Web Application Security Checklist

Practical pre-launch checks for any web app. Tick what's done; investigate what isn't.

Authentication & sessions

- [ ] Enforce strong passwords and offer MFA on all accounts
- [ ] Lock out or rate-limit repeated failed logins
- [ ] Use secure, HttpOnly, SameSite session cookies
- [ ] Invalidate sessions on logout and password change
- [ ] Protect password reset flows against account takeover

Authorization & access control

- [ ] Enforce server-side authorization on every request (no trusting the UI)
- [ ] Apply least privilege for users, services, and API keys
- [ ] Prevent insecure direct object reference (IDOR) by checking ownership
- [ ] Separate admin functions and protect them tightly

Input handling

- [ ] Validate and sanitize all user input server-side
- [ ] Use parameterized queries to prevent SQL injection
- [ ] Encode output to prevent cross-site scripting (XSS)
- [ ] Protect state-changing actions with anti-CSRF tokens
- [ ] Restrict and validate file uploads (type, size, storage)

Transport, headers & config

- [ ] Force HTTPS everywhere with HSTS enabled
- [ ] Set security headers: CSP, X-Content-Type-Options, Referrer-Policy
- [ ] Disable directory listing and remove debug endpoints in production
- [ ] Keep frameworks and dependencies patched

Data, logging & monitoring

- [ ] Encrypt sensitive data at rest and in transit
- [ ] Never log secrets, tokens, or full card/PII data
- [ ] Log security events and monitor for anomalies
- [ ] Have backups and a tested restore process

guardioninfosec@gmail.com