PCI APPROVED SCANNING VENDOR (ASV) ONLINE PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://pciasvonline.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. **Which mitigation technique is commonly used to defend against cross-site scripting (XSS)?**

   A. Input validation and output encoding

   B. Relying on client-side scripting

   C. Storing passwords in plaintext

   D. Disable all JavaScript on clients

2. **Which of the following vulnerabilities would cause an automatic failure?**

   A. Cross-site scripting (XSS) flaws

   B. Directory traversal on web server

   C. Default or built-in accounts with default passwords

   D. Rootkits

3. **Which statement accurately describes SSL usage on host devices in PCI scanning?**

   A. Any form of SSL on a host device is an automatic failure, with the exception for POS devices that can prove no downgrade vulnerability.

   B. SSL on host devices is always allowed if the device is PCI-compliant.

   C. POS devices are never subject to SSL restrictions.

   D. SSL usage on host devices is unrelated to PCI scope.

4. **In the Overall Scan Results, what information is not included?**

   A. IP addresses

   B. Pass/fail status

   C. Date for scan expiration

   D. Number of components scanned

5. **Insecure direct object references and directory traversal are examples of which vulnerability category?**

   A. Cross-site scripting

   B. Improper access control

   C. CSRF

   D. Broken authentication

6. What are the 3 sections of the CVSS Environmental, Impact Subscore Modifiers Metric?

A. Confidentiality Requirement; Integrity Requirement; Availability Requirement

B. Confidentiality Impact; Integrity Impact; Availability Impact

C. Access Vector; Attack Complexity; Privileges Required

D. Confidentiality Requirement; Integrity; Availability

7. Which frequency is required for external vulnerability scans?

A. Quarterly.

B. Monthly.

C. Semiannually.

D. Annually.

8. What is the primary goal of monitoring and alerting in the cardholder data environment?

A. To store logs for audit purposes only.

B. To increase data throughput.

C. To alert personnel to suspected compromises.

D. To encrypt data at rest.

9. Which standard addresses the protection of sensitive data at the point of interaction devices and their cryptographic keys used with that protection?

A. PCI PTS - PIN Security

B. PCI PTS - POI

C. PCI PTS - HSM

D. PCI Card Production

10. What action is recommended for any required services, protocols, or daemons that are insecure?

A. Do not configure additional security features for insecure services

B. Implement additional security features for any required services, protocols, or daemons considered insecure

C. Remove all insecure services the moment they appear in logs

D. Ignore the risk of insecure services

Answers

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

Explanations

1. Which mitigation technique is commonly used to defend against cross-site scripting (XSS)?

A. Input validation and output encoding

B. Relying on client-side scripting

C. Storing passwords in plaintext

D. Disable all JavaScript on clients

Cross-site scripting is prevented by controlling untrusted input and how it's rendered in a browser. The most effective and commonly used defense is to validate inputs to reject dangerous content and to encode data on output so anything potentially harmful is treated as text rather than executable code. Input validation reduces the amount of unsafe data that can enter the system, while output encoding neutralizes data when it's displayed by transforming characters like <, >, &, and quotes into safe HTML entities. The right encoding depends on the context—HTML content needs HTML entity encoding, URLs need URL encoding, and data injected into scripts or attributes requires context-appropriate escaping. Together with broader safeguards like content security policies and proper data sanitization, this approach provides solid protection against XSS. Relying on client-side scripting alone isn't enough because security controls must be enforced on the server and validated by the browser; storing passwords in plaintext has nothing to do with preventing XSS and creates other serious risks; disabling JavaScript on clients is impractical and would break legitimate functionality while not reliably stopping XSS.

2. Which of the following vulnerabilities would cause an automatic failure?

A. Cross-site scripting (XSS) flaws

B. Directory traversal on web server

C. Default or built-in accounts with default passwords

D. Rootkits

Automatic failure happens when a vulnerability reveals a baseline security control failure that is universally unacceptable. Default or built-in accounts with default passwords are such a case because those credentials are widely known and easily exploited across many systems. PCI DSS requires disabling or changing default accounts and using unique, strong passwords, so having defaults present means the environment is immediately insecure and fails the assessment regardless of other issues. The other vulnerabilities are serious and require fixes, but they depend on context and remediation steps; they aren't universally disqualifying in the same automatic way as default credentials.

3. Which statement accurately describes SSL usage on host devices in PCI scanning?

A. Any form of SSL on a host device is an automatic failure, with the exception for POS devices that can prove no downgrade vulnerability.

B. SSL on host devices is always allowed if the device is PCI-compliant.

C. POS devices are never subject to SSL restrictions.

D. SSL usage on host devices is unrelated to PCI scope.

SSL on host devices is treated as a red flag in PCI scanning because cardholder data must be protected with strong cryptography and legacy protocols like SSL are not considered acceptable for protecting data in transit. When a host device uses SSL, it often signals the presence of weak or deprecated encryption (or a potential downgrade path), which ASV scans flag as a failure. The only exception is POS devices, which may be allowed to use SSL if they can prove there is no downgrade vulnerability—meaning they won't expose data through weaker protocols or older TLS versions. In short, strong, up-to-date encryption is required across the environment, and SSL usage on host devices is not permitted unless a POS device can demonstrate it isn't vulnerable to downgrades.

