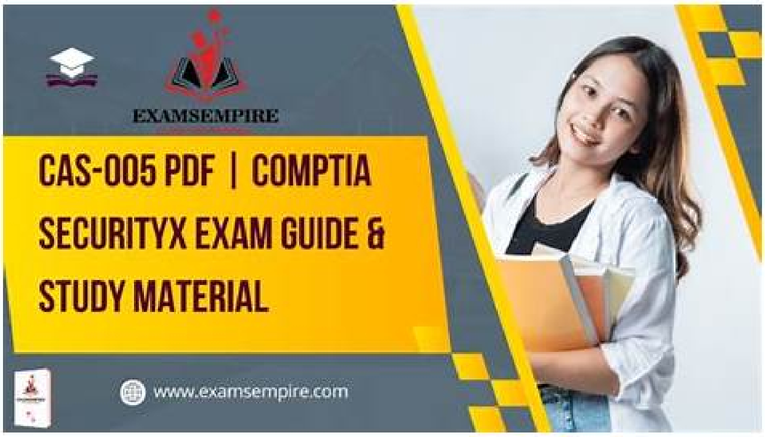
# 100% Pass Quiz 2026 CAS-005: CompTIA SecurityX Certification Exam Updated Detail Explanation



P.S. Free 2026 CompTIA CAS-005 dumps are available on Google Drive shared by Actual4dump: https://drive.google.com/open?id=1NQUwtMftW02a5hUvsDS7r3o5I4ydiVe3

It is a common sense that in terms of a kind of CompTIA SecurityX Certification Exam test torrent, the pass rate would be the best advertisement, since only the pass rate can be the most powerful evidence to show whether the CAS-005 Guide Torrent is effective and useful or not. We are so proud to tell you that according to the statistics from the feedback of all of our customers, the pass rate among our customers who prepared for the exam under the guidance of our CompTIA SecurityX Certification Exam test torrent has reached as high as 98%to 100%, which definitely marks the highest pass rate in the field. Therefore, you can carry out the targeted training to improve yourself in order to make the best performance in the real exam, most importantly, you can repeat to do the situation test as you like.

## CompTIA CAS-005 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Governance, Risk, and Compliance: This section of the exam measures the skills of CompTIA security architects that cover the implementation of governance components based on organizational security requirements, including developing policies, procedures, and standards. Candidates will learn about managing security programs, including awareness training on phishing and social engineering. |
| Topic 2 | • Security Operations: This domain is designed for CompTIA security architects and covers analyzing data to support monitoring and response activities, as well as assessing vulnerabilities and recommending solutions to reduce attack surfaces. Candidates will apply threat-hunting techniques and utilize threat intelligence concepts to enhance operational security. |
| Topic 3 | • Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems. |
| Topic 4 | • Security Engineering: This section measures the skills of CompTIA security architects that involve troubleshooting common issues related to identity and access management (IAM) components within an enterprise environment. Candidates will analyze requirements to enhance endpoint and server security while implementing hardware security technologies. This domain also emphasizes the importance of advanced cryptographic concepts in securing systems. |

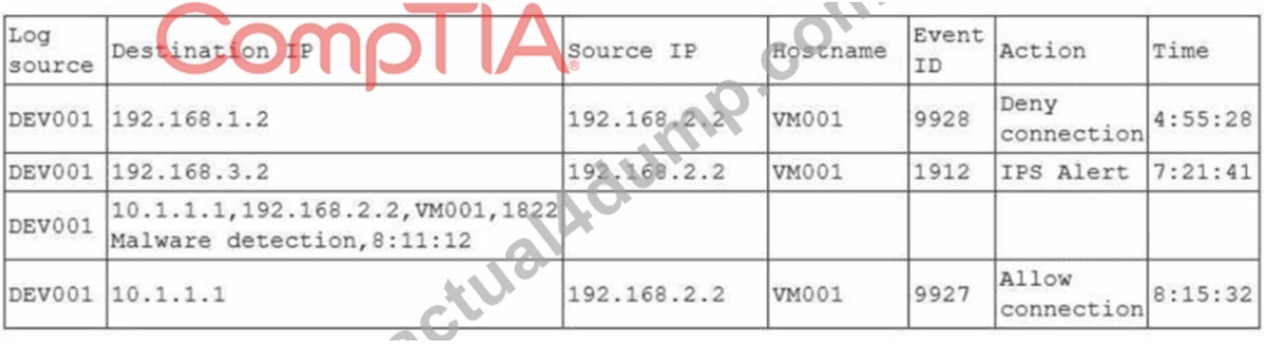
**>> CAS-005 Detail Explanation <<**

## New CAS-005 Dumps Files - Test CAS-005 Pattern

As an experienced exam dumps provider, our website offers you most reliable CompTIA real dumps and study guide. We offer customer with most comprehensive CAS-005 exam pdf and the guarantee of high pass rate. The key of our success is to constantly provide the best quality CAS-005 Dumps Torrent with the best customer service.

