Western Governors University (WGU) ITEC2034 D385 Software Security and Testing Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here’s how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don’t just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. In the provided function, what is returned when the first argument x is None?

A. y

B. None

C. x

D. 0

2. Which HTTP header indicates the type of content the server will respond with?

A. Content-Type

B. Accept

C. Server

D. User-Agent

3. CORS relaxes which security policy for certain resources?

A. Same-origin policy

B. Content security policy

C. Privacy policy

D. Access control policy

4. In the AES encrypt method shown, which mode is used for the cipher?

A. CTR

B. CBC

C. ECB

D. OFB

5. Which HTTP status code means the request requires authentication to proceed?

A. Unauthorized - Your request requires authentication

B. Forbidden - Access is denied

C. Not Found - The resource does not exist

D. Internal Server Error - Server failure

6. In the password length check program, what message is printed when a 7-character password is entered?

A. Your password is long enough.

B. Your password is too short.

C. Password must be at least 8 characters.

D. Password length is invalid.

7. Which permission setting corresponds to granting read, write, and execute only to the owner and no permissions to others?

A. Owner has read, write, and execute; others have no permissions.

B. Owner has read only; others have read.

C. Everyone has read, write, and execute.

D. Owner has execute only; others have no permissions.

8. What is the exact name of the function used to guard against log injection attacks?

A. validate()

B. sanitize()

C. escape()

D. filter()

9. What does SCA stand for and what does it do?

A. Software Composition Analysis

B. Static Code Analysis

C. Secure Communications Analysis

D. System Compliance Assessment

10. When you send credentials with a request, which header is described as carrying authentication information in the material?

A. Authentication

B. Authorization

C. Cookie

D. X-API-Key

Answers

1. A
2. A
3. A
4. A
5. A
6. B
7. A
8. A
9. A
10. A

Explanations

1. In the provided function, what is returned when the first argument x is None?

A. y

B. None

C. x

D. 0

The function treats None as a signal to fall back to the second argument. If the first parameter is None, it returns the second parameter (y) instead of the first. This pattern uses None as a sentinel for "no value here" and uses the other value as the default. For example, if you call the function with the first argument as None, you'll get the second argument back because the code path for that case returns y. So the returned value is the second argument.

2. Which HTTP header indicates the type of content the server will respond with?

A. Content-Type

B. Accept

C. Server

D. User-Agent

The main idea here is how the server communicates what kind of data will be in the response body. The header that indicates this is Content-Type. It appears in the server's response and specifies the media type, such as text/html; charset=UTF-8, application/json, or image/png, so the client can render or process the payload correctly. Other headers have different roles: Accept is sent by the client to say what content types it can handle, not what the server will send. The Server header reveals information about the server software, not the data format. The User-Agent header identifies the client making the request, again not the response content type.

3. CORS relaxes which security policy for certain resources?

A. Same-origin policy

B. Content security policy

C. Privacy policy

D. Access control policy

Cross-origin access is restricted by the same-origin policy, which prevents a web page from reading data from a different origin. CORS provides a controlled way to relax that restriction for specific resources. When a server wants to allow cross-origin requests, it includes headers like Access-Control-Allow-Origin in its responses, indicating which origins are permitted. For certain types of requests, the browser may perform a preflight check (an OPTIONS request) to verify allowed methods and headers before the actual request is made. If the server approves, the cross-origin request proceeds. The other options don't fit because Content Security Policy controls what resources a page can fetch or execute (not the cross-origin access itself), privacy policy describes data handling practices, and access control policy is a broader term not the browser mechanism used to enable cross-origin sharing.

4. In the AES encrypt method shown, which mode is used for the cipher?

A. CTR

B. CBC

C. ECB

D. OFB

This question tests how a block cipher like AES is used to generate a keystream and apply it to the plaintext. In CTR mode, AES is run on a unique counter value (often a nonce combined with a counter) to produce a keystream block. Each plaintext block is then XORed with the corresponding keystream block to create ciphertext. The counter is incremented for every block, and encryption and decryption both regenerate the same keystream when the same key and nonce are used, so XOR recovers the original text. This approach has advantages: you don't need padding, and you can process data in parallel since each keystream block is independent of others, as long as the nonce-counter pair is never reused with the same key. Other modes either chain blocks (making decryption depend on previous ciphertext in CBC) or produce a keystream in a different way (ECB is insecure due to repeating patterns, OFB/CFB feed back previous outputs rather than using a counter). If the shown AES encrypt method uses a counter to derive a keystream and XORs it with the plaintext, that indicates CTR mode.

