1

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

A) Cross-Site Scripting (XSS)

B) SQL Injection

C) Session Riding

D) Denial of Service (DoS)

Correct Answer: C

2

Question: What is a potential consequence of a successful CSRF attack?

A) Server overload

B) Unauthorized fund transfers

C) Disclosure of server configuration

D) Remote code execution

Correct Answer: B

3

Question: How does CSRF trick a user into executing an unwanted action?

A) By exploiting vulnerabilities in server-side code

B) By using malicious social engineering tactics, like deceptive emails or links

C) By directly injecting malicious code into a web application

D) By flooding the server with requests

Correct Answer: B

4

Question: Why is it difficult to distinguish a legitimate request from a forged one in a CSRF attack?

A) The attacker uses a different IP address.

B) The user is authenticated at the time of the attack.

C) The forged request uses a different browser.

D) The forged request uses a different HTTP method.

Correct Answer: B

5

Question: In the provided example, what is the purpose of modifying the GET request?

A) To transfer funds to the attacker's account.

B) To display a different message to the user.

C) To crash the bank's server.

D) To steal the user's login credentials.

Correct Answer: A

6

Question: How does an attacker distribute a malicious link in a CSRF attack?

A) By posting it on a public forum

B) By directly modifying the target website's code

C) By sending it through email

D) By exploiting vulnerabilities in the user's browser

Correct Answer: C

7

Question: What are the two primary approaches to prevent CSRF attacks?

A) Input validation and output encoding

B) Using anti-CSRF tokens and preventing the browser from sending cookies in third-party contexts

C) Firewall rules and intrusion detection systems

D) Regular password changes and two-factor authentication

Correct Answer: B

8

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

A) To encrypt sensitive data transmitted between the user and the server

B) To verify the origin of a request and ensure it is legitimate

C) To store the user's login credentials securely

D) To prevent SQL injection attacks

Correct Answer: B

9

Question: Which characteristic is crucial for a well-designed anti-CSRF token?

A) It should be easily predictable by the user.

B) It should remain the same for multiple user sessions.

C) It should be a cryptographically random value.

D) It should be visible to the user in the URL.

Correct Answer: C

10

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

A) To allow third-party websites to access the cookie.

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

C) To store sensitive user data on the client-side.

D) To increase the lifespan of a cookie.

Correct Answer: B

11

Question: Which practice is recommended to mitigate the risk of CSRF attacks?

A) Sharing passwords across multiple websites.

B) Allowing browsers to remember passwords for convenience.

C) Logging off web applications when not in use.

D) Continuously browsing different websites while logged into sensitive applications.

Correct Answer: C