



CS0-001^{Q&As}

CompTIA Cybersecurity Analyst

Pass CompTIA CS0-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4lead.com/cs0-001.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

A security incident has been created after noticing unusual behavior from a Windows domain controller. The server administrator has discovered that a user logged in to the server with elevated permissions, but the user's account does not follow the standard corporate naming scheme. There are also several other accounts in the administrators group that do not follow this naming scheme. Which of the following is the possible cause for this behavior and the BEST remediation step?

- A. The Windows Active Directory domain controller has not completed synchronization, and should force the domain controller to sync.
- B. The server has been compromised and should be removed from the network and cleaned before reintroducing it to the network.
- C. The server administrator created user accounts cloning the wrong user ID, and the accounts should be removed from administrators and placed in an employee group.
- D. The naming scheme allows for too many variations, and the account naming convention should be updated to enforce organizational policies.

Correct Answer: D

QUESTION 2

Given the following access log:

```
access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /js/query-ui/js/?a.aspectRatio:this.originalSize.height%7c%7c%3ba=e(HTTP/1.1" 403 22  
access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /js/query-ui/js/?a.aspectRatio:this.originalSize.height | | 1;a=e( HTTP/1.1" 303 333  
access_log: 10.1.1.3 - -[66.66.132.6 -100] "Get /scripts/query-ui/js/J);F.optgroup=F .option:F .tbody=F .tfoot=F .colorgroup=F .caption=F .thead:F .td;if (!c.support.htmlSerialize)F._default=(1, HTTP/1.1" 403 338
```

Which of the following accurately describes what this log displays?

- A. A vulnerability in jQuery
- B. Application integration with an externally hosted database
- C. A vulnerability scan performed from the Internet
- D. A vulnerability in Javascript

Correct Answer: C

QUESTION 3

During a quarterly review of user accounts and activity, a security analyst noticed that after a password reset the head



of human resources has been logging in from multiple external locations, including several overseas. Further review of the account showed access rights to a number of corporate applications, including a sensitive accounting application used for employee bonuses. Which of the following security methods could be used to mitigate this risk?

- A. RADIUS identity management
- B. Context-based authentication
- C. Privilege escalation restrictions
- D. Elimination of self-service password resets

Correct Answer: B

QUESTION 4

A computer at a company was used to commit a crime. The system was seized and removed for further analysis. Which of the following is the purpose of labeling cables and connections when seizing the computer system?

- A. To capture the system configuration as it was at the time it was removed
- B. To maintain the chain of custody
- C. To block any communication with the computer system from attack
- D. To document the model, manufacturer, and type of cables connected

Correct Answer: A

QUESTION 5

As part of the SDLC, software developers are testing the security of a new web application by inputting large amounts of random data. Which of the following types of testing is being performed?

- A. Fuzzing
- B. Regression testing
- C. Stress testing
- D. Input validation

Correct Answer: A

[CS0-001 PDF Dumps](#)

[CS0-001 VCE Dumps](#)

[CS0-001 Practice Test](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.pass4lead.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © pass4lead, All Rights Reserved.