Rails Security Checklist

15 essential security measures for every Rails application.

Essential security measures for every Rails application. Use this checklist to audit your app's security posture.

Rails Version

- [ ] Running latest stable Rails version
- [ ] No known CVEs for your Rails version

Dependencies

- [ ] Gems audited for CVEs (bundler-audit)
- [ ] Dependabot or Renovate configured
- [ ] Outdated gems identified and scheduled for update

HTTP Security Headers

- [ ] HSTS (Strict-Transport-Security) enabled
- [ ] Content Security Policy (CSP) configured
- [ ] X-Frame-Options set (SAMEORIGIN or DENY)
- [ ] X-Content-Type-Options: nosniff set

SSL/TLS

- [ ] HTTPS enforced across all routes
- [ ] Valid SSL certificate (no expirations)
- [ ] TLS 1.2 or higher enforced

Application Security

- [ ] CSRF token protection enabled
- [ ] SQL injection prevention (parameterized queries)
- [ ] XSS prevention (output escaping)
- [ ] Secure session cookie configuration

Infrastructure

- [ ] Rate limiting configured
- [ ] Brute force protection (Rack::Attack)
- [ ] Secrets management (not in code)
- [ ] Dependency scanning in CI