

Angular Security Checklist (Production-Ready)

This checklist is designed for Senior / Lead Angular engineers to validate frontend security before production deployment.

1. XSS Protection

- Avoid using innerHTML and direct DOM manipulation
- Never use bypassSecurityTrust* unless content is fully trusted
- Use Angular template bindings ({{ }})
- Enable strict Content Security Policy (CSP)

2. Authentication & Tokens

- Do not store JWT in localStorage or sessionStorage
- Prefer HttpOnly, Secure cookies
- Use short-lived access tokens with refresh tokens
- Always enforce authentication on backend APIs

3. CSRF Protection

- Use cookie-based authentication with XSRF tokens
- Enable HttpClientXsrfModule
- Do not disable XSRF protection in production

4. Authorization

- Never rely on route guards for security
- Validate roles and permissions on backend
- Prevent IDOR by validating resource ownership

5. Routing & Navigation

- Avoid exposing sensitive data in route parameters
- Do not trust query params or route params
- Protect admin routes at API level

6. Angular Universal (SSR)

- Never expose secrets in TransferState
- Strip sensitive data before server-side rendering
- Validate user context on server

7. HTTP & Network Security

- Force HTTPS with HSTS enabled
- Use secure headers: CSP, X-Frame-Options
- Prevent clickjacking with frame-ancestors none

8. Dependency & Build Security

- Audit npm dependencies regularly
- Lock dependency versions
- Remove unused libraries
- Scan CI pipeline for vulnerabilities

9. Frontend Logic & UI

- Do not trust frontend feature flags
- Hide UI is not security
- Prevent over-privileged client logic

10. Production Hardening

- Disable Angular debug tools in prod
- Enable strict TypeScript mode
- Log security events on backend
- Monitor anomalies and abuse