



CAS-004^{Q&As}

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

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

<https://www.passapply.com/cas-004.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

An application developer has been informed of a web application that is susceptible to a clickjacking vulnerability Which of the following code snippets would be MOST applicable to resolve this vulnerability?

- A. Content-Security-Policy frame-ancestors: \\\none\\
- B. \$escaped_command = escapeshellcmd(\$args); exec (\$escaped_command, \$output, \$return_var);
- C. \$sqlQuery= '\\SELECT * FROM custTable WHERE User=? AND Pass=?\\' parameters.add("User", username)
- D. require '\\digest/sha2\\' sha256 = Digest::SHA2.new(256)

Correct Answer: A

Content-Security-Policy: frame-ancestors \\\none';

This prevents any domain from framing the content This setting is recommended unless a specific need has been identified for framing

QUESTION 2

Which of the following controls primarily detects abuse of privilege but does not prevent it?

- A. Off-boarding
- B. Separation of duties
- C. Least privilege
- D. Job rotation

Correct Answer: A

QUESTION 3

A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:

```
High (CVSS: 10.0)
NVT: PHP 'php_escapeshellcmd()' Buffer Overflow Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803317)
Product detection result: cpe:/a:php:php:5.3.6 by NVD Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.0.800109)

Summary
This host is running PHP and is prone to buffer overflow vulnerability.
Vulnerability Detection Result: Installed version: 5.3.6
Fixed version: 5.3.15/5.4.5

Impact
Successful exploitation could allow attackers to execute arbitrary code and failed attempts will likely result in denial-of-service conditions. Impact Level: System/Application
```

Which of the following MOST appropriate corrective action to document for this finding?

- A. The product owner should perform a business impact assessment regarding the ability to implement a WAF.
- B. The application developer should use a static code analysis tool to ensure any application code is not vulnerable to



buffer overflows.

C. The system administrator should evaluate dependencies and perform upgrade as necessary.

D. The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.

Correct Answer: A

QUESTION 4

The Chief Information Security Officer (CISO) asked a security manager to set up a system that sends an alert whenever a mobile device enters a sensitive area of the company's data center. The CISO would also like to be able to alert the individual who is entering the area that the access was logged and monitored. Which of the following would meet these requirements?

A. Near-field communication

B. Short Message Service

C. Geofencing

D. Bluetooth

Correct Answer: C

Geofencing is a technology that allows you to set up virtual boundaries or geographic zones and trigger actions when a mobile device enters or exits those predefined areas. In this case, you can set up a geofence around the sensitive area of the data center, and when a mobile device enters that area, it can trigger an alert to be sent to the security team and optionally notify the individual entering the area that their access has been logged and monitored. Geofencing is commonly used for location-based security and notifications.

QUESTION 5

An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.

Which of the following is the MOST cost-effective solution?

A. Move the server to a cloud provider.

B. Change the operating system.

C. Buy a new server and create an active-active cluster.

D. Upgrade the server with a new one.

Correct Answer: A



VCE & PDF

PassApply.com

<https://www.passapply.com/cas-004.html>

2024 Latest passapply CAS-004 PDF and VCE dumps Download

[Latest CAS-004 Dumps](#)

[CAS-004 Practice Test](#)

[CAS-004 Braindumps](#)