

CAS-003^{Q&As}

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

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

<https://www.leads4pass.com/cas-003.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

Given the code snippet below:

```
#include <stdio.h>
#include <stdlib.h>
int main(void) {
    char username[8];
    printf("Enter your username: ");
    gets(username)
    printf("\n");
    if (username == NULL) {
        printf("you did not enter a username\n");
    }
    if strcmp(username, "admin") {
        printf("%s", "Admin user, enter your physical token value: ");
        // rest of conditional logic here has been snipped for brevity
    } else [
        printf ("Standard user, enter your password: ");
        // rest of conditional logic here has been snipped for brevity
    }
}
```

Which of the following vulnerability types is the MOST concerning?

- A. Only short usernames are supported, which could result in brute forcing of credentials.
- B. Buffer overflow in the username parameter could lead to a memory corruption vulnerability.
- C. Hardcoded usernames with different code paths taken depend on which user is entered.
- D. Format string vulnerability is present for admin users but not for standard users.

Correct Answer: B

QUESTION 2

A software company is releasing a new mobile application to a broad set of external customers. Because the software company is rapidly releasing new features, it has built in an over-the-air software update process that can automatically update the application at launch time. Which of the following security controls should be recommended by the company's security architect to protect the integrity of the update process? (Choose two.)

- A. Validate cryptographic signatures applied to software updates
- B. Perform certificate pinning of the associated code signing key
- C. Require HTTPS connections for downloads of software updates
- D. Ensure there are multiple download mirrors for availability
- E. Enforce a click-through process with user opt-in for new features

Correct Answer: AB

QUESTION 3

A Chief Information Security Officer (CISO) is creating a security committee involving multiple business units of the corporation. Which of the following is the BEST justification to ensure collaboration across business units?

- A. A risk to one business unit is a risk avoided by all business units, and liberal BYOD policies create new and unexpected avenues for attackers to exploit enterprises.
- B. A single point of coordination is required to ensure cybersecurity issues are addressed in protected, compartmentalized groups.
- C. Without business unit collaboration, risks introduced by one unit that affect another unit may go without compensating controls.
- D. The CISO is uniquely positioned to control the flow of vulnerability information between business units.

Correct Answer: C

QUESTION 4

A new corporate policy requires that all employees have access to corporate resources on personal mobile devices. The information assurance manager is concerned about the potential for inadvertent and malicious data disclosure if a device is lost, while users are concerned about corporate overreach. Which of the following controls would address these concerns and should be reflected in the company's mobile device policy?

- A. Place corporate applications in a container
- B. Enable geolocation on all devices
- C. install remote wiping capabilities
- D. Ensure all company communications use a VPN

Correct Answer: A

QUESTION 5

A company is implementing a new secure identity application, given the following requirements

1.

The cryptographic secrets used in the application must never be exposed to users or the OS

2.

The application must work on mobile devices.

3.

The application must work with the company's badge reader system

Which of the following mobile device specifications are required for this design? (Select TWO).

A. Secure element

B. Biometrics

C. UEFI

D. SEAndroid

E. NFC

F. HSM

Correct Answer: BE

[CAS-003 VCE Dumps](#)

[CAS-003 Exam Questions](#)

[CAS-003 Braindumps](#)