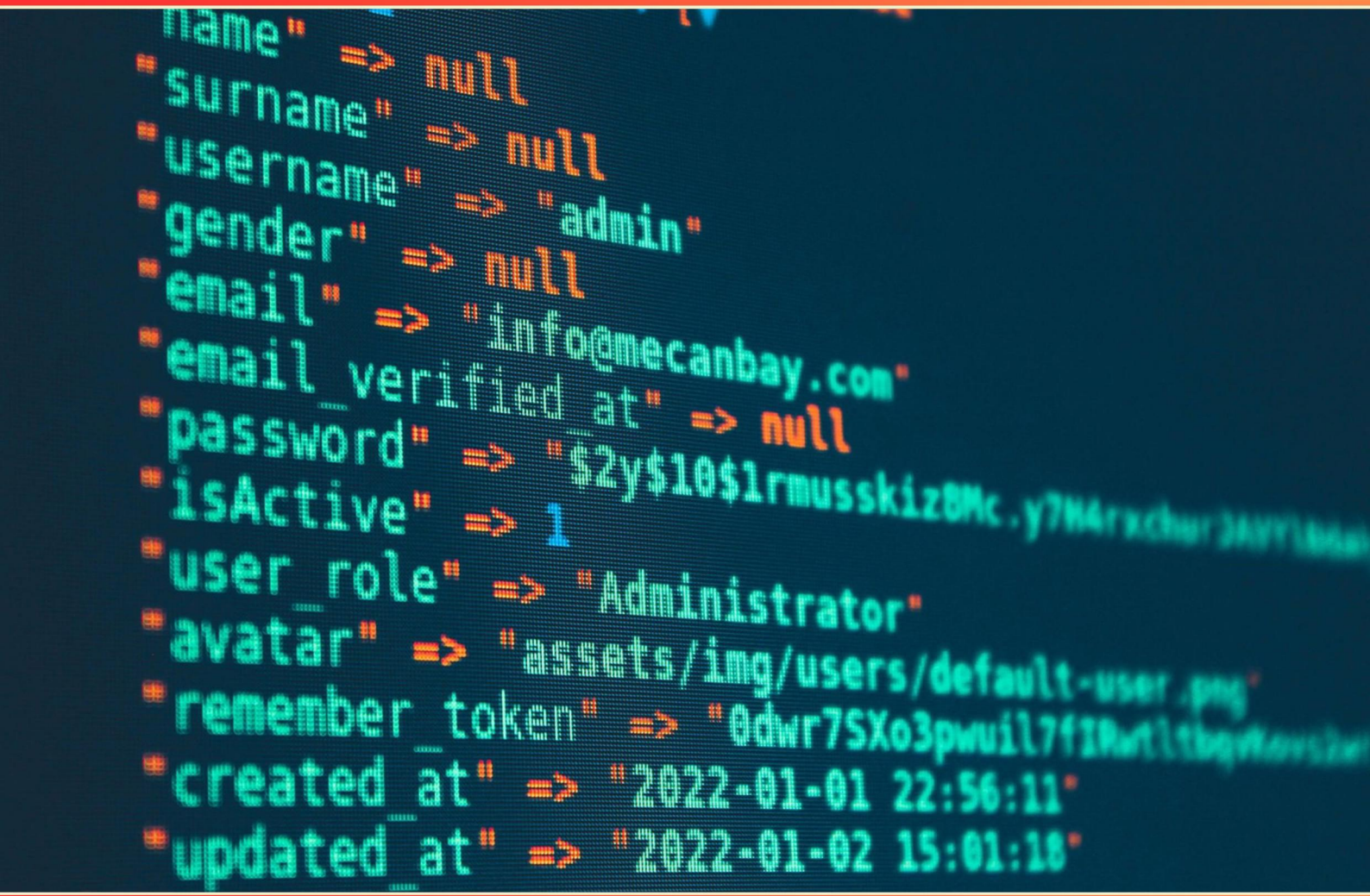
WESTERN GOVERNORS UNIVERSITY (WGU) ITEC2034 D385 SOFTWARE SECURITY AND TESTING PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://wgu-itec2034d385softwaresectesting.examzify.com

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 API code snippet that performs a GET request and prints result content, which HTTP status would you expect from a forbidden resource?**

   A. 200 - OK

   B. 403 - FORBIDDEN

   C. 404 - NOT FOUND

   D. 500 - SERVER ERROR

2. **What is an incident response plan and what are its typical steps?**

   A. A plan for creating and marketing software features.

   B. A plan for data backups and disaster recovery.

   C. A plan for hiring and budgeting.

   D. A plan for detecting, containing, eradicating, and recovering from security incidents, including preparation, detection, containment, eradication, recovery, and lessons learned.