4. In the Overall Scan Results, what information is not included?

A. IP addresses

B. Pass/fail status

C. Date for scan expiration

D. Number of components scanned

In an Overall Scan Results view, you get a quick, high-level snapshot of the scan: whether the scan passed or failed, when the current scan results expire (so you know when to rescan for compliance), and how many components were included in the assessment. The specific IP addresses of the scanned hosts aren't shown in this summary; you'd see those details in the per-host or detailed results if you need them. This keeps the overview focused on outcome, timing, and scope, which is what you need to gauge compliance quickly. So, the information not included in the Overall Scan Results is the IP addresses.

5. Insecure direct object references and directory traversal are examples of which vulnerability category?

A. Cross-site scripting

B. Improper access control

C. CSRF

D. Broken authentication

These examples show a failure to enforce proper authorization for accessing resources. Insecure direct object references occur when an app exposes direct references to internal objects (like IDs) and doesn't verify that the requester is allowed to access that object; changing the reference can reveal or modify data the user shouldn't see. Directory traversal likewise lets an attacker manipulate file paths to reach restricted files outside the intended directory, bypassing access checks. Both highlight weaknesses in controlling who can access what, which is the essence of improper access control. The other options describe different issues: cross-site scripting involves injecting scripts into pages, CSRF tricks a user into performing unintended actions, and broken authentication concerns weaknesses in login or session management.

6. What are the 3 sections of the CVSS Environmental, Impact Subscore Modifiers Metric?

A. Confidentiality Requirement; Integrity Requirement; Availability Requirement

B. Confidentiality Impact; Integrity Impact; Availability Impact

C. Access Vector; Attack Complexity; Privileges Required

D. Confidentiality Requirement; Integrity; Availability

In CVSS, the Environmental metrics include modifiers that tailor the impact of a vulnerability to a specific environment. The three sections that make up the Impact Subscore Modifiers are Confidentiality Requirement, Integrity Requirement, and Availability Requirement. These modifiers indicate how critical each security property is to the organization, and they adjust the impact score accordingly (for example, making confidentiality more or less impactful depending on how important it is in that environment). The other options mix up terms from different parts of CVSS: one lists the actual impact metrics (Confidentiality Impact, Integrity Impact, Availability Impact) rather than the environmental modifiers; another lists exploitability factors (Access Vector, Attack Complexity, Privileges Required); and the last option blends some correct terms with missing wording (Integrity and Availability without the "Requirement" qualifier).

7. Which frequency is required for external vulnerability scans?

A. Quarterly.

B. Monthly.

C. Semiannually.

D. Annually.

External vulnerability scans must be done at least every quarter by an Approved Scanning Vendor. This quarterly cadence ensures that publicly exposed systems are regularly checked for newly discovered vulnerabilities, keeping the assessment current without requiring monthly scans. Performing scans more often than quarterly isn't the standard minimum, while semiannual or annual frequencies would leave longer gaps where vulnerabilities could go undetected. Additionally, after any significant change to the network, a re-scan is required to verify that new changes haven't introduced unaddressed weaknesses.

8. What is the primary goal of monitoring and alerting in the cardholder data environment?

A. To store logs for audit purposes only.

B. To increase data throughput.

C. To alert personnel to suspected compromises.

D. To encrypt data at rest.

Monitoring and alerting focus on detecting security events in the cardholder data environment and notifying the right people so they can respond quickly. This quick notification enables containment and remediation before an attacker can cause significant damage or exfiltrate data. Logs and data are collected to support ongoing visibility and incident response, but their primary purpose in this context is to drive timely alerts and actions, not just to store information for audits. Increasing data throughput isn't related to detecting and responding to incidents, and encrypting data at rest is about protecting data's confidentiality, not about real-time detection. The point of monitoring and alerting is to recognize suspected compromises as soon as they happen and initiate a rapid response to protect cardholder data.

9. Which standard addresses the protection of sensitive data at the point of interaction devices and their cryptographic keys used with that protection?

A. PCI PTS - PIN Security

B. PCI PTS - POI

C. PCI PTS - HSM

D. PCI Card Production

This question tests understanding of which PCI PTS standard covers protecting sensitive data at the point of interaction devices and the cryptographic keys used with that protection. Point of Interaction devices include card readers and PIN pads where data is captured in the moment of payment. The PCI PTS standard for POI specifically sets security requirements for these devices, including how they protect sensitive data on the device and how cryptographic keys are managed and safeguarded there. It also covers aspects like secure key injection and tamper-resistant hardware, which are essential for maintaining data integrity right at the device level. This focus differentiates it from PIN Security, which centers on PIN data handling itself, and from HSM, which relates to secure back-end cryptographic processors rather than the on-device protection at the point of interaction. Card Production governs secure card manufacturing rather than on-device data protection.

10. What action is recommended for any required services, protocols, or daemons that are insecure?

A. Do not configure additional security features for insecure services

B. Implement additional security features for any required services, protocols, or daemons considered insecure

C. Remove all insecure services the moment they appear in logs

D. Ignore the risk of insecure services

When a required service, protocol, or daemon is insecure, you don't abandon it or ignore the risk. The proper approach is to add compensating controls to reduce the risk so the service can remain in use without exposing the environment to heightened threats. This means implementing additional security features and safeguards around that service, such as enabling strong encryption for communications (for example, TLS with up-to-date ciphers), enforcing strong authentication, applying the latest patches and secure configurations, disabling deprecated options, restricting access with firewalls and precise access controls, and enhancing monitoring and logging. You may also segment the network to limit exposure and implement controls like rate limiting or intrusion detection where appropriate. The goal is to bring the overall risk to an acceptable level while still meeting operational needs. Removing or ignoring insecure services would either disrupt operations or leave the system vulnerable, which is not acceptable.

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://pciasvonline.examzify.com

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