CAS-004Q&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.pass2lead.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:

1.

Unstructured data being exfiltrated after an employee leaves the organization

2.

Data being exfiltrated as a result of compromised credentials

3.

Sensitive information in emails being exfiltrated

Which of the following solutions should the security team implement to mitigate the risk of data loss?

A. Mobile device management, remote wipe, and data loss detection

B. Conditional access, DoH, and full disk encryption

C. Mobile application management, MFA, and DRM

D. Certificates, DLP, and geofencing

Correct Answer: C

QUESTION 2

A company just released a new video card. Due to limited supply and high demand, attackers are employing automated systems to purchase the device through the company\\'s web store so they can resell it on the secondary market. The company\\'s intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems.

Which of the following now describes the level of risk?

A. Inherent

B. Low

C. Mitigated

D. Residual.

E. Transferred

Correct Answer: D

QUESTION 3

A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.

```
Test email sent from bp_app01 to external client_app01_mailing_list.
```

Which of the following should the security analyst perform?

A. Contact the security department at the business partner and alert them to the email event.

B. Block the IP address for the business partner at the perimeter firewall.

C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.

D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

Correct Answer: A

QUESTION 4

SIMULATION

A product development team has submitted code snippets for review pnor to release INSTRUCTIONS.

Analyze the code snippets and then select one vulnerability and one fix for each code snippet If at any time you would like to bang back the initial state of the simulation, please click the Reset All button.

Code Snippet 1

```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103

Web server code:
--
String accountQuery = "SELECT * from users WHERE userid = ?";
PreparedStatement stmt = connection.prepareStatement (accountQuery);
stmt.setString(1, request.getParameter("userid"));
ResultSet queryResponse = stmt.executeQuery();
--
```

Vulnerability 1

- ◯ Server-side request forgery
- ◯ Cross-site scripting
- ◯ Cross-request request forgery
- ◯ Indirect object reference
- ◯ SQL injection

Fix 1

- ◯ Implement anti-forgery tokens.
- ◯ Perform output encoding of `queryResponse`.
- ◯ Ensure `userid` belongs to logged-in user.
- ◯ Inspect URLs and disallow arbitrary requests.
- ◯ Perform input sanitization of the `userid` field.

Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103

API endpoint (/searchDirectory):
…
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5, 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
  userId = request.getParam(userid)

ldapLookup = 'ldapsearch      -D "cn' + userId + '" -W -p 389
                              -h loginserver.comptia.org
                              -b "dc=comptia,dc=org" -s sub -x "(objectclass=")"'
accountLookup = subprocess.popen(ldapLookup)