## CompTIA SecurityX Certification Exam Sample Questions (Q168-Q173):

**NEW QUESTION # 168**
A security analyst is reviewing a SIEM and generates the following report:



| Log source | Destination IP | Source IP | Hostname | Event ID | Action | Time |
|---|---|---|---|---|---|---|
| DEV001 | 192.168.1.2 | 192.168.2.2 | VM001 | 9928 | Deny connection | 4:55:28 |
| DEV001 | 192.168.3.2 | 192.168.2.2 | VM001 | 1912 | IPS Alert | 7:21:41 |
| DEV001 | 10.1.1.1,192.168.2.2,VM001,1822<br>Malware detection,8:11:12 | | | | | |
| DEV001 | 10.1.1.1 | 192.168.2.2 | VM001 | 9927 | Allow connection | 8:15:32 |

Later, the incident response team notices an attack was executed on the VM001 host. Which of the following should the security analyst do to enhance the alerting process on the SIEM platform?

- A. Perform a log correlation on the SIEM solution.
- B. Create a new rule set to detect malware.
- C. Improve parsing of data on the SIEM.
- D. Include the EDR solution on the SIEM as a new log source.

**Answer: A**

Explanation:
The SIEM already contains multiple events that, if correlated, would have indicated an active attack sequence on VM001-such as denied connections, IPS alerts, malware detection, and then an allowed connection. CAS-005 Security Operations objectives emphasize log correlation as a way to enhance detection by linking related events across different time stamps and data sources into a single, higher-confidence alert.
Option A (adding EDR logs) could add visibility but does not address the need to connect existing events for earlier detection.
Option C (improving parsing) ensures readability but does not create actionable alerts.
Option D (creating a new malware detection rule) is redundant since malware detection already appeared in logs; the issue was the lack of correlation to act on it in time.
By correlating IDS, IPS, firewall, and malware detection logs, the SIEM can raise a higher-priority alert before the attack is completed.

**NEW QUESTION # 169**
An organization has been using self-managed encryption keys rather than the free keys managed by the cloud provider. The Chief Information Security Officer (CISO) reviews the monthly bill and realizes the self-managed keys are more costly than anticipated. Which of the following should the CISO recommend to reduce costs while maintaining a strong security posture?

- A. Begin using cloud-managed keys on all new resources deployed in the cloud.
- B. Adjust the configuration for cloud provider keys on data that is classified as public.
- C. Extend the key rotation period to one year so that the cloud provider can use cached keys.
- D. Utilize an on-premises HSM to locally manage keys.

**Answer: B**

Explanation:
Comprehensive and Detailed Step by Step
Understanding the Scenario: Theorganization is using customer-managed encryption keys in the cloud, which is more expensive than using the cloud provider's free managed keys. The CISO needs to find a way to reduce costs without significantly weakening the security posture.
Analyzing the Answer Choices:
A :Utilize an on-premises HSM to locally manage keys: While on-premises HSMs offer strong security, they introduce additional costs and complexity (procurement, maintenance, etc.). This option is unlikely to reduce costs compared to cloud-based key

management.
B :Adjust the configuration for cloud provider keys on data that is classified as public: This is the most practical and cost-effective approach. Data classified as public doesn't require the same level of protection as sensitive data. Using the cloud provider's free managed keys for public data can significantly reduce costs without compromising security, as the data is intended to be publicly accessible anyway.
Reference:
C : Begin using cloud-managed keys on all new resources deployed in the cloud: While this would reduce costs, it's a broad approach that doesn't consider the sensitivity of the data. Applying cloud-managed keys to sensitive data might not be acceptable from a security standpoint.
D : Extend the key rotation period to one year so that the cloud provider can use cached keys: Extending the key rotation period weakens security. Frequent key rotation is a security best practice to limit the impact of a potential key compromise.
Risk-Based Approach: Using cloud-provider-managed keys for public data is a reasonable risk-based decision. Public data, by definition, is not confidential.
Cost Optimization: This directly addresses the CISO's concern about cost, as cloud-provider-managed keys are often free or significantly cheaper.
Security Balance: It maintains a strong security posture for sensitive data by continuing to use customer-managed keys where appropriate, while optimizing costs for less sensitive data.
CASP+ Relevance: This approach demonstrates an understanding of risk management, data classification, and cost-benefit analysis in security decision-making, all of which are important topics in CASP+.
Elaboration on Data Classification:
Data Classification Policy: Organizations should have a clear data classification policy that defines different levels of data sensitivity (e.g., public, internal, confidential, restricted).
Security Controls Based on Classification: Security controls, including encryption key management, should be applied based on the data's classification level.
Cost-Benefit Analysis: Data classification helps organizations make informed decisions about where to invest in stronger security controls and where cost optimization is acceptable.
In conclusion, adjusting the configuration to use cloud-provider-managed keys for data classified as public is the most effective way to reduce costs while maintaining a strong security posture. It's a practical, risk-based approach that aligns with data classification principles and cost-benefit considerations, all of which are important concepts covered in the CASP+ exam objectives.

