CS0-003$^{\text{Q\&As}}$

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

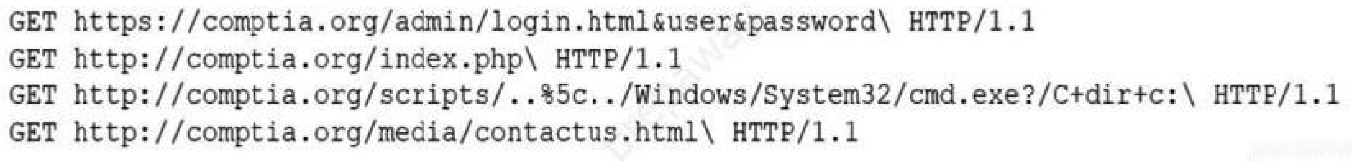
Following Questions and Answers are all new published by CompTIA Official Exam Center

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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

A security analyst is reviewing the following log entries to identify anomalous activity:



```
GET https://comptia.org/admin/login.html&user&password\ HTTP/1.1
GET http://comptia.org/index.php\ HTTP/1.1
GET http://comptia.org/scripts/..%5c../Windows/System32/cmd.exe?/C+dir+c:\ HTTP/1.1
GET http://comptia.org/media/contactus.html\ HTTP/1.1
```

Which of the following attack types is occurring?

A. Directory traversal

B. SQL injection

C. Buffer overflow

D. Cross-site scripting

Correct Answer: A

A directory traversal attack is a type of web application attack that exploits insufficient input validation or improper configuration to access files or directories that are outside the intended scope of the web server. The log entries given in the question show s" sequences in the URL, which indicate an attempt to move up one level in the directory structure. For "" tries to access the /etc/passwd file, which contains user account information on Linux systems. If successful, this attack could allow an attacker to read, modify, or execute files on the web server that are not meant to be accessible.

QUESTION 2

A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to

A. This is a normal password change URL.

B. The security operations center is performing a routine password audit.

C. A new VPN gateway has been deployed.

D. A social engineering attack is underway.

Correct Answer: D

QUESTION 3

A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user\\'s workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?

A. Create a timeline of events detailinq the date stamps, user account hostname and IP information associated with the activities

B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation

C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identity the case as an HR-related investigation

D. Notify the SOC manager for awareness after confirmation that the activity was intentional

Correct Answer: B

The best way to ensure that the investigation complies with HR or privacy policies is to ensure that the case details do not reflect any user-identifiable information, such as name, email address, phone number, or employee ID. This can help protect the privacy and confidentiality of the user and prevent any potential discrimination or retaliation. Additionally, password protecting the evidence and restricting access to personnel related to the investigation can help preserve the integrity and security of the evidence and prevent any unauthorized or accidental disclosure or modification.

QUESTION 4

A development team is discussing the implementation of parameterized queries to address several software vulnerabilities. Which of the following is the most likely type of vulnerability the team is trying to remediate?

A. SQL injection

B. CSRF

C. On-path attack

D. XSS

Correct Answer: A

QUESTION 5

A consumer credit card database was compromised, and multiple representatives are unable to review the appropriate customer information. Which of the following should the cybersecurity analyst do first?

A. Start the containment effort.

B. Confirm the incident.

C. Notify local law enforcement officials.

D. Inform the senior management team.

Correct Answer: B

Latest CS0-003 Dumps CS0-003 Study Guide CS0-003 Braindumps