Test CyberSecurity

Total points 10/10

Dear Student!

At the end of the block, we encourage you to take the test yourself. The results are only for you, they will help you verify the extent to which knowledge was acquired by you.

After the test you will receive point information on how it went :)

Good luck!
SDA team

0 of 0 points

Name and surname *

Brikena Agalliu

Test questions — 10 of 10 points

✓ Cross-site Scripting (XSS) attack is about: * 1/1

- (●) Placing malicious code (usually Javascript) in the content of the attacked website. ✓
- ( ) Eavesdropping and modifying messages sent between two parties without their knowledge nor consent.
- ( ) Forcing user's browser to execute an unauthorized (unwanted) request.
- ( ) Impersonating the attacker as another person to force the victim to open a link (e.g. sent in an email).

✓ Select the true statement: * 1/1

- ( ) The use of HTTPS makes it impossible to eavesdrop and modify communication between computers.
- (●) HTTPS uses the TLS protocol to establish a secure, encrypted connection with the server. ✓
- ( ) HTTPS uses only asymmetric cryptography.
- ( ) HTTPS uses only symmetric cryptography.

✓ A SQL injection attack can cause: * 1/1

- (●) All answers are correct. ✓
- ( ) Modification or deletion of data tored in the database by the attacker.
- ( ) Logging in the attacker as victim despite entering wrong password.
- ( ) Unauthorized access to other user's data by the attacker.

✓ Select hash functions which are considered to be safe nowadays (no vulnerabilities have been found in them so far and they are recommended to use in applications) *1/1

- (●) SHA-2, SHA-3 ✓
- ( ) MD5, SHA-1, SHA-2, SHA-3
- ( ) SHA-1, SHA-2, SHA-3
- ( ) MD5, SHA-1

✓ Select the true statement regarding certificates: * 1/1

- ( ) The cetficiate contains information about the issuer, enrirty, expiry date and used agorithms. It does not have public key - it is read from the operating systems's

algorithms. It does not have public key - it is read from the operating system's keystore.

We can create so called self-signed certificate, which will be widely accepted on the Internet.

We can order a widely recognized (commonly accepted) certificate for our website from certification authority (CA). ✓

Root certificates are saved in operating system by user who wants to use Internet safely.

✓ Select the FALSE sentence regarding session hijacking attack: * 1/1

Confirming operations using one-time SMS passwords or mobile application authorization in NOT an obstacle for the attacker who hijacked our session. ✓

The attacker may intercept our session then he learns the content of our browser's cookie for given site.

We can protect ourselves against session hijacking by using HTTPS.

Server can implement additional safety measures on its side to protect against session hijacking.

✓ DDoS attack is about: * 1/1

Obtaining unauthorized access by the attacker to the server, along with possibility to execute any code with elevated (root) privileges.

Using a computer to send a crafted request that freezes the server and prevents real users from using website.

Using multiple computers to send multiple requests to one server in other to overwhelm it with request processing and prevent real users from using website effectively. ✓

Using a computer to send multiple requests to a single server in other to overwhelm it with request processing and prevent real users from using website effectively.

✓ Does HTTPS prevent DNS spoofing attack? * 1/1

Yes - if the attacker does not have server's private key. ✓

Yes - always.

No - never.

Yes - but only if the attacker does not have access to the network device that is used to access the Internet (e.g. a router in a cafe).

✓ What is the difference between symmetric and asymmetric encryption? Select the true statement. *1/1

Symmetric encryption uses a common, shared key to both encrypt and decrypt messages. Asymmetric encryption uses two separate keys for encryption and decryption. ✓

Asymmetric encryption uses a common, shared key to both encrypt and decrypt messages.Symmetric encryption uses two separate keys for encryption and decryption

Symmetric encryption requires longer keys (with more bits of key length) than asymmetric encryption (to ensure same level of security)

Both symmetric and asymmetric cryptography use same algorithms

✓ The best way to store passwords in a database is to... * 1/1

Store them as digest (hash value) calculated from plaintext password with salt. ✓

Store them as digest (hash value) calculated from plaintext password.

Store them as plaintext.

Store them as encrypted text.