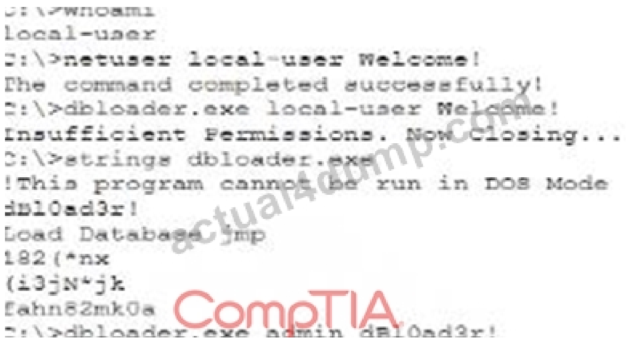
**NEW QUESTION # 170**
A systems engineer is configuring SSO for a business that will be using SaaS applications for its remote-only workforce. Privileged actions in SaaS applications must be allowed only from corporate mobile devices that meet minimum security requirements, but BYOD must also be permitted for other activity. Which of the following would best meet this objective?

- A. Block any connections from outside the business's network security boundary.
- B. Configure device attestations and continuous authorization controls.
- C. Deploy application protection policies using a corporate, cloud-based MDM solution.
- D. Install machine certificates on corporate devices and perform checks against the clients.

**Answer: B**

Explanation:
Device attestation ensures that only corporate-approved devices can perform privileged actions in SaaS applications. Continuous authorization monitors ongoing device compliance, dynamically adjusting permissions based on security posture.
* Blocking connections (A) is too restrictive and does not accommodate BYOD.
* Machine certificates (B) help with authentication but do not provide continuous security assessment.
* MDM policies (D) secure mobile devices but do not apply real-time access controls for SaaS applications.

**NEW QUESTION # 171**
Recent repents indicate that a software tool is being exploited Attackers were able to bypass user access controls and load a database. A security analyst needs to find the vulnerability and recommend a mitigation. The analyst generates the following output:



```
C:\>whoami
local-user
C:\>netuser local-user Welcome!
The command completed successfully!
C:\>dbloader.exe local-user Welcome!
Insufficient Permissions. Now Closing...
C:\>strings dbloader.exe
!This program cannot be run in DOS Mode
dBl0ad3r!
Load Database jmp
182(*nx
(i3jN*jk
fahn82mk0a
C:\>dbloader.exe admin dBl0ad3r!
```

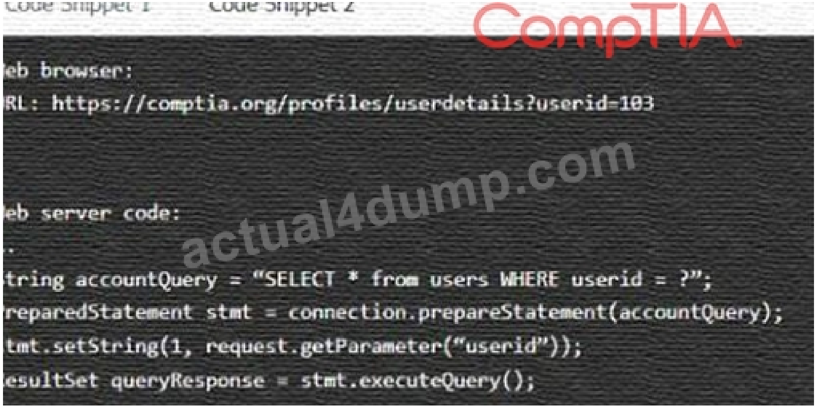
Which of the following would the analyst most likely recommend?

- A. Installing appropriate EDR tools to block pass-the-hash attempts
- B. Adding additional time to software development to perform fuzz testing
- C. Not allowing users to change their local passwords
- D. Removing hard coded credentials from the source code

**Answer: D**

Explanation:
The output indicates that the software tool contains hard-coded credentials, which attackers can exploit to bypass user access controls and load the database. The mostlikely recommendation is to remove hard-coded credentials from the source code. Here's why:
Security Best Practices: Hard-coded credentials are a significant security risk because they can be easily discovered through reverse engineering or simple inspection of the code. Removing them reduces the risk of unauthorized access.
Credential Management: Credentials should be managed securely using environment variables, secure vaults, or configuration management tools that provide encryption and access controls.
Mitigation of Exploits: By eliminating hard-coded credentials, the organization can prevent attackers from easily bypassing authentication mechanisms and gaining unauthorized access to sensitive systems.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
OWASP Top Ten: Insecure Design
NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations

