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

Copyright **1**

Table of Contents **2**

Introduction **3**

How to Use This Guide **4**

Questions **5**

Answers **8**

Explanations **10**

Next Steps **15**

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. What does HTTP status code 200 indicate?

A. OK - The request was successful

B. Created - The resource was created

C. Bad Request - The request is wrong or missing information

D. Not Found - The requested resource does not exist

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

A. validate()

B. sanitize()

C. escape()

D. filter()

3. In the 403 server response question, which status code indicates the server understood the request but refuses to authorize?

A. 200

B. 403

C. 404

D. 500

4. Which API design practice helps prevent privilege escalation by controlling access at both resource and field levels?

A. Implement resource and field-level access control

B. Use role-based authentication only

C. Rely on client-side checks

D. Encrypt all API responses

5. 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.

6. Which HTTP header indicates what content types the client can accept in responses?

- **A. Content-Type**
- **B. Accept**
- **C. Server**
- **D. User-Agent**

7. Which HTTP status code indicates the endpoint does not allow for that specific HTTP method?

- **A. OK - The request was successful**
- **B. Not Found - The resource does not exist**
- **C. Method Not Allowed - The endpoint does not allow for that specific HTTP method**
- **D. Created - The resource was created**

8. Which outcome is a likely result if a site is vulnerable to cross-site scripting?

- **A. Access the user's data**
- **B. Steal server configuration**
- **C. Change database schemas**
- **D. Disable user accounts**

9. Which HTTP status code indicates access is forbidden due to insufficient permissions?

- **A. Unauthorized - Authentication is required**
- **B. Forbidden - The website can be reached, but more permissions are needed before accessing further**
- **C. Not Found - The resource does not exist**
- **D. Conflict - The request could not be completed due to a conflict**

10. Which statement describes 403 Forbidden?

- **A. The server understands the request but refuses to authorize it**
- **B. The request lacks valid authentication credentials**
- **C. The resource cannot be found**
- **D. The request is malformed**

Answers

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

Explanations

1. What does HTTP status code 200 indicate?

A. OK - The request was successful

B. Created - The resource was created

C. Bad Request - The request is wrong or missing information

D. Not Found - The requested resource does not exist

HTTP status codes tell the client how a request turned out. A 200 OK means the request was received, understood, and processed successfully, and the server is returning the requested content or a confirmation of the action. This is the general signal of success for most operations; for example, a GET returns the resource with 200, while a POST may return 200 if the action succeeded, though 201 Created is used when a new resource is actually created. The other options reflect different outcomes: Created means a new resource was created, Bad Request means the request had invalid syntax or missing data, and Not Found means the requested resource doesn't exist.

2. 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.

3. In the 403 server response question, which status code indicates the server understood the request but refuses to authorize?

A. 200

B. 403

C. 404

D. 500

Authorization is denied even though the server understood the request. A 403 Forbidden is returned when access to the resource is not allowed for the authenticated user or the client lacks the necessary permissions, so the server refuses to authorize the request despite understanding it. By contrast, a 200 means the request succeeded and the resource is returned, a 404 means the resource cannot be found, and a 500 indicates a server-side error. If authentication were missing or invalid, you'd typically see a 401 Unauthorized instead.

4. Which API design practice helps prevent privilege escalation by controlling access at both resource and field levels?

A. Implement resource and field-level access control

B. Use role-based authentication only

C. Rely on client-side checks

D. Encrypt all API responses

Access control must be enforced at multiple levels to prevent privilege escalation. Implementing resource and field-level access control means every API call is checked for both whether the user can access the resource and whether they are allowed to view or modify specific fields within that resource. This layered authorization blocks scenarios where a user can reach a resource but is still barred from sensitive data or actions inside it. For example, a user may be allowed to read customer records but not to see salaries, and not allowed to modify protected fields. If you only apply checks at the resource level, sensitive fields could be exposed; if you only apply field-level checks, you might still permit access to the resource itself. Other options fall short: role-based authentication verifies identity but not what they can do; client-side checks can be bypassed; encryption protects data in transit but does not enforce who can access or see fields on the server side.

5. 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.

6. Which HTTP header indicates what content types the client can accept in responses?

A. Content-Type

B. Accept

C. Server

D. User-Agent

Content negotiation in HTTP uses the Accept header to indicate which content types the client can process in responses. It lets the server choose a representation that the client can handle, and it can include quality values to express preference among types. If no acceptable type is available, the server may respond with an error such as Not Acceptable. The other headers aren't about what content types the client can accept: Content-Type describes the media type of the body being sent or received, Server identifies the server software, and User-Agent describes the client application.

7. Which HTTP status code indicates the endpoint does not allow for that specific HTTP method?

A. OK - The request was successful

B. Not Found - The resource does not exist

C. Method Not Allowed - The endpoint does not allow for that specific HTTP method

D. Created - The resource was created

When a client uses an HTTP method that the endpoint does not support for the requested resource, the server responds with 405 Method Not Allowed. This signals that the resource exists, but the particular method you're using isn't permitted for it, and often the response includes an Allow header listing the allowed methods. This is different from OK, which means the request succeeded; Not Found means the resource can't be located; and Created means a new resource was created as a result of the request. The 405 status specifically identifies a method-mismatch rather than a missing resource or a successful operation.

8. Which outcome is a likely result if a site is vulnerable to cross-site scripting?

A. Access the user's data

B. Steal server configuration

C. Change database schemas

D. Disable user accounts

Cross-site scripting lets an attacker run malicious code in the victim's browser. That code can read data that the page exposes or stores in the browser, such as session cookies, tokens, or information the user has entered into forms. With access to these client-side data, an attacker can impersonate the user or steal sensitive details, which is why accessing the user's data is the most likely outcome of an XSS vulnerability. The other options involve server-side access or administrative controls, which XSS doesn't directly grant just by injecting scripts into a page.

9. Which HTTP status code indicates access is forbidden due to insufficient permissions?

A. Unauthorized - Authentication is required

B. Forbidden - The website can be reached, but more permissions are needed before accessing further

C. Not Found - The resource does not exist

D. Conflict - The request could not be completed due to a conflict

HTTP status codes that deal with access control tell you why a request didn't succeed in terms of permissions. When a resource is reachable but your user account doesn't have the rights to view it, the server responds with a forbidden status. This means the request was understood and you might be authenticated, but you're not allowed to access that resource due to insufficient permissions. It's different from an authentication failure, where you're missing or have invalid credentials, and it's different from not found (the resource doesn't exist) or a conflict (the request would create an inconsistent state). So the option that describes access as forbidden because more permissions are needed is the correct one. If you need to act, you'd typically request the appropriate role or permissions, or contact an administrator to grant access.

10. Which statement describes 403 Forbidden?

A. The server understands the request but refuses to authorize it

B. The request lacks valid authentication credentials

C. The resource cannot be found

D. The request is malformed

When a server returns 403 Forbidden, it means the server understood your request but will not grant access. This is about permission rather than proving who you are. If you haven't provided valid credentials, you'd typically see a 401 Unauthorized instead. If the resource doesn't exist, the server would respond with 404 Not Found. If the request itself is malformed, you'd get 400 Bad Request. So the statement that the server understands the request but refuses to authorize it best captures this status: access is explicitly denied due to permissions, even though the request is otherwise valid.

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!