1

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

A) An attack that forces a user to log out of an application.

B) An attack that tricks a web browser into executing unwanted actions in an application where a user is logged in.

C) A type of virus that infects web browsers.

D) A method for securely transferring funds online.

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 (stolen session cookies)

D) Installation of malware on the user's computer

Correct Answer: D

3

Question: How does a CSRF attack typically trick a user into executing a forged request?

A) By installing a keylogger on the user's computer.

B) By using malicious social engineering, such as an email or link.

C) By exploiting a vulnerability in the web server software.

D) By directly accessing the user's bank account.

Correct Answer: B

4

Question: Which of the following is a primary approach to prevent CSRF attacks?

A) Installing antivirus software.

B) Using strong passwords.

C) Synchronizing the cookie with an anti-CSRF token.

D) Disabling JavaScript in the web browser.

Correct Answer: C

5

Question: What is the purpose of the SameSite cookie attribute?

A) To allow third-party websites to access cookies.

B) To instruct the browser to disable third-party usage for specific cookies.

C) To encrypt cookies to prevent eavesdropping.

D) To store user credentials securely.

Correct Answer: B

6

Question: Which of the following is NOT a characteristic of a well-designed anti-CSRF token?

A) Unique for each user session.

B) Easily predictable by an attacker.

C) Cryptographically random value of significant length.

D) Automatically expires after a suitable amount of time.

Correct Answer: B