if (userExists(accountLookup))
     accountFound = true
else
     accountFound = false
…
```

Vulnerability 2

- ◯ Command injection
- ◯ SQL injection
- ◯ Authorization bypass
- ◯ Denial of service
- ◯ Credentials passed via GET

Fix 2

- ◯ Implement prepared statements and bind variables.
- ◯ HTTP POST should be used for sensitive parameters.
- ◯ Perform input sanitization of the `userid` field.
- ◯ Prevent the "authenticated" value from being overridden by a GET parameter.
- ◯ Remove the `serve_forever` instruction.

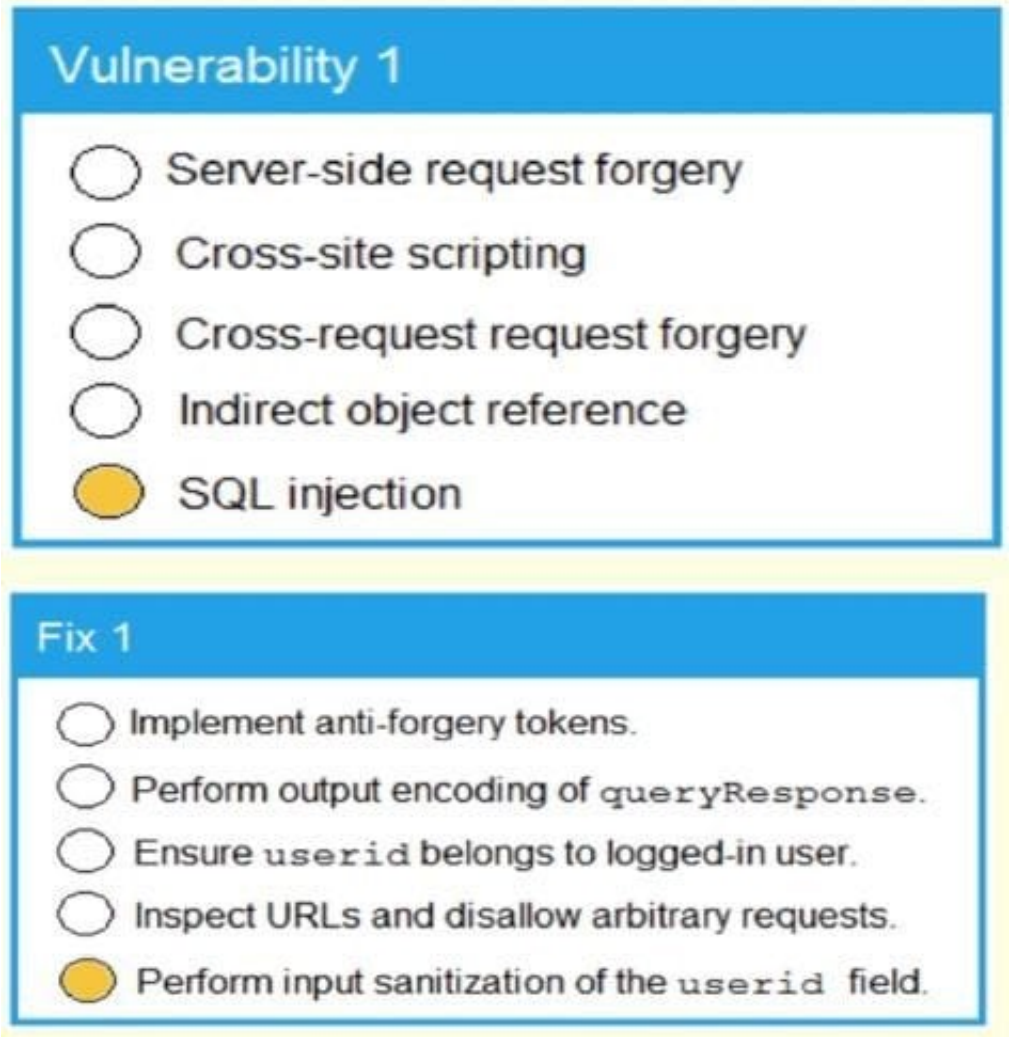
A. Check the answer in explanation below.

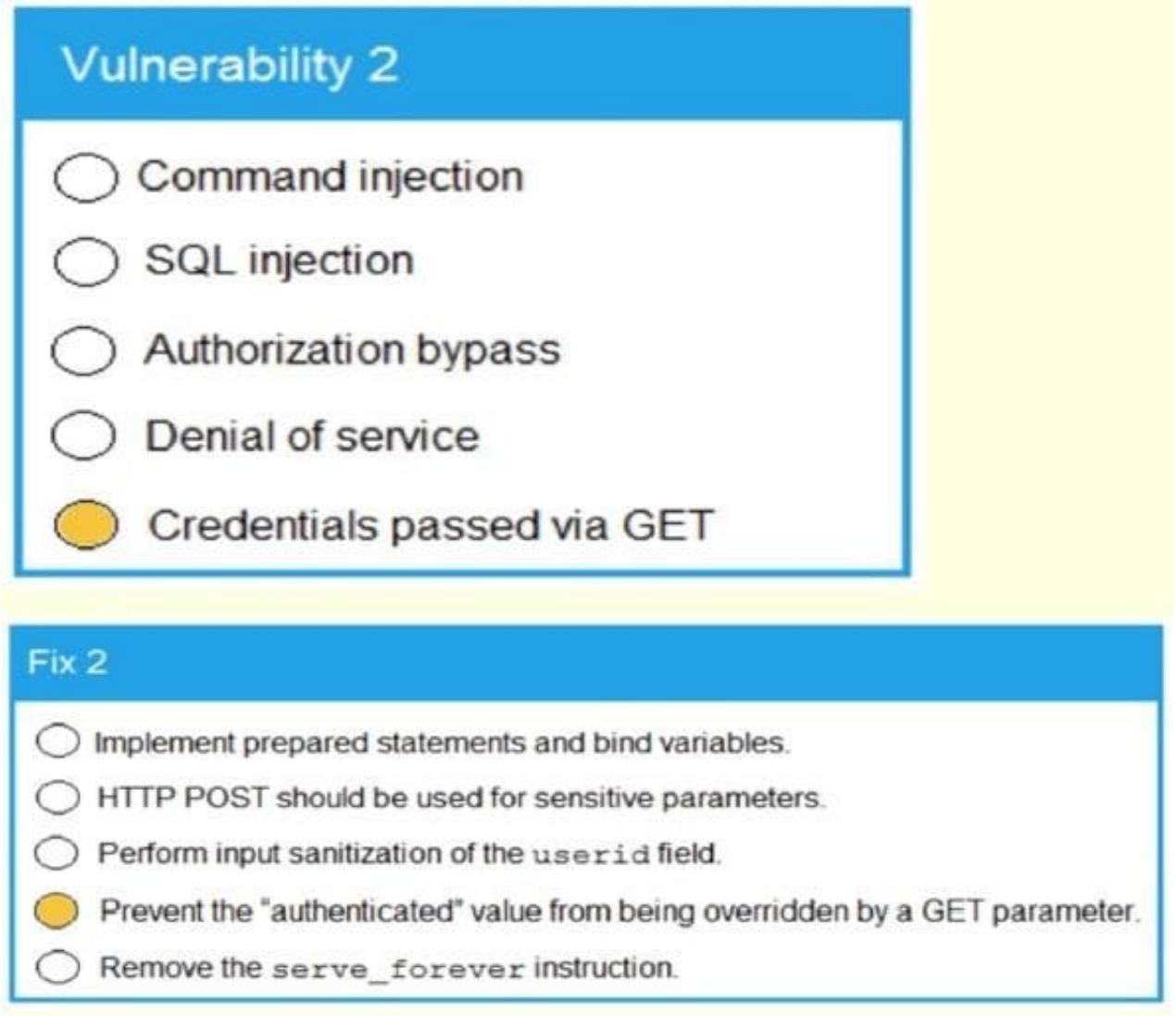
B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A





QUESTION 5

The Chief Information Officer (CIO) wants to establish a non-binding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a formal partnership. Which of the following would MOST likely be used?

A. MOU

B. OLA

C. NDA

D. SLA

Correct Answer: A

QUESTION 6

A MSSP has taken on a large client that has government compliance requirements. Due to the sensitive nature of communications to its aerospace partners, the MSSP must ensure that all communications to and from the client web portal are secured by industry-standard asymmetric encryption methods. Which of the following should the MSSP configure to BEST meet this objective?

A. ChaCha20

B. RSA

C. AES256

D. RIPEMD

Correct Answer: B

QUESTION 7

Which of the following communication protocols is used to create PANs with small, low-power digital radios and supports a large number of nodes?

A. Zigbee

B. Wi-Fi

C. CAN

D. Modbus

E. DNP3

Correct Answer: A

QUESTION 8

Which of the following is used to assess compliance with internal and external requirements?

A. RACI matrix

B. Audit report

C. After-action report

