Web Application Security Checklist

Authentication & Session Management

- Enforce strong password policies (length, complexity).
- Implement Multi-Factor Authentication (MFA).
- Secure session ID generation and handling (HttpOnly, Secure flags).
- Implement proper session timeout and termination.

Access Control

- Enforce Principle of Least Privilege.
- Verify object references (IDOR prevention).
- Restrict access to administrative interfaces.

Input Validation & Output Encoding

- Validate all input against a strict allow-list.
- Encode all output to prevent XSS.
- Use parameterized queries to prevent SQLi.

Cryptography

- Use strong, modern encryption algorithms (AES-256, RSA-2048).
- Hash passwords using strong hashing algorithms (Argon2, bcrypt).
- Manage keys securely.