1. Which of the following is not a database security threat?
   1. Unauthorized access
   2. Data corruption
   3. **Database redundancy**
   4. Data theft
2. Which authentication method requires users to provide something they know?
   1. Biometric authentication
   2. Two-factor authentication
   3. **Password authentication**
   4. Token-based authentication
3. Which access control model assigns permissions to subjects and objects based on predefined rules?
   1. **Mandatory Access Control (MAC)**
   2. Role-Based Access Control (RBAC)
   3. Discretionary Access Control (DAC)
   4. Rule-Based Access Control (RBAC)
4. What is the primary goal of encryption in database security?
   1. Authentication
   2. Data integrity
   3. **Data confidentiality**
   4. Access control
5. Which of the following is an example of a physical database security measure?
   1. Database encryption
   2. Role-based access control
   3. **Network firewalls**
   4. Backup and recovery procedures
6. Which type of database attack involves flooding a database server with requests to disrupt its normal functioning?
   1. SQL injection
   2. **Denial-of-Service (DoS)**
   3. Buffer overflow
   4. Cross-site scripting (XSS)
7. What is the purpose of intrusion detection systems (IDS) in database security?
   1. Prevent unauthorized access to databases
   2. **Detect and respond to potential security breaches**
   3. Encrypt database connections
   4. Backup and restore databases
8. Which of the following is an example of a database security best practice?
   1. Storing passwords in plain text
   2. Sharing database credentials with colleagues
   3. **Regularly applying software patches and updates**
   4. Allowing anonymous access to the database
9. Which security measure ensures that users can access only the data they are authorized to view or modify?
   1. Database encryption
   2. **Access control**
   3. Intrusion detection
   4. Data masking
10. What is the purpose of data masking in database security?
    1. Preventing unauthorized access to the database
    2. **Protecting sensitive data by replacing it with realistic but fictitious data**
    3. Encrypting data during transmission
    4. Creating database backups for disaster recovery
11. Which database security measure involves defining user roles and granting permissions based on those roles?
    1. Database auditing
    2. Two-factor authentication
    3. **Role-based access control**
    4. Intrusion prevention system
12. Which of the following is an example of a database security vulnerability?
    1. Strong password policy
    2. Regular database backups
    3. **Lack of input validation**
    4. Encrypted database connections
13. What is the purpose of database auditing?
    1. Encrypting database backups
    2. **Monitoring and recording database activities**
    3. Preventing SQL injection attacks
    4. Managing user roles and permissions
14. Which security measure involves storing a hash value of a password instead of the actual password?
    1. Password encryption
    2. Password cracking
    3. **Password hashing**
    4. Password salting
15. Which type of database attack involves injecting malicious SQL code into an application's input fields?
    1. Cross-site scripting (XSS)
    2. Buffer overflow
    3. Denial-of-Service (DoS)
    4. **SQL injection**
16. What is the purpose of database backup and recovery procedures in database security?
    1. Encrypting database connections
    2. Monitoring and recording database activities
    3. **Protecting against data loss and corruption**
    4. Defining user roles and permissions
17. Which of the following is an example of a database security control?
    1. **Regular data backups**
    2. Database triggers
    3. Database normalization
    4. Database indexing
18. What is the purpose of database encryption?
    1. Preventing unauthorized access to the database
    2. Detecting and responding to security breaches
    3. **Protecting data confidentiality**
    4. Monitoring and recording database activities
19. Which of the following is an example of a database security breach?
    1. Regularly updating database software
    2. Using strong and unique passwords
    3. **Unauthorized access to sensitive data**
    4. Encrypting database connections
20. Which security measure involves securing database connections using SSL/TLS protocols?
    1. Database auditing
    2. Database normalization
    3. Database indexing
    4. **Database encryption**
21. What is the purpose of a firewall in database security?
    1. **Preventing unauthorized access to the database**
    2. Detecting and responding to security breaches
    3. Encrypting database connections
    4. Monitoring and recording database activities
22. Which of the following is an example of a database security policy?
    1. Two-factor authentication
    2. Intrusion detection system (IDS)
    3. **Password complexity requirements**
    4. Database normalization
23. What is the primary purpose of access control lists (ACLs) in database security?
    1. Encrypting database backups
    2. **Managing user roles and permissions**
    3. Monitoring and recording database activities
    4. Preventing SQL injection attacks
24. Which security measure involves regularly testing and validating the security of a database system?
    1. **Vulnerability scanning**
    2. Database indexing
    3. Database normalization
    4. Database auditing
25. What is the purpose of a database security incident response plan?
    1. Regularly updating database software
    2. **Detecting and responding to security breaches**
    3. Encrypting database connections
    4. Defining user roles and permissions
26. Which of the following is an example of a database security control at the application level?
    1. Two-factor authentication
    2. Regular data backups
    3. **Input validation**
    4. Database indexing
27. Data security threats include :
    1. privacy invasion
    2. hardware protection
    3. fraudulent manipulation od data
    4. **all of the above**
28. \_\_\_\_\_\_\_ is responsible for using that the database remains in a consistent state despite system failure.
    1. Storage manager
    2. **Transaction manager**
    3. End user
    4. Sophisticated
29. Prevention of access to the database by unauthorized users is referred to as :
    1. Integrity
    2. Productivity
    3. **Security**
    4. Reliability
30. Data integrity means :
    1. providing first access to stored data
    2. **ensuring correctness and consistency of data**
    3. providing data sharing
    4. none of the above