security-requirements

Top 10 Basic Security Requirements for Python Code

Input Validation
All user inputs must be validated for correct type, length, format, and range to prevent injection attacks.

Secure Password Storage
Passwords must be hashed using strong cryptographic algorithms (e.g., bcrypt, Argon2) with appropriate salting, never stored in plaintext.

Secure Authentication
Implement proper authentication with rate limiting, account lockouts after failed attempts, and secure session management.

Protection Against SQL Injection
Use parameterized queries or ORM frameworks when interacting with databases instead of string concatenation.

Secret Management
API keys, tokens, and credentials must be stored in secure environment variables or dedicated secret management tools, never hardcoded.

Secure File Operations
Validate file paths, types, and operations to prevent path traversal attacks and unauthorized file access.

HTTPS Communication
All network traffic must use HTTPS with valid certificates; insecure HTTP should not be used for sensitive information.

Logging & Error Handling
Implement proper error handling without exposing sensitive information in error messages; maintain secure audit logs.

Regular Dependency Updates
Keep all dependencies updated to address known vulnerabilities through regular security patches.

Principle of Least Privilege
Code should only request and use the minimum permissions necessary to function correctly.