security concerns with general vulnerability types

1. What type of vulnerability occurs when software does not properly validate or sanitize input?

- A) SQL injection
- B) Cross-site scripting (XSS)
- C) Buffer overflow
- D) Code injection
- **Answer: D) Code injection**

2. Which vulnerability occurs when an attacker intercepts and alters communication between two parties?

- A) Man-in-the-middle (MITM) attack
- B) Denial-of-Service (DoS) attack
- C) Spoofing
- D) Phishing
- **Answer: A) Man-in-the-middle (MITM) attack**

3. What type of vulnerability allows an attacker to execute arbitrary commands on a host operating system?

- A) Buffer overflow
- B) SQL injection
- C) Command injection
- D) Cross-site scripting (XSS)
- **Answer: C) Command injection**

4. Which vulnerability occurs when software does not properly protect sensitive information?

- A) Insecure direct object references
- B) Security misconfiguration
- C) Insecure deserialization
- D) Information disclosure
- **Answer: D) Information disclosure**

5. What vulnerability allows an attacker to impersonate another user by stealing their session token?

- A) Cross-site request forgery (CSRF)

- B) Session fixation

- C) Cross-site scripting (XSS)

- D) Broken authentication

- **Answer: B) Session fixation**

6. Which vulnerability arises from using outdated or vulnerable software?

- A) Security misconfiguration

- B) Insecure deserialization

- C) Using components with known vulnerabilities

- D) Insufficient logging and monitoring

- **Answer: C) Using components with known vulnerabilities**

7. What type of vulnerability allows an attacker to gain unauthorized access by exploiting weak or default credentials?

- A) Insufficient logging and monitoring

- B) Broken authentication

- C) Insecure direct object references

- D) Brute force attack

- **Answer: B) Broken authentication**

8. Which vulnerability occurs when an application does not properly protect sensitive data during transmission?

- A) Insecure deserialization

- B) Security misconfiguration

- C) Insufficient transport layer protection

- D) XML external entity (XXE) injection

- **Answer: C) Insufficient transport layer protection**

9. What vulnerability allows an attacker to bypass access controls by manipulating URLs?

- A) Insecure direct object references
- B) Security misconfiguration
- C) URL redirection
- D) Insufficient logging and monitoring
- **Answer: A) Insecure direct object references**

10. Which vulnerability allows an attacker to exploit a flaw in a cryptographic algorithm?

- A) Cryptographic issues
- B) Insufficient logging and monitoring
- C) Security misconfiguration
- D) Insecure deserialization
- **Answer: A) Cryptographic issues**

11. What type of vulnerability occurs when an application does not properly validate or sanitize input in XML documents?

- A) XML external entity (XXE) injection
- B) Broken authentication
- C) Insecure direct object references
- D) Insufficient transport layer protection
- **Answer: A) XML external entity (XXE) injection**

12. Which vulnerability allows an attacker to trick a user into clicking a malicious link or downloading a malicious attachment?

- A) Cross-site request forgery (CSRF)
- B) Phishing
- C) Spoofing
- D) Man-in-the-middle (MITM) attack
- **Answer: B) Phishing**

13. What vulnerability allows an attacker to manipulate an application into performing unauthorized actions?

- A) Broken access control

- B) Insufficient logging and monitoring

- C) Insecure deserialization

- D) Security misconfiguration

- **Answer: A) Broken access control**

14. Which vulnerability arises from not properly restricting the types of files that can be uploaded?

- A) Insufficient logging and monitoring

- B) Security misconfiguration

- C) Unrestricted file upload

- D) Insecure deserialization

- **Answer: C) Unrestricted file upload**

15. What type of vulnerability occurs when an application does not properly restrict the size or number of inputs it accepts?

- A) Insecure deserialization

- B) Buffer overflow

- C) Denial-of-Service (DoS) attack

- D) Insufficient logging and monitoring

- **Answer: C) Denial-of-Service (DoS) attack**

16. Which vulnerability occurs when an application does not properly validate or sanitize input in SQL queries?

- A) SQL injection

- B) Command injection

- C) XML external entity (XXE) injection

- D) Cross-site scripting (XSS)

- **Answer: A) SQL injection**

17. What vulnerability allows an attacker to manipulate an application into revealing confidential information?

- A) Information disclosure

- B) Security misconfiguration

- C) Insufficient transport layer protection

- D) Insufficient logging and monitoring

- **Answer: A) Information disclosure**

18. Which vulnerability occurs when an application does not properly protect sensitive information in memory?

- A) Insecure deserialization

- B) Security misconfiguration

- C) Memory leak

- D) Information disclosure

- **Answer: C) Memory leak**

19. What type of vulnerability allows an attacker to execute scripts in a victim's browser?

- A) Cross-site scripting (XSS)

- B) Cross-site request forgery (CSRF)

- C) XML external entity (XXE) injection

- D) Insufficient transport layer protection

- **Answer: A) Cross-site scripting (XSS)**

20. Which vulnerability allows an attacker to manipulate an application's business logic to gain unauthorized access?

- A) Broken access control

- B) Insufficient logging and monitoring

- C) Insecure deserialization

- D) Security misconfiguration

- **Answer: A) Broken access control**

21. What vulnerability allows an attacker to remotely execute code on a server?

- A) Command injection

- B) Remote code execution

- C) Buffer overflow

- D) Insufficient logging and monitoring

- **Answer: B) Remote code execution**

22. Which vulnerability occurs when an application does not properly restrict users from accessing unauthorized resources?

- A) Broken access control
- B) Insufficient logging and monitoring
- C) Insecure deserialization
- D) Security misconfiguration
- **Answer: A) Broken access control**