## **OWASP Top Ten (2021)**

The **Open Web Application Security Project (OWASP)** highlights the most critical security risks for web applications. The 2021 Top 10 list includes:

- 1. Broken Access Control
- 2. **Cryptographic Failures** (e.g., use of deprecated algorithms like MD5, SHA1)
- 3. Injection Attacks:
  - Example: Using unvalidated input in SQL queries, such as:
    SELECT \* FROM users WHERE username = 'userInput';
  - Risk: Queries that allow username = 'navin' OR 1=1 can expose all user data.
  - **Prevention**: Use prepared statements to prevent SQL injection.
- 4. Insecure Design
- 5. Security Misconfiguration (e.g., default configurations in use)
- 6. Vulnerable and Outdated Components
- 7. Identification and Authentication Failures
- 8. Software and Data Integrity Failures
- 9. Security Logging and Monitoring Failures
- 10.Server-Side Request Forgery (SSRF)

## **Note:**

You can see the latest top 10 OWASP attacks: OWASP Top 10 Attacks

