1

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

A) Cross-Site Scripting (XSS)

B) SQL Injection

C) Session Riding

D) Clickjacking

Correct Answer: C

2

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

A) Server crashes

B) Unauthorized fund transfers

C) Denial of Service (DoS)

D) Malware installation

Correct Answer: B

3

Question: How does CSRF exploit user authentication?

A) By guessing the user's password

B) By exploiting vulnerabilities in the web server

C) By tricking the user's browser into sending a forged request while the user is logged in

D) By installing a keylogger on the user's computer

Correct Answer: C

4

Question: Which HTTP method is often used in CSRF attacks, as shown in the example?

A) POST

B) PUT

C) DELETE

D) GET

Correct Answer: D

5

Question: How might an attacker distribute a CSRF attack?

A) Through a software update

B) Through a malicious email containing a hyperlink

C) By directly accessing the web server

D) By installing a Trojan horse on the user's computer

Correct Answer: B

6

Question: What is a primary approach to preventing CSRF attacks?

A) Using strong passwords

B) Installing a firewall

C) Using anti-CSRF tokens

D) Regularly updating the operating system

Correct Answer: C

7

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

A) To encrypt user data

B) To verify the authenticity of a request

C) To prevent SQL injection attacks

D) To prevent cross-site scripting attacks

Correct Answer: B

8

Question: What is a characteristic of a well-designed anti-CSRF token?

A) It should be the same for all users.

B) It should be easily guessable.

C) It should be unique for each user session.

D) It should be stored in plain text.

Correct Answer: C

9

Question: What is the SameSite cookie attribute designed to do?

A) Allow third-party sites to access cookies

B) Encrypt cookies to prevent eavesdropping

C) Disable third-party usage for specific cookies

D) Store cookies on the user's hard drive

Correct Answer: C

10

Question: How does the SameSite cookie attribute help prevent CSRF attacks?

A) By encrypting the cookie data

B) By restricting cookies to first-party contexts

C) By allowing only HTTPS connections

D) By preventing the browser from storing cookies

Correct Answer: B

11

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

A) Sharing passwords with trusted friends

B) Leaving web applications logged in even when not in use

C) Logging off web applications when not in use

D) Using the same password for all online accounts

Correct Answer: C

12

Question: What is the recommended practice regarding browser password management for enhanced security against CSRF and other attacks?

A) Always allow browsers to remember passwords.

B) Avoid allowing browsers to remember passwords.

C) Use a single, complex password for all accounts.

D) Regularly clear browsing history but retain saved passwords.

Correct Answer: B

13

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

A) Data theft (stolen session cookies)

B) Changed passwords

C) Unauthorized fund transfers

D) Installation of ransomware

Correct Answer: D