SQL INJECTION REVIEW

Areas to evaluate for potential SQL Injection attacks.

DATABASE

- Sufficient and appropriate database user permissions set
- Extraneous or unused database features disabled
- Database logging enabled
- Database backup / restore procedure
- Database connection filtering procedures enabled (example: MySQL has options to prevent execution of multiple SQL statements in a single query)
- Database drivers up to date

APPLICATION

- Using filtering options
- Using parameterization options
- Using DB calls only when needed? (Could you use a static site generator?)
- Code lint/checks for potential SQL injection points
- Manual check for SQL Injection prone points
- Application logging

WEB SERVER OR WEB APPLICATION FIREWALL

- Use WAF SQL Injection pre-filters
- Rate limit to prevent mass SQL Injection attempts
- Alert on SQL Injection pattern attempts