312-39Q&As

Certified SOC Analyst (CSA)

Pass Pegasystems 312-39 Exam with 100% Guarantee

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

https://www.leads4pass.com/312-39.html

100% Passing Guarantee
100% Money Back Assurance

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

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

QUESTION 1

Sam, a security analyst with INFOSOL INC., while monitoring and analyzing IIS logs, detected an event matching regex /\\w*((\%27)|(\\\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix.

What does this event log indicate?

A. SQL Injection Attack

B. Parameter Tampering Attack

C. XSS Attack

D. Directory Traversal Attack

Correct Answer: A

Reference: https://community.broadcom.com/symantecenterprise/communities/community-home/ librarydocuments/viewdocument?DocumentKey=001f5e09-88b4-4a9a-b3104c20578eecf9andCommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68andtab=librarydocuments

---

QUESTION 2

An attacker exploits the logic validation mechanisms of an e-commerce website. He successfully purchases a product worth $100 for $10 by modifying the URL exchanged between the client and the server.

Original URL: http://www.buyonline.com/product.aspx?profile=12anddebit=100 Modified URL: http://www.buyonline.com/product.aspx?profile=12anddebit=10

Identify the attack depicted in the above scenario.

A. Denial-of-Service Attack

B. SQL Injection Attack

C. Parameter Tampering Attack

D. Session Fixation Attack

Correct Answer: D

QUESTION 3

Bonney\\'s system has been compromised by a gruesome malware.

What is the primary step that is advisable to Bonney in order to contain the malware incident from spreading?

A. Complaint to police in a formal way regarding the incident

B. Turn off the infected machine

C. Leave it to the network administrators to handle

D. Call the legal department in the organization and inform about the incident

Correct Answer: B

QUESTION 4

Which of the following factors determine the choice of SIEM architecture?

A. SMTP Configuration

B. DHCP Configuration

C. DNS Configuration

D. Network Topology

Correct Answer: C

QUESTION 5

Which of the following data source will a SOC Analyst use to monitor connections to the insecure ports?

A. Netstat Data

B. DNS Data

C. IIS Data

D. DHCP Data

Correct Answer: A