18

Any C programmer should use functions that protect his program against buffer overflow attacks. Which of the following functions qualifies for this?

A. fgets
B. printf
C. strcat
D. strcpy

Question 19

Which of the following techniques offers the WORST protection against stack overflows?

A. Stack canaries
B. Non-executable stack
C. Use Java (without pointers and memory access)
D. Use statements that checks lengths

Question 20

To prevent XSS attacks, escaping metacharacters is necessary. What is the MAIN difficulty in this?

A. Some XSS attacks consist of seemingly harmless characters
B. How to escape depends on the context in the HTML document
C. You have to do this in every location where user input is rendered
D. The OWASP XSS prevention cheat sheet offers only a limited set of options

Question 21

An attacker can upload and store malware files on a server. Which option offers the best protection against an XSS attack in this scenario?

A. Escaping metacharacters in uploaded files
B. Input validation on filename, content type and file content
C. Use the Content-disposition header, so that downloaded content is saved to disk
D. Use Same Origin Policy (SOP) to prevent access to objects in application's browser context

Question 22

Which of the following is NOT a good practice for validating encoded input?

A. First normalize, then validate and then process the normalized input
B. Use length checks that take encodings into account
C. Validation is performed after the input has been decoded
D. Implement the same secure code conversion functions on all subsystems

Question 23

Which of the following is an example of a visual spoofing attack using Unicode?

A. malware.\xe2\x80\xaeexe.txt rendered as: malware.txt.exe
B. '\xc0\xbcscript\xc0\xbe' rendered as: <script>
C. Lowercase <scrİpt> will produce <script>
D. '%3c%2fbutton%3e' rendered as: </button>

Question 24

Which of the following is NOT an Input handling practice?

A. Beware of higher order injections
B. Before system access, authenticate all users
C. Check lengths and sizes of input data
D. Escape right before processing by subsystem

Question 25

What is the most effective authorisation check?

A. Site-Map Security Trimming feature to define access to certain pages
B. Principal Permission annotation to restrict access to a method / class to a certain role
C. Implement extra checks in subsystems
D. Centralise authorisation checks, instead of ad-hoc checks

Question 26

Why is a distinction between internally developed code and third-party code less relevant, from a security perspective?

A. Only 10% of applications comply with the OWASP Top 10
B. Internally developed code often contains third-party libraries and components
C. Both internally developed code and third-party code are prone to side-channel attacks
D. Internally developed code and open source code are only marginally safer than (closed source) third-party code

Question 27

Which actions are generally NOT considered as system hardening?

A. Apply latest security patches
B. Disable debug functions
C. Source code review
D. Restrict unnecessary features like plugins

Question 28

Which of the following information does NOT enable a Side Channel attack?

A. Introducing faults to test error handling code paths
B. Monitor duration of calculations with known inputs
C. Monitor the electricity consumption during operations
D. Compare resulting length of packet linked to different inputs

Question 29

What is NOT considered a good practice for Error handling?

A. System should handle unhandled exceptions with a generic error message (no debug information)
B. Debug information should be logged, but never displayed to the user
C. An error message should include an error id for the user's reference
D. To avoid breaking in, block a user account after a fixed number of failed login attempt

Question 30

Which of the following statements is known as Kerckhoffs's principle?

A. The encryption system must not be required to be a secret, and its falling into the hands of the enemy should not cause any inconvenience
B. The encryption system must be practically, if not mathematically, indecipherable
C. The encryption system must be portable, and its usage and function must not require the concourse of several people
D. The encryption system must be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe

Question 31

Which of the following problems can NOT be solved using cryptography?

A. Ensure the authenticity of communication messages
B. Ensure that it is impossible to capture communicated data
C. Secure the exchange of symmetric session keys over the Internet
D. Ensure that an actor cannot deny his actions

Question 32

What is the best way Eve can set up a Man-in-the-Middle (MitM) attack to interfere with the secret communications between Alice and Bob?

A. Eve decrypts messages Alice sent to Bob using Alice’s public key
B. Eve tricks the certificate authority (CA) into believing that she is Alice, depositing a new public key
C. Eve tricks Alice into using Eve's public key instead of Bob's public key
D. Eve uses both Alice’s and Bob’s public keys to decrypt the keys of the message exchanged between them

Question 33

Which of the following is NOT a valid crypto guideline?

