Tips for secured coding practices

1. Validate Inputs

Check everything users enter to make sure it's safe and as expected (e.g., numbers should be numbers, not letters).

2. Encode Outputs

Protect your website by converting special characters (like <, >) into safe versions before showing them to users.

3. Strong Authentication

Use strong passwords and multi-factor authentication to make sure only the right people can access your application.

4. Limit Access

Give the least amount of access needed for users and programs to do their job—no more.

5. Encrypt Data

Protect sensitive information by encrypting it when stored and during transmission.

6. Handle Errors Carefully

Don’t show technical error details to users; instead, log them securely for developers to review.

7. Use Secure Libraries

Only use trusted and up-to-date third-party libraries and tools to avoid known vulnerabilities.

8. Secure Communication

Use HTTPS to encrypt data being sent between the user and your server.

9. Regular Security Testing

Test your code regularly for vulnerabilities using tools and manual reviews.

10. Educate Your Team

Teach developers about security best practices to keep everyone on the same page.

Following these simple steps helps protect your application from common security risks and makes it more robust against attacks.