3. **What does cross-origin resource sharing (CORS) allow browsers to do?**

   A. Override the same-origin policy for specific resources

   B. Block all cross-origin requests by default

   C. Encrypt cross-origin requests

   D. Require authentication for cross-origin requests

4. **What does STRIDE stand for in threat modeling?**

   A. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

   B. Spoofing; Tampering; Repudiation; Information Disclosure; Denial of Service; Privilege Elevation

   C. Spoofing, Tampering, Repudiation, Data Disclosure, Denial of Service, Elevation of Privilege

   D. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Privilege Elevation

5. **Given r = range(1, 10) and num = int(input()), which value prints 'The number input is in the range from 1 and 10'?**

   A. The number input is in the range from 1 and 10.

   B. The number input is not in the range from 1 and 10.

   C. The number input is between 1 and 9 inclusive.

   D. The number input is out of range.

6. In the grant_permission function, when result is False, what permission is assigned to the file?

A. Read permission for owner, group, and others

B. Read, write, execute for owner only

C. No permissions

D. Read and write for all

7. The Celsius to Fahrenheit function uses an assertion. What condition does this assertion enforce?

A. Non-negative Temperature

B. Temperature must be an integer

C. Output must be Fahrenheit

D. Inputs and outputs must be transformed atomically

8. What is the primary defense against log injection attacks?

A. Sanitize outbound log messages

B. Validate input fields

C. Encrypt log files

D. Disable logging

9. CORS relaxes which security policy for certain resources?

A. Same-origin policy

B. Content security policy

C. Privacy policy

D. Access control policy

10. What are security controls and provide examples in software?

A. Security controls are decorative UI elements.

B. Security controls are measures to reduce risk. Examples: authentication, authorization, encryption, input validation, logging, and secure communications.

C. Security controls are only physical devices.

D. Security controls replace the need for secure coding.

Answers

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

Explanations

1. In the API code snippet that performs a GET request and prints result content, which HTTP status would you expect from a forbidden resource?

A. 200 - OK

B. 403 - FORBIDDEN

C. 404 - NOT FOUND

D. 500 - SERVER ERROR

Access control is shown by HTTP status codes. If a resource exists but the client isn't allowed to access it, the server returns 403 Forbidden, signaling that authentication may be present but the client lacks the necessary permissions. A 200 OK would indicate the request succeeded and content was returned, which isn't the case for a restricted resource. A 404 Not Found means the resource doesn't exist at that location, not simply that access is blocked. A 500 Server Error points to a problem on the server, not an access control issue. So for a resource you're not allowed to access, 403 Forbidden is the appropriate response.

2. What is an incident response plan and what are its typical steps?

A. A plan for creating and marketing software features.

B. A plan for data backups and disaster recovery.

C. A plan for hiring and budgeting.

D. A plan for detecting, containing, eradicating, and recovering from security incidents, including preparation, detection, containment, eradication, recovery, and lessons learned.

An incident response plan is a structured, repeatable process for handling security incidents so you can detect them quickly, contain their impact, remove the threat, and restore normal operations while learning from the event. It typically covers preparation (team roles, communication plans, and playbooks), detection and analysis (monitoring, alert triage, and incident classification), containment (short-term actions to limit spread), eradication (removing the threat and cleaning affected systems), recovery (restoring services and validating systems are clean), and lessons learned (post-incident review to improve defenses and responses). This sequence helps ensure incidents don't escalate, evidence is preserved for forensics and legal needs, and defenses get strengthened over time. The other options describe activities outside the full scope of incident response: planning for feature development, birth of data backups and disaster recovery (which are broader business continuity concerns), or HR and budgeting tasks. While backups and DR are important and can support recovery, they do not by themselves constitute an incident response plan.

3. What does cross-origin resource sharing (CORS) allow browsers to do?

A. Override the same-origin policy for specific resources

B. Block all cross-origin requests by default

C. Encrypt cross-origin requests

D. Require authentication for cross-origin requests

CORS lets the browser relax the same-origin policy for certain cross-origin requests when the server explicitly allows it. In practice, this means a server can opt in to let a web page from another origin access its resources by sending headers like Access-Control-Allow-Origin. The browser may also perform a preflight check using an OPTIONS request for some non-simple requests before granting access. This mechanism does not apply to all cross-origin requests automatically, only to those the server has permitted. It isn't about encrypting traffic (that's TLS/HTTPS) and it doesn't inherently require authentication for access—the server's response may or may not require credentials. So the best description is that it allows browsers to override the same-origin policy for specific resources.