A. Store crypto keys separate from data (better: do not store)
B. Choose strong crypto keys (like passwords)
C. Scenario for compromised crypto keys
D. Use a secret (closed source) random number generating algorithm

Question 34

Which of the following problems is NOT related to the (in)security of SSL/TLS?

A. There could be (unknown) bugs in the protocols
B. The CA is compromised (Dutch Diginotar)
C. Certificate chain not fully checked
D. If false public keys are distributed, the communicated data is at risk

Question 35

What is the best description of the focus of the Framework Secure Software?

A. Certify the security of a piece of software and give developers feedback on the security of the application under construction
B. Prescribes what should be done in the software development process
C. How organisations can improve the security delivered by the development process
D. Compare and categorise the practices organisations use. Some best practices are more advanced than others

Question 36

Which process is (partly) described by the following steps: 1) identify system assets 2) identify system information content and supported business processes 3) identify parties interested in attacking the system?

A. threat modelling
B. risk analysis
C. risk management
D. asset management

Question 37

To determine the attack surface, a data flow diagram (DFD) can be composed. Which elements does a DFD contain?

A. Information input and output for the system, the data flows through the system, the data stores and the system border
B. Agents (closed rectangle), processes (ellipse), data stores (open rectangle), data flows (arrow) and trust boundaries (dotted line)
C. A visual overview of the flow of information, where data comes from, where it goes and how it gets stored
D. Entities (square), processes (circles), Data stores (open rectangle), Data flows (line) and the system border

Question 38

Which of the following actions is NOT an element of Threat management (part of architectural analysis)?

A. Accept (+ person who accepts responsibility)
B. Move risk (insurance)
C. Manage security requirements (create, update, delete)
D. Stop development (lost cause)

Question 39

What is generally NOT considered a disadvantage of pentests?

A. The system needs to be mature enough to be ready for tests
B. From the results it is often difficult to see what the scope and thoroughness of the pentest was
C. Testers need to have expert knowledge to perform pentests
D. Pentesting cannot be done by the development team

Question 40

What is NOT a disadvantage of vulnerability scanners?

A. Security scanners can be quite difficult to use
B. Security scanners can detect false positives
C. Security scanners do not find everything, only known vulnerabilities
D. It requires security knowledge to understand the output of Security scanners

j

Answers

Question	Answer	Explanation
1	D	The answer "Consumers focus on price and features en software vendors are not liable for insecure products" is the only answer which contains 2 cause-and-effect arguments
2	B	A Vulnerability can lead to Threat, the attacker can develop an Exploit, after an attack a Patch can be developed to repair a vilnerability
3	B	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
4	A	When a programmer is unaware that his browser component directly communicate with the web server, he could forget to address security in this component
5	C	The (security) differences between GET and POST are that GET parameters are visible in URL (and therefore in the Browser address bar and in various logs) and a POST request modifies the application state
6	D	LOCK is listed a custom HTTP verb
7	D	PHP offers the associative arrays like $_GET, $_POST, $_COOKIE, $_REQUEST to access the HTTP requests. Access Headers with the function apache_request_headers().
8	A	A password with an SMS token is the best option, because it combines 2 authentication factors
9	B	GET parameters will leak in your browser history, while POST requests and cookies do not suffer from this. A login parameter is not very practical
10	C	The user is misled in performing actions on an transparant page overlaying the visible web site page; this Javascript is NOT an effective protection; the X-Frame-Options values are described wrong
11	A	<name>Alice</name><name>Bob</name><name>Eve</name>
12	A	A system file is protected and cannot be changed by any regular user
13	D	[JDBC] PreparedStatement statement = connection.prepareStatement("SELECT * FROM people WHERE lastName = ?"); statement.setString(1, name); //lastName is a VARCHAR
14	B	Because there are many metacharacters, it is easy to miss a few. An important one that should not be forgotten is the escape character itself. Therefore it is usually not a good idea to write your own escaping routines
15	B	Stored procedures are defined in the database itself and hide the internals of SQL queries from application programmers. The call to the stored procedure needs to be free from SQL injection
16	A	\+[0-9]{2}\s*[0-9]{2}\s*[0-9]{7} is the best regular expression, because it combines white space flexibility with strictest test on number groups
17	D	With the Von Neumann architecture, programs and data share the same memory unit. This allowed very flexible computers, that can load programs from input devices and execute them. Self-modifying code allowed smaller programs to be executed.
18	A	The best defense against buffer overflows is to check the length. Alternatives exist to most of the dangerous C functions, such as fgets instead of gets.
19	C	The language interpreter and extensions are probably written in C or C++ for efficiency and could vulnerable to a buffer overflow. So programs in Java, Python, PHP and so on, can be vulnerable to buffer overflow attacks

