CCI-AUX (fc2d6b9a)

2019-11-7 5:29:48

Exam Instructions

As shown in the example below, each test item has three parts: an optional scenario, a question (stem), and alternatives. For each test item, please answer the stem, evaluate the item, and optionally write a comment. If you believe there is a problem in the answer, report the issue using the report error button at the side. Thank you.

Question

How many centimeters in a meter?

A. 1
B. 1000
C. 100
D. 100,000
E. 1,000,000

Review

A-Accept

B-Accept w/ Minor Revisions

C-Accept w/ Major Revisions

D-Reject

Comments

Review

{{submitted_answers.text}}

{{submitted_answers.comments}}

Question A2-2

Alice wants to send a file to Bob over an Internet connection.

Alice wants to make sure that only Bob and Alice can read the file.

Question. Choose the action by Alice that best accomplishes this goal:

A. Cryptographically hash the file and send the resulting hash value to Bob.
B. Sign the file for Bob to authenticate.
C. Transform the file into a previously agreed upon obscure format.
D. Ensure Alice and Bob's operating systems have the latest security patches.
E. Encrypt the file with a symmetric cipher using a secret key known to Alice and Bob.

Question A2-3

Alice wants to send a file to Bob over an Internet connection.

Bob wants to convince himself that the message truly came from Alice.

Question. Choose the action by Alice that best accomplishes this goal:

A. Sign the message with her private key.
B. Include the time and date in her message.
C. After sending the file, also send a text message to Bob confirming she has sent the file.
D. Send the message over a virtual private network (VPN).
E. Insert an image of her handwritten signature to the file.

Question A3-1

When a user Mike O'Brien registered a new account for an online shopping site, he was required to provide his username, address, first and last name, and a password. Immediately after Mike submitted his request, you—as the security engineer—observe a database input error message in the logs.

Question. The error message suggests that the system places undue trust in one of its elements. Choose that untrustworthy element:

A. Correctness of the database error logs.
B. Text entered by users into the registration form.
C. Trustworthiness of the database administrator.
D. Integrity of database content.
E. Strength of encryption protecting the database.

Question A3-2

When a user Mike O'Brien registered a new account for an online shopping site, he was required to provide his username, address, first and last name, and a password. Immediately after Mike submitted his request, you—as the security engineer—observe a database input error message in the logs.

Question. For this error message, choose the potential vulnerability that warrants the most concern:

A. Mike's input may cause the database to execute unintended code.
B. Mike may access sensitive data stored in the database due to improper firewall configuration.
C. The system may include malicious code implementing a backdoor.
D. An eavesdropper may read unencrypted communications between Mike and the server.
E. A software error may allow users to change their purchase amount.

Question A3-4

When a user Mike O'Brien registered a new account for an online shopping site, he was required to provide his username, address, first and last name, and a password. Immediately after Mike submitted his request, you—as the security engineer—observe a database input error message in the logs.

Exploiting the reported database error, an attacker was able to sign in as any customer.

Question. Choose the vulnerability that most likely permitted this attack:

A. Weak firewall configuration.
B. Weak encryption.
C. Programming error improperly processes apostrophes.
D. Infrequent password changes.
E. Customer passwords are long but simple.

Question B1-1

A bank offers online banking services. To connect to these services from her home computer, the user searches for the bank's name and follows the first link returned by the search. She logs into the website by entering her username and password. She then performs several banking transactions.

The day after she logged into the website, the user discovers that one thousand dollars were withdrawn from her account without her knowledge. The link she had followed led her to a fake banking site which stole her credentials.

Question. To mitigate this fraud, choose how the online banking services should be improved:

A. The user's browser must authenticate the bank's website.
B. The user's password must be long and complex.
C. All communication between the user and the bank must be encrypted.
D. The password must be cryptographically hashed before it is transmitted.
E. Pay the search engine to list the genuine banking site first.

Question C1-2

Bob's manager Alice is traveling abroad to give a sales presentation about an important new product. Bob receives an email with the following message: "Bob, I just arrived and the airline lost my luggage. Would you please send me the technical specifications? Thanks, Alice."

Question. Choose the LEAST effective practice to protect the technical specifications in this scenario:

A. Enforce a strict access control policy.
B. Use an email system that automatically authenticates messages.
C. Train all employees on sound cybersecurity practices.
D. When traveling, keep sensitive information in your physical presence.
E. Keep company security procedures secret.

Question H1-1

A medical device company is developing a new insulin pump embedded in the patient for releasing measured amounts of insulin into the patient. The patient's glucose monitor sends data wirelessly to a remote server. The server calculates insulin dosages and sends the data wirelessly to the patient's embedded insulin pump for releasing measured amounts of insulin. It is important that malicious behavior be detectable.

Question. Choose the security goal that is the LEAST important for the company's proposed system:

A. Availability of the remote server.
B. Integrity of the communicated data.
C. Authentication of the remote server by the insulin pump.
D. Confidentiality of the patient's data transmitted from server to pump.
E. Non-repudiation by server of data it sends to the insulin pump.

Definitions

Non-repudiation: A party, having taken an action, cannot deny taking the action.

Question T2-1

ACME Corporation is moving its headquarters across town. To facilitate the move, ACME:

- hired a moving company with guarded trucks to move company property.
- encrypted all backup data and then migrated it to a third-party cloud provider.
- instructed employees to place documents in a wheeled bin with locked cover (located in the old building's lobby), to be shredded the next day.
- instructed employees to exchange their old IDs and keys for new ones when they arrive at the new building.
- instructed employees to throw unwanted non-sensitive materials into the corporate dumpster behind the old building.

Jim is a disgruntled former employee of the prototype design team who wants to steal sensitive plans for a prototype that was not selected for production.

Question. Choose the way that is most promising (easiest, minimizing risk, favorable chance of success) way for Jim to acquire this information:

A. Compromise the third-party cloud provider.
B. Take the wheeled bin.
C. Show up to the new building and ask for a key, pretending to have lost his old ID.
D. Impersonate a moving company employee and steal a truck.
E. Search the dumpster at the old building.

Question Z1-1

Alice recently purchased a smart thermostat for her home. She can configure the security settings of the thermostat from her phone through an Internet connection. Recently, she read in the news that thermostats like hers were used to perform a Distributed Denial of Service (DDoS) attack against political websites.

Question. Choose the action that best reduces the likelihood that the thermostat can be used in a DDoS attack:

A. Use a virtual private network (VPN) to require all changes to security settings on the thermostat to be initiated from Alice's phone.
B. Encrypt all messages between her phone and her thermostat using strong encryption.
C. Implement intrusion detection on the thermostat and shut off the thermostat if an intrusion is detected.
D. Install a firewall on the thermostat to filter in-coming and out-going messages.
E. Cryptographically sign all messages between her phone and her thermostat.