sql223

1. What is SQL Injection? How does it work? ■
2. What are the different types of SQL Injection? ■
   - Classic SQLi ■
   - Blind SQLi ■
   - Time-based SQLi ■
   - Error-based SQLi ■
3. How can you prevent SQL Injection in an application? ■
4. What are prepared statements and how do they help prevent SQL Injection? ■
5. What role does input validation play in preventing SQL attacks? ■
6. How does a Web Application Firewall (WAF) help prevent SQL Injection? ■
7. What is parameterized querying? Provide an example in SQL. ■
8. Can you explain the difference between White-listing and Black-listing input validation? ■
9. What is the impact of SQL Injection on a database? ■
10. What are the best practices for securing a database? ■
11. How do you implement Role-Based Access Control (RBAC) in SQL? ■
12. What is the principle of Least Privilege in database security? ■
13. How can you restrict user permissions in SQL? ■
14. What are stored procedures, and how do they help in security? ■
15. How do you audit user activities in a database? ■
16. What are SQL GRANT and REVOKE statements? How are they used? ■
17. What is Database Encryption? What are the types of encryption in SQL databases? ■
18. How do Transparent Data Encryption (TDE) and Column-Level Encryption work? ■
19. How can you prevent privilege escalation in SQL? ■
20. What is Data Masking, and how is it used in SQL databases? ■
21. What is the difference between hashing and encryption in database security? ■
22. How do GDPR and HIPAA regulations impact database security? ■
23. What is SQL Database Auditing? Why is it important? ■
24. How can you detect suspicious activities in an SQL database? ■
25. What are database security best practices for cloud-based databases? ■
26. How do you prevent unauthorized access to database backups? ■
27. What is the difference between database-level and application-level security? ■
28. What is a Man-in-the-Middle (MITM) attack in SQL? How do you prevent it? ■
29. What is a Timing Attack, and how can it be used in SQL? ■

30. What is a NoSQL Injection? How does it differ from SQL Injection? ■
31. How do you protect a database from insider threats? ■
32. What are the security risks of using dynamic SQL? ■
33. What are the risks of exposing database error messages to users? ■
34. How can you secure database connections over a network? ■
35. What is the role of database firewalls in cybersecurity? ■
36. How does SQL Server Always Encrypted protect sensitive data? ■
37. What are shadow databases, and how can they pose a security risk? ■
38. How would you detect if a system is under an SQL Injection attack? ■
39. A company experiences a data breach due to SQL Injection. What steps should they take to
40. You find that a user has access to more data than necessary. How would you resolve this iss
41. How would you secure API endpoints that interact with a SQL database? ■
42. You suspect that an attacker is trying to exploit a timing-based SQL Injection. What do you d
43. How would you ensure secure authentication and authorization in a database-driven web app
44. What logging and monitoring techniques would you use to detect SQL security threats? ■
45. You are asked to secure a legacy database with poor security practices. What steps would y