University of Central Florida (UCF) CIS3360 Security in Computing Final Practice Exam (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. **Remote File Inclusion (RFI) attacks exploit which PHP function?**

   A. require_once

   B. include

   C. open_url

   D. fetch_file

2. **In the context of security measures, what does the term "vulnerabilities" refer to?**

   A. The physical strength of an organization's network

   B. Weaknesses that can be exploited by attackers

   C. Access control settings that are too strict

   D. Non-compliance with industry regulations

3. **Which of the following is an exclusive right provided by a patent?**

   A. The right to modify the invention

   B. The right to sell the invention for 20 years

   C. The right to license the invention to others

   D. All of the above

4. **Which language is typically used for querying databases?**

   A. Data Manipulation Language (DML)

   B. Structured Query Language (SQL)

   C. Hypertext Markup Language (HTML)

   D. JavaScript

5. **What doctrine allows for various uses of copyrighted works without requiring permission?**

   A. Fair Use Doctrine

   B. Public Domain Doctrine

   C. First Sale Doctrine

   D. Transformative Use Doctrine

6. What action should be taken regularly to protect against vulnerabilities?

- **A. Ignore security warnings**
- **B. Change passwords**
- **C. Expand network access**
- **D. Disable antivirus software**

7. What type of malicious content is typically uploaded in Local File Inclusion (LFI) vulnerabilities?

- **A. Image Files**
- **B. Executable Programs**
- **C. Malicious Code**
- **D. HTML Files**

8. Data in databases is usually stored in which structure?

- **A. Files**
- **B. Tables**
- **C. Folders**
- **D. Entries**

9. What is the significance of multi-factor authentication?

- **A. It eliminates all security risks related to online access**
- **B. It enhances security by requiring multiple verification factors**
- **C. It simplifies the process of password recovery**
- **D. It allows for a single password to protect multiple accounts**

10. Name one common method used in phishing attacks.

- **A. Creating secure websites**
- **B. Sending fraudulent emails to trick users**
- **C. Implementing multi-factor authentication**
- **D. Using secure servers**

Answers

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

Explanations

1. Remote File Inclusion (RFI) attacks exploit which PHP function?

A. require_once

B. include

C. open_url

D. fetch_file

Remote File Inclusion (RFI) attacks primarily exploit the 'include' function in PHP. This function is designed to include and evaluate a specified file in the execution of the script. When user input is not properly sanitized, an attacker can manipulate the URL or input to include a malicious file from a remote server. This is dangerous because if the attacker succeeds, they can execute arbitrary code on the target server, leading to a full compromise of the application or even the server itself. The inclusion of files located on a remote server circumvents local security controls and can allow attackers to bypass restrictions that might protect the system from executing malicious code locally. This makes the 'include' function particularly vulnerable in scenarios where user input is not properly controlled. The other functions listed do not have the same inherent risk for RFI, which is why they are not the correct choice.

2. In the context of security measures, what does the term "vulnerabilities" refer to?

A. The physical strength of an organization's network

B. Weaknesses that can be exploited by attackers

C. Access control settings that are too strict

D. Non-compliance with industry regulations

The term "vulnerabilities" in the context of security measures specifically refers to weaknesses in a system, network, or application that can be exploited by attackers to gain unauthorized access, disrupt services, or cause harm to assets. Identifying and understanding these vulnerabilities is crucial for developing effective security strategies that can protect systems from potential threats. By recognizing vulnerabilities, organizations can implement appropriate security controls, conduct risk assessments, and establish preventative measures to mitigate the risks of exploitation. This concept serves as the foundation of security practices, as it highlights the need to strengthen defensive measures against potential breaches that could compromise sensitive information or systems. The other options, while they touch on aspects of security, do not accurately define vulnerabilities. They focus on physical aspects, access control, or compliance, which, although important, do not capture the essence of what vulnerabilities represent in the broader context of cybersecurity.

