Secure Coding Practices Checklist

OWASP practices mapped to CWE mitigations

Input Validation

- ■ All user input validated on the server side
- ■ Input length, type, and range constraints enforced
- ■ Allow-list validation preferred over deny-list
- ■ File uploads restricted by type, size, and scanned for malware

Output Encoding

- ■ Context-appropriate output encoding applied (HTML, JS, URL, CSS)
- ■ Parameterized queries used for all database operations
- ■ Content-Type headers set correctly on all responses
- ■ CSP headers configured to prevent XSS

Authentication & Session

- ■ Passwords hashed with Argon2id/bcrypt (never stored in plaintext)
- ■ Multi-factor authentication available for sensitive operations
- ■ Session tokens are random, sufficient length, and HTTP-only
- ■ Session invalidated on logout and after timeout

Error Handling & Logging

- ■ Generic error messages shown to users (no stack traces)
- ■ Errors logged with context but without sensitive data
- ■ Security events logged (auth failures, privilege changes, access denials)
- ■ No secrets, PII, or tokens in log output

AI-Generated Code

- ■ All AI-generated code reviewed for OWASP Top 10 vulnerabilities
- ■ AI output validated against security requirements before merge
- ■ AI-generated code tagged with provenance markers