D. Business continuity plan

Correct Answer: B

Reference: https://reciprocity.com/a-guide-to-completing-an-internal-audit-for-compliance-management/#:~:text=Compliance%20audit.,a%20policy%20or%20statutory%20requirement

QUESTION 9

A law firm experienced a breach in which access was gained to a secure server. During an investigation to determine how the breach occurred, an employee admitted to clicking on a spear-phishing link. A security analyst reviewed the event logs and found the following:

1.

PAM had not been bypassed.

2.

DLP did not trigger any alerts.

3.

The antivirus was updated to the most current signatures.

Which of the following MOST likely occurred?

A. Exploitation

B. Exfiltration

C. Privilege escalation

D. Lateral movement

Correct Answer: D

QUESTION 10

A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLS-protected HTTP sessions from systems that do not send traffic to those sites.

The technician will define this threat as:

A. a decrypting RSA using obsolete and weakened encryption attack.

B. a zero-day attack.

C. an advanced persistent threat.

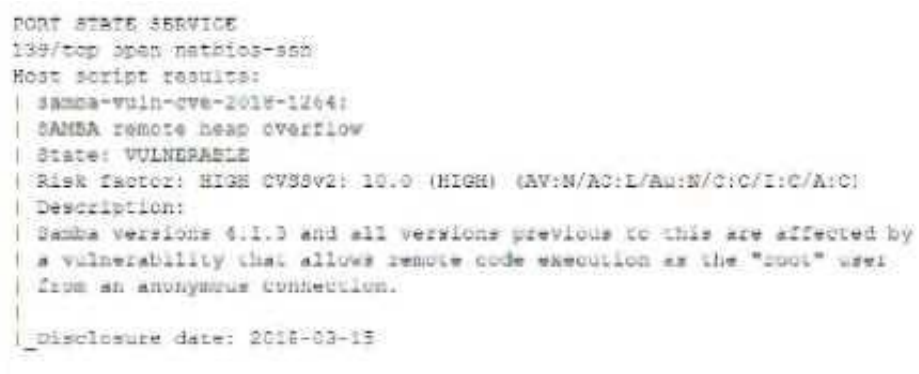
D. an on-path attack.

Correct Answer: C

Reference: https://www.internetsociety.org/deploy360/tls/basics/

QUESTION 11

A security is testing a server finds the following in the output of a vulnerability scan:



Which of the following will the security analyst most likely use NEXT to explore this further?

A. Exploitation framework

B. Reverse engineering tools

C. Vulnerability scanner

D. Visualization tool

Correct Answer: A

QUESTION 12

A security manager wants to standardize security settings, firmware, and software across a heterogeneous environment. Which of the following can be used in combination to meet these goals? (Choose three).

A. Attestation services