3. Which of the following is an exclusive right provided by a patent?

A. The right to modify the invention

B. The right to sell the invention for 20 years

C. The right to license the invention to others

D. All of the above

A patent grants the inventor a set of exclusive rights, which are designed to protect the intellectual property associated with an invention. This means that the inventor has the authority to control how their invention is used, reproduced, and distributed. The right to modify the invention refers to the inventor's ability to make changes or improvements to their creation. This is important because it allows the inventor to refine their invention without fear of infringement from others. The right to sell the invention for 20 years indicates that the patent holder can commercially exploit their invention for two decades, preventing others from selling or manufacturing the patented invention without permission. This time frame is established to encourage innovation while eventually allowing the public to benefit from the invention once the patent expires. Furthermore, the right to license the invention to others provides a means for the patent holder to generate income by allowing third parties to use their invention under specified conditions. This can be a vital part of a patent strategy, as it can lead to partnerships and expanded market reach. Since all of these rights — modification, sale, and licensing — are inherently included in a patent's exclusivity, the comprehensive nature of the rights confirms that option "All of the above" is indeed correct.

4. Which language is typically used for querying databases?

A. Data Manipulation Language (DML)

B. Structured Query Language (SQL)

C. Hypertext Markup Language (HTML)

D. JavaScript

Structured Query Language (SQL) is the standard programming language specifically designed for managing and manipulating relational databases. It allows users to perform various operations such as querying data, updating records, inserting new data, and deleting existing records. SQL provides a set of commands that facilitate these tasks in a structured manner, making it easier to interact with the database and retrieve the information required for various applications. While Data Manipulation Language (DML) is a subset of SQL that focuses on data manipulation, it does not encompass the full range of features and functionalities that SQL offers. Hypertext Markup Language (HTML) is primarily used for creating and structuring content on the web, not for querying databases. JavaScript, although frequently used for enhancing interactivity on web pages, is not specifically tailored for database queries. Hence, SQL is recognized as the appropriate and dedicated language for querying databases, making it the correct choice for this question.

5. What doctrine allows for various uses of copyrighted works without requiring permission?

A. Fair Use Doctrine

B. Public Domain Doctrine

C. First Sale Doctrine

D. Transformative Use Doctrine

The Fair Use Doctrine is an essential legal principle that permits limited use of copyrighted material without needing to obtain permission from the copyright owner. This doctrine is crucial because it balances the interests of copyright holders with the public interest in the dissemination of knowledge and information. Fair use is often applied in specific contexts, such as criticism, comment, news reporting, teaching, and scholarship. Factors that are considered when determining whether a use qualifies as fair include the purpose and character of the use (commercial or educational), the nature of the copyrighted work, the amount and substantiality of the portion used, and the effect of the use on the market for the original work. In contrast, the Public Domain Doctrine pertains to works that are no longer protected by copyright and can be used freely by anyone. The First Sale Doctrine allows the owner of a lawfully acquired copyrighted work to resell or distribute that work after purchase, but it does not permit new uses of the work without permission. Transformative Use, while relevant within the context of fair use by allowing modifications, is not a standalone doctrine like fair use. Thus, the Fair Use Doctrine stands out as the correct answer, as it specifically grants the authority for various uses of copyrighted works without requiring prior permission.

6. What action should be taken regularly to protect against vulnerabilities?

A. Ignore security warnings

B. Change passwords

C. Expand network access

D. Disable antivirus software

Changing passwords regularly is a crucial action to protect against vulnerabilities because it helps mitigate the risk of unauthorized access to sensitive information. Regular password updates reduce the window of opportunity for attackers who may have acquired passwords through various means, such as phishing, keylogging, or breaches of other services. This practice not only ensures that an account remains secure over time but also encourages the use of unique, complex passwords that further enhance security. In addition, regularly changing passwords can help individuals or organizations identify any potentially compromised accounts sooner rather than later. It is generally recommended to follow best practices, such as creating strong passwords that combine letters, numbers, and special characters and utilizing password managers to maintain unique passwords for different accounts. The other options do not contribute to effective security practices. Ignoring security warnings can lead to exposure to threats; expanding network access may increase the risk of attacks; and disabling antivirus software leaves systems vulnerable to malicious software. Each of these actions counteracts the goal of maintaining a secure computing environment.

