1

Question: What does CSRF stand for?

A) Cross-Site Request Forgery

B) Cross-System Resource Failure

C) Critical Site Response Failure

D) Cross-Site Resource Forgery

Correct Answer: A

2

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

A) Unauthorized fund transfers

B) Changed passwords

C) Data theft (stolen session cookies)

D) Denial of Service (DoS)

Correct Answer: D

3

Question: How does a CSRF attack typically trick a user?

A) By installing malware on the user's computer

B) By exploiting a vulnerability in the web server

C) By tricking the user into clicking a malicious link or submitting a forged request

D) By directly accessing the user's account credentials

Correct Answer: C

4

Question: In the provided bank transfer example, what does the attacker modify in the GET request?

A) The transfer amount

B) The recipient's account number

C) The HTTP protocol version

D) The bank's URL

Correct Answer: B

5

Question: Which HTTP method is used in the provided bank transfer example to illustrate a CSRF attack?

A) POST

B) GET

C) PUT

D) DELETE

Correct Answer: B

6

Question: How many primary approaches are mentioned for preventing CSRF attacks?

A) 1

B) 2

C) 3

D) 4

Correct Answer: B

7

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

A) To encrypt the user's password

B) To verify the authenticity of a request

C) To track the user's browsing history

D) To prevent phishing attacks

Correct Answer: B

8

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

A) Unique for each user session

B) Publicly accessible

C) Cryptographically random

D) Expires after a suitable amount of time

Correct Answer: B

9

Question: What does the `SameSite` cookie attribute control?

A) The expiration time of a cookie

B) The domain where a cookie is valid

C) Whether a cookie is sent in cross-site requests

D) The security level of a cookie

Correct Answer: C

10

Question: Which of the following is a recommended best practice for CSRF protection?

A) Sharing passwords across multiple websites

B) Logging off web applications when not in use

C) Allowing browsers to remember passwords for convenience

D) Browsing multiple websites while logged into sensitive applications like online banking

Correct Answer: B