5. Which HTTP status code means the request requires authentication to proceed?

A. Unauthorized - Your request requires authentication

B. Forbidden - Access is denied

C. Not Found - The resource does not exist

D. Internal Server Error - Server failure

When a client tries to access a protected resource, HTTP uses status codes to tell the client what to do next with authentication and authorization. The code that signals authentication is required is the one that indicates the request needs the client to provide valid credentials before it can proceed. This is described as Unauthorized, and it corresponds to 401 Unauthorized. It directly communicates that authentication is necessary to access the resource, often accompanied by a WWW-Authenticate header that explains how to authenticate. If the client does provide valid credentials but isn't allowed to access the resource, a different code is used to indicate that access is forbidden for the authenticated user. The other two options describe separate issues: Not Found means the resource doesn't exist, and Internal Server Error means something went wrong on the server.

6. In the password length check program, what message is printed when a 7-character password is entered?

A. Your password is long enough.

B. Your password is too short.

C. Password must be at least 8 characters.

D. Password length is invalid.

This question tests how a password length check communicates when the input doesn't meet the minimum requirement. If the policy is that passwords must be at least eight characters, a seven-character input fails the check length < 8, so the program prints a message indicating it is too short. That feedback directly tells the user to provide a longer password. If the password had eight or more characters, you'd expect a positive response like that it is long enough. The option about needing at least eight characters is a policy statement, not the immediate runtime message for a seven-character input. The phrase about the length being invalid would be used in cases outside the normal minimum-length failure, such as non-numeric input or lengths outside the accepted range.

7. Which permission setting corresponds to granting read, write, and execute only to the owner and no permissions to others?

A. Owner has read, write, and execute; others have no permissions.

B. Owner has read only; others have read.

C. Everyone has read, write, and execute.

D. Owner has execute only; others have no permissions.

Understanding Unix-like file permissions and how read, write, and execute are assigned to the owner, group, and others. The correct setting is when the owner has read, write, and execute, and others have no permissions. This means the owner can read the file, modify it, and run it if it's a program, while no one else can access it at all. In common notation, that's rwx for the owner and --- for everyone else, often represented numerically as 700. The other descriptions either grant some permission to others, or restrict the owner's access, so they don't meet the requirement of exclusive owner access with no permissions for others.

8. What is the exact name of the function used to guard against log injection attacks?

A. validate()

B. sanitize()

C. escape()

D. filter()

Guarding against log injection hinges on ensuring that what gets written to logs is safe and exactly what you expect to record. Using a function named to validate input embodies this approach: it checks that the data conforms to a defined, safe pattern and rejects or handles anything outside those rules. By validating the input before logging, you prevent characters or sequences that could alter the log's structure, such as control characters or newlines, from slipping in. This upfront check is the most direct way to enforce that only safe content makes it into log files. Sanitizing would remove or neutralize dangerous content after it's seen, escaping would encode characters to prevent interpretation at the point of use, and filtering would apply rules to allow or deny data, but none conveys the same explicit upfront enforcement as validation.

9. What does SCA stand for and what does it do?

A. Software Composition Analysis

B. Static Code Analysis

C. Secure Communications Analysis

D. System Compliance Assessment

Software Composition Analysis is about the building blocks that make up your software—the third-party libraries and open-source components you depend on. SCA stands for Software Composition Analysis, and its job is to create an inventory of these components, including their versions and licenses, and to identify known vulnerabilities associated with them. It often uses a Software Bill of Materials to map each component to vulnerability databases (like CVEs) so you can see where risk lives and prioritize remediation. This is different from Static Code Analysis, which inspects your own source code for defects or security flaws without focusing on external dependencies. The other terms mentioned refer to other security or governance activities, not the practice of cataloging and assessing software components. So, the correct understanding is that SCA stands for Software Composition Analysis, and it helps manage risk from third-party components by revealing what's in the software, what licenses apply, and where vulnerabilities exist.

10. When you send credentials with a request, which header is described as carrying authentication information in the material?

A. Authentication

B. Authorization

C. Cookie

D. X-API-Key

When credentials are sent with a request, the header responsible for delivering that proof of identity is described as carrying authentication information. This header's purpose is to convey the data that proves who the client is, so the server can verify identity and determine what the client is allowed to do. In practice, many systems use a header named for the action of proving identity, and the value (such as a token or encoded credentials) is what the server checks to authenticate the user. While other headers like Authorization (the standard in many implementations), Cookie (for session state), or X-API-Key (for API keys) can also carry credentials, the material identifies the header in question specifically as the one that carries authentication information, making it the best match for this scenario.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://wgu-itec2034d385softwaresectesting.examzify.com

We wish you the very best on your exam journey. You've got this!