7. What type of malicious content is typically uploaded in Local File Inclusion (LFI) vulnerabilities?

A. Image Files

B. Executable Programs

C. Malicious Code

D. HTML Files

Local File Inclusion (LFI) vulnerabilities occur when a web application allows users to include files from the server's file system without proper validation. This exploitation enables an attacker to traverse directories and include files that should not be accessible to the user, often leading to severe security breaches. The most commonly uploaded malicious content in the context of LFI vulnerabilities is malicious code. This is because the attacker can include files that contain code, such as PHP scripts or other server-side scripts, and execute that code on the server. This can lead to remote code execution, unauthorized access to sensitive information, or manipulation of server-side logic. While executable programs, image files, and HTML files could be relevant in different contexts, they do not serve the same immediate purpose as malicious code in LFI scenarios. Malicious code is specifically crafted to carry out harmful actions, which aligns directly with the goals of attackers exploiting LFI vulnerabilities.

8. Data in databases is usually stored in which structure?

A. Files

B. Tables

C. Folders

D. Entries

The data in databases is typically organized in tables, which consist of rows and columns. This tabular format allows for efficient data management and retrieval. Each table represents a specific entity, such as customers or products, where each row corresponds to a unique record and each column represents an attribute of that record. Using tables enables relational databases to utilize powerful querying languages, such as SQL, which can manipulate and retrieve data from multiple tables using relationships defined between them. This structured approach not only facilitates easier data management and organization but also enhances data integrity and reduces redundancy. On the other hand, files may refer to various types of data storage but do not inherently provide the structured organization that tables do. Folders are primarily used for storing files in a hierarchy and do not organize data in a way conducive for relational database operations. Entries, while they can refer to individual data points within a table, do not encompass the broader organizational structure that tables provide.

9. What is the significance of multi-factor authentication?

A. It eliminates all security risks related to online access

B. It enhances security by requiring multiple verification factors

C. It simplifies the process of password recovery

D. It allows for a single password to protect multiple accounts

Multi-factor authentication (MFA) is significant because it enhances security by requiring multiple verification factors before granting access to an account or system. This approach adds an additional layer of defense beyond just a password, which is traditionally the sole factor for authentication. In more detail, MFA typically involves a combination of something the user knows (like a password), something the user has (like a smartphone or a hardware token), and something the user is (like a fingerprint or other biometric verification). By requiring these multiple factors, even if one factor, such as a password, is compromised, an attacker would still need to overcome the additional barriers to gain access. This significantly reduces the likelihood of unauthorized access and helps protect sensitive data against various threats like phishing attacks, credential theft, and brute-force attempts. Other options do not accurately reflect the essence of what multi-factor authentication provides. For example, while MFA increases security, it does not eliminate all risks associated with online access, as there are always potential vulnerabilities that can be exploited. Similarly, MFA does not simplify the password recovery process or facilitate the use of a single password for multiple accounts, as its primary focus is on enhancing security through verification diversity rather than streamlining user convenience in those areas.

10. Name one common method used in phishing attacks.

A. Creating secure websites

B. Sending fraudulent emails to trick users

C. Implementing multi-factor authentication

D. Using secure servers

Sending fraudulent emails to trick users is a foundational technique used in phishing attacks. This method typically involves attackers crafting messages that appear to come from legitimate sources, such as banks, online services, or even colleagues, with the intent of deceiving recipients into revealing sensitive information like passwords or credit card numbers. The emails often include urgent requests for action, deceptive links, or attachments that may contain malware. The effectiveness of this method lies in its ability to exploit human psychology, such as the fear of account suspension or the lure of urgent offers, prompting users to act without due diligence. Recognizing and understanding this method is crucial for strengthening awareness and defenses against phishing threats. Other options like creating secure websites, implementing multi-factor authentication, and using secure servers involve protective measures that can help mitigate phishing risks but do not constitute methods employed by attackers in the phishing process itself.

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://ucf-cis3360-final.examzify.com

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