B. TPM

C. HIPS software

D. OOB management software

E. Group Policy

F. EDR software

G. MDM software

Correct Answer: BEF

QUESTION 13

A security engineer is reviewing a record of events after a recent data breach incident that Involved the following:

1.

A hacker conducted reconnaissance and developed a footprint of the company s Internet- facing web application assets.

2.

A vulnerability in a third-party horary was exploited by the hacker, resulting in the compromise of a local account.

3.

The hacker took advantage of the account\\'s excessive privileges to access a data store and exfilltrate the data without detection.

Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

A. Dynamic analysis

B. Secure web gateway

C. Software composition analysis

D. User behavior analysis

E. Web application firewall

Correct Answer: C

QUESTION 14

A company wants to protect its intellectual property from theft. The company has already applied ACLs and DACs. Which of the following should the company use to prevent data theft?

A. Watermarking

B. DRM

C. NDA

D. Access logging

Correct Answer: B

QUESTION 15

In order to authenticate employees who, call in remotely, a company\\'s help desk staff must be able to view partial information about employees because the full information may be considered sensitive. Which of the following solutions should be implemented to authenticate employees?

A. Data scrubbing

B. Field masking

C. Encryption in transit

D. Metadata

Correct Answer: B

Field masking is a technique used to partially conceal sensitive information while still allowing authorized personnel to authenticate users or perform necessary tasks. In this case, it would allow help desk staff to view partial information about employees without exposing the entire sensitive dataset.