



Free Questions for ITS-110 by go4braindumps

Shared by Davis on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An IoT developer needs to ensure that user passwords for a smartphone app are stored securely. Which of the following methods should the developer use to meet this requirement?

Options:

- A- Encrypt all stored passwords using 256-bit Advanced Encryption Standard (AES-256)
- B- Encrypt all stored passwords using 128-bit Twofish
- C- Hash all passwords using Message Digest 5 (MD5)
- D- Store all passwords in read-only memory

Answer:

A

Question 2

Question Type: MultipleChoice

It is a new employee's first day on the job. When trying to access secured systems, he incorrectly enters his credentials multiple times. Which resulting action should take place?

Options:

- A- His account is deleted.
- B- He receives a new password.
- C- His account is locked.
- D- He notifies Human Resources.

Answer:

C

Question 3

Question Type: MultipleChoice

A web application is connected to an IoT endpoint. A hacker wants to steal data from the connection between them. Which of the following is NOT a method of attack that could be used to facilitate stealing data?

Options:

- A- Cross-Site Request Forgery (CSRF)
- B- SQL Injection (SQLi)
- C- Cross-Site Scripting (XSS)
- D- LDAP Injection

Answer:

D

Question 4

Question Type: MultipleChoice

A hacker is sniffing network traffic with plans to intercept user credentials and then use them to log into remote websites. Which of the following attacks could the hacker be attempting? (Choose two.)

Options:

- A- Masquerading

- B-** Brute force
- C-** Directory traversal
- D-** Session replay
- E-** Spear phishing

Answer:

B, E

Question 5

Question Type: MultipleChoice

If a site administrator wants to improve the secure access to a cloud portal, which of the following would be the BEST countermeasure to implement?

Options:

- A-** Require frequent password changes
- B-** Mandate multi-factor authentication (MFA)

C- Utilize role-based access control (RBAC)

D- Require separation of duties

Answer:

C

Question 6

Question Type: MultipleChoice

A hacker is able to access privileged information via an IoT portal by modifying a SQL parameter in a URL. Which of the following BEST describes the vulnerability that allows this type of attack?

Options:

A- Unvalidated redirect or forwarding

B- Insecure HTTP session management

C- Unsecure direct object references

D- Unhandled malformed URLs

Answer:

D

Question 7

Question Type: MultipleChoice

An IoT system administrator discovers that hackers are using rainbow tables to compromise user accounts on their cloud management portal. What should the administrator do in order to mitigate this risk?

Options:

- A- Implement robust password policies
- B- Implement certificates on all login pages
- C- Implement granular role-based access
- D- Implement URL filtering

Answer:

C

Question 8

Question Type: MultipleChoice

Which of the following policies provides the BEST protection against identity theft when data stored on an IoT portal has been compromised?

Options:

- A- Data retention polices
- B- Data categorization policies
- C- Data anonymization policies
- D- Data disposal policies

Answer:

C

Question 9

Question Type: MultipleChoice

A hacker is able to extract users' names, birth dates, height, and weight from an IoT manufacturer's user portal. Which of the following types of data has been compromised?

Options:

- A- Protected health information
- B- Personal health information
- C- Personal identity information
- D- Personally identifiable information

Answer:

D

To Get Premium Files for ITS-110 Visit

<https://www.p2pexams.com/products/its-110>

For More Free Questions Visit

<https://www.p2pexams.com/certnexus/pdf/its-110>