20	B	Because HTML consists of a mix of several languages, how to escape depends on the context in the HTML document
21	C	Using the Content-disposition header to save downloaded content to disk is the best protection to guarantee that uploaded files will not be opened in the application's browser
22	C	Validation after input decoding is necessary, but so is validation before decoding. For instance, the decoding function can have a known vulnerability like a buffer overflow
23	A	The Unicode `RIGHT-TO-LEFT OVERRIDE' character will cause all subsequent characters to be rendered (and only rendered) from right to left. This is an example of a visual spoofing attack
24	B	Authenticating users does not imply that their input can be trusted
25	D	Checking privileges is best done by a centralized mechanism, instead of ad-hoc checks. Answer B and C are restricted to .NET systems. Answer C is only valid when the system contains subsystems, like a database or web server
26	B	Customers consider 40% to be third-party applications. Between 30 and 70% of internally developed applications are actually comprised of third-party libraries and components [Veracode's "state of software security" report]
27	C	Hardening are all actions that improve the security of a system by changing configuration and installation. Source code review does not fall in that category
28	A	A Side Channel attack uses meta information to destill information, like the duration of calculations with known inputs. It does not involve introducing processing faults
29	D	If a user account is locked after a fixed number of failed login attempts, it is easy to make the system unavailable for any user
30	A	The security of the encryption system must not rely on the secrecy of its workings, only on the strength of the (secret) encryption key. That is: no security by obscurity
31	B	Capturing of communicated data is always impossible if the attacker has access to the communication medium, like the Internet. To te able to decypher it, is another matter entirely
32	C	Eve tricks Alice in using Eve's public key instead of Bob's public key. This way Eve can decrypt the messages Alice sent to Bob and send Bob an altered message using his public key
33	D	Always use a good random number (publicly known) generating algorithm. Remember Kerkhoff's principle: no security by obscurity
34	D	The risk of false public keys is a Key Management problem and is unrelated to SSL/TLS
35	A	The Framework Secure Software is aimed at certifying the security of a piece of software and give developers feedback on the security of the application under construction
36	A	For an adequate system protection, we first need to identify the threats using the threat modeling process: 1) identify system assets 2) identify information content and supported business processes 3) identify parties interested in attacking these
37	B	To support the Threat Modeling process, a DFD shows all agents (or external entities to the system), processes, data stores, data flows and trust boundaries of a system
38	C	Manage security requirements is not an element of Threat management
39	D	Basic pentesting can be done by the development team, using tools like OWASP zap and the OWASP testing guide
40	A	The big advantage of Security scanners is that they are easy to use and very fast

How to book your exam?

All our exams are delivered through an online examination system called ProctorU. To enrol for an exam, go to: https://www.seco-institute.org/certification-exams/how-to-book-exam/
Make sure you are fully prepared. Use the ProctorU Preparation checklist to assess whether you are ready to take the exam.

Review the examination rules at
https://www.seco-institute.org/html/filesystem/storeFolder/10/Rules-and-Regulations-for-SECO-Institute-Examinations-2017-11.pdf

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.

SECO-Institute doesn't issue certification titles for Foundation courses. However, upon successful completion of your Foundation exam, you can claim your digital badge free of charge at the SECO-Institute.

https://www.seco-institute.org/claim-your-foundation-badge

SPF-Sample Exam-EN-v1.0