4. What does STRIDE stand for in threat modeling?

A. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

B. Spoofing; Tampering; Repudiation; Information Disclosure; Denial of Service; Privilege Elevation

C. Spoofing, Tampering, Repudiation, Data Disclosure, Denial of Service, Elevation of Privilege

D. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Privilege Elevation

In threat modeling, STRIDE refers to six categories of security threats used to categorize and reason about risks systematically. The canonical expansion is Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege. This exact phrasing is why that option is the best match: it uses the standard terms, including Information Disclosure (not Data Disclosure) and Elevation of Privilege (not Privilege Elevation). The other choices differ only in wording or order, but they don't align with the widely adopted STRIDE names. Knowing STRIDE helps you map attacker goals to concrete threats— impersonating users, altering data, denying accountability, leaking information, taking down services, or obtaining higher access.

5. Given r = range(1, 10) and num = int(input()), which value prints 'The number input is in the range from 1 and 10'?

A. The number input is in the range from 1 and 10.

B. The number input is not in the range from 1 and 10.

C. The number input is between 1 and 9 inclusive.

D. The number input is out of range.

The key idea is how Python defines range boundaries. range(1, 10) includes numbers starting at 1 up to, but not including, 10. So the valid values are 1 through 9. If your code prints the message about being in the range only when the input is actually in the range, then an input like 10 would not satisfy that condition and would trigger the message that the number is not in the range. That matches the option stating not in the range. In short, 10 is outside the range 1–9, so the not-in-range message is printed, which is why that option is correct.

6. In the grant_permission function, when result is False, what permission is assigned to the file?

A. Read permission for owner, group, and others

B. Read, write, execute for owner only

C. No permissions

D. Read and write for all

The main idea is to use a safe, minimal permission when the attempted grant doesn't succeed. If the grant operation fails, the function falls back to giving everyone read access. This means the file is still viewable by the owner, the group, and others, but cannot be modified or executed. Granting read for all is a conservative default that preserves accessibility without opening the door to changes or runs that could cause security or integrity issues. This is preferable to giving no permissions, which would block access entirely, or to granting write or execute rights to some users, which would increase risk or violate the intended access level when the initial grant couldn't be completed. Granting read for all provides a balanced, non-destructive fallback that keeps the file usable in typical workflows.

7. The Celsius to Fahrenheit function uses an assertion. What condition does this assertion enforce?

A. Non-negative Temperature

B. Temperature must be an integer

C. Output must be Fahrenheit

D. Inputs and outputs must be transformed atomically

It's about validating the input the function will accept. An assertion here is used to enforce the allowed domain of input values, ensuring the function only runs when the input meets a certain condition. In this case, the assertion requires the input temperature to be non-negative. This means the function is designed to handle temperatures at or above 0 degrees Celsius, perhaps because the implementation uses an unsigned numeric type or follows a specific constraint of the system. This is the best fit because the conversion formula itself will produce a valid Fahrenheit value for any real Celsius input, including negatives. The assertion isn't about the output unit (Fahrenheit is already the intended output by definition), nor does it require the input to be an integer, and it isn't about atomicity of transformations.

8. What is the primary defense against log injection attacks?

A. Sanitize outbound log messages

B. Validate input fields

C. Encrypt log files

D. Disable logging

Log injection attacks happen when untrusted input is written into log files in a way that can alter the log's structure or create fake entries. Sanitizing outbound log messages is the best defense because it neutralizes any problematic content before it's written. By escaping or encoding dangerous characters and removing or neutralizing newlines, carriage returns, tabs, or other control sequences, you ensure that data coming from users cannot break the log format or be used to insert misleading entries. This protection is applied exactly where the threat manifests—at the point of logging—so even if the data itself is untrusted, the resulting log remains trustworthy and parseable. Input validation is important for many security concerns, but it doesn't guarantee safe logging by itself, since content can pass through multiple layers before being logged. Encrypting log files helps with confidentiality and integrity after the fact, but it doesn't stop the possibility of log-format manipulation occurring during entry creation. Disabling logging would eliminate the risk of log injection, but it defeats the purpose of having logs for auditing and troubleshooting. A practical defense, often complemented by structured logging with a fixed schema, is to sanitize and properly encode log data to maintain a clean, reliable audit trail.

9. 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.

10. What are security controls and provide examples in software?

A. Security controls are decorative UI elements.

B. Security controls are measures to reduce risk. Examples: authentication, authorization, encryption, input validation, logging, and secure communications.

C. Security controls are only physical devices.

D. Security controls replace the need for secure coding.

Security controls are the measures built into a software system to reduce risk by preventing, detecting, or responding to threats. In software, they include authentication to verify identity, authorization to enforce permissions, encryption to protect data at rest and in transit, input validation to block malformed or malicious data, logging to monitor activity and support incident response, and secure communications to ensure data integrity and confidentiality over networks. These controls work together to limit exposure so that even when a vulnerability exists, exploitation is harder and the potential impact is smaller. The other options don't fit because decorative UI elements don't address risk, physical devices alone aren't the primary form of software controls, and relying on secure coding alone doesn't replace the need for ongoing protective measures.

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!