1

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

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

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

C) A type of virus that infects a user's computer.

D) A phishing attack that steals 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 (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?

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

B) By sending a malicious email or link that triggers a forged request.

C) By directly accessing the web application's server.

D) By using brute-force to guess the user's password.

Correct Answer: B

4

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

A) Using strong passwords

B) Installing antivirus software

C) Synchronizing the cookie with an anti-CSRF token

D) Regularly clearing browser history

Correct Answer: C

5

Question: What is the function of the `SameSite` cookie attribute?

A) It encrypts the cookie data.

B) It instructs the browser to disable third-party usage for specific cookies.

C) It extends the lifespan of the cookie.

D) It allows the cookie to be accessed by any website.

Correct Answer: B