1

Question: What is Cross-Site Request Forgery (CSRF)?

A) An attack that allows attackers to access a server without authentication.

B) An attack that tricks a user's browser into executing unwanted actions in an application they are logged into.

C) A type of malware that encrypts user data and demands a ransom.

D) A phishing attack that attempts to steal user credentials.

Correct Answer: B

2

Question: Which of the following is NOT a potential consequence of a successful CSRF attack?

A) Unauthorized fund transfers

B) Changed passwords

C) Data theft (e.g., stolen session cookies)

D) Denial of Service (DoS) attack

Correct Answer: D

3

Question: What is the primary purpose of an anti-CSRF token?

A) To encrypt user data before transmission.

B) To verify the authenticity of a user's request.

C) To prevent brute-force attacks.

D) To mask the user's IP address.

Correct Answer: B

4

Question: The `SameSite` cookie attribute helps prevent CSRF attacks by:

A) Encrypting the cookie data.

B) Restricting cookies to be sent only in a first-party context.

C) Masking the user's IP address.

D) Implementing two-factor authentication.

Correct Answer: B

5

Question: Which of the following is NOT a good practice for CSRF protection?

A) Logging off web applications when not in use.

B) Regularly updating usernames and passwords.

C) Saving passwords in the browser for convenience.

D) Avoiding simultaneously browsing while logged into sensitive applications.

Correct Answer: C