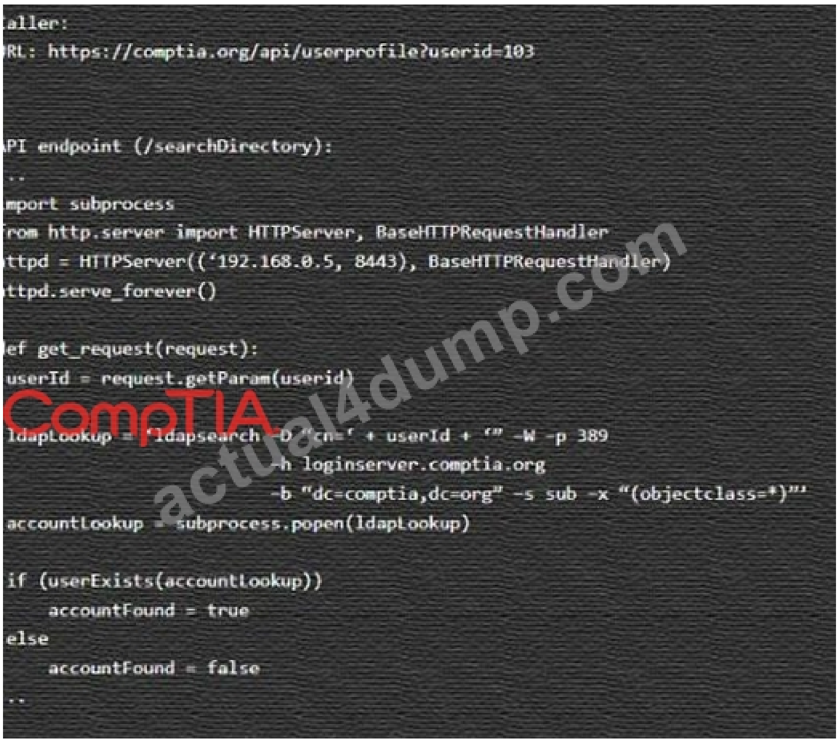
**NEW QUESTION # 172**
A product development team has submitted code snippets for review prior to release.
INSTRUCTIONS
Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.
Code Snippet 1



```
eb browser:
RL: https://comptia.org/profiles/userdetails?userid=103

eb server code:
.
tring accountQuery = "SELECT * from users WHERE userid = ?";
reparedStatement stmt = connection.prepareStatement(accountQuery);
tmt.setString(1, request.getParameter("userid"));
esultSet queryResponse = stmt.executeQuery();
```

Code Snippet 2



```
aller:
RL: https://comptia.org/api/userprofile?userid=103


PI endpoint (/searchDirectory):
..
mport subprocess
rom http.server import HTTPServer, BaseHTTPRequestHandler
ttpd = HTTPServer(('192.168.0.5, 8443), BaseHTTPRequestHandler)
ttpd.serve_forever()

ef get_request(request):
 userId = request.getParam(userid)

 ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                          -h loginserver.comptia.org
                          -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
 ..
```

Vulnerability 1:
SQL injection
Cross-site request forgery
Server-side request forgery
Indirect object reference
Cross-site scripting
Fix 1:
Perform input sanitization of the userid field.
Perform output encoding of queryResponse,
Ensure usex:ia belongs to logged-in user.
Inspect URLS and disallow arbitrary requests.
Implement anti-forgery tokens.
Vulnerability 2
1) Denial of service
2) Command injection
3) SQL injection
4) Authorization bypass
5) Credentials passed via GET
Fix 2
A) Implement prepared statements and bind
variables.
B) Remove the serve_forever instruction.
C) Prevent the "authenticated" value from being overridden by a GET parameter.
D) HTTP POST should be used for sensitive parameters.
E) Perform input sanitization of the userid field.

**Answer:**

Explanation:
See the solution below in explanation.
Explanation:
Code Snippet 1
Vulnerability 1: SQL injection
SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.
Fix 1: Perform input sanitization of the userid field.
Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the

database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.
Code Snippet 2
Vulnerability 2: Cross-site request forgery
Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.
Fix 2: Implement anti-forgery tokens.
Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti- forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

**NEW QUESTION # 173**
......

simulation tests of our CAS-005 learning materials have the functions of timing and mocking exams, which will allow you to adapt to the exam environment in advance and it will be of great benefit for subsequent exams. After you complete the learning task, the system of our CAS-005 test prep will generate statistical reports based on your performance so that you can identify your weaknesses and conduct targeted training and develop your own learning plan. For the complex part of our CAS-005 Exam Question, you may be too cumbersome, but our system has explained and analyzed this according to the actual situation to eliminate your doubts and make you learn better.