1. Initial Reconnaissance:

- **Information Gathering**: Collect all necessary details about the application, such as URLs, IP addresses, server details, and associated technologies.
- **Automated Scanning**: Use tools like OWASP ZAP, Burp Suite, or Nessus to perform initial automated scans to detect common vulnerabilities.

2. Authentication and Authorization Testing:

- **Brute Force Attacks**: Test for weak passwords and poor authentication mechanisms.
- **Session Management**: Ensure session tokens are secure, properly invalidated after logout, and not easily predictable.
- **Access Control**: Check for improper access controls, ensuring users can only access resources they're authorized to.

3. Input Validation:

- **SQL Injection**: Verify that user inputs are sanitized to prevent SQL injection attacks.
- **Cross-Site Scripting (XSS)**: Ensure that all inputs are properly validated and encoded.
- **Command Injection**: Test for vulnerabilities where user inputs are executed as commands on the server.

4. Configuration and Deployment Management:

- **Server Configuration**: Check for unnecessary services and open ports. Ensure that configurations follow best security practices.
- **Software Updates**: Ensure all components, including the web server, database, and libraries, are up to date with the latest security patches.

5. Data Protection:

- **Encryption**: Confirm that sensitive data is encrypted both in transit (using HTTPS) and at rest.
- **Error Handling**: Ensure that error messages do not expose sensitive information.
- **Data Backup**: Verify that regular data backups are performed and stored securely.

6. Business Logic Testing:

- **Workflow Testing**: Test for logic flaws that can be exploited, such as unauthorized fund transfers or privilege escalation.
- **Transaction Security**: Ensure that business processes are robust against manipulation.

7. Final Reporting and Mitigation:

- **Document Findings**: Prepare a comprehensive report detailing the vulnerabilities discovered and recommended fixes.
- **Implementation of Fixes**: Work with the development team to implement security patches and best practices.

- **Follow-up Testing**: Perform retesting to ensure that all vulnerabilities have been adequately addressed.