Security Rubric

CRITERION	1	2	3	4	5
Input sanitization	Raw user input in innerHTML, no output encoding, SQL concatenation	Some escaping but inconsistent, dangerouslySetInnerHTML in use	Framework auto-escaping relied on, parameterized queries	CSP headers, DOMPurify for rich content, input validation schemas	Strict CSP, automated XSS scanning in CI, no raw HTML paths
Auth & sessions	Tokens in localStorage, no CSRF protection, shared credentials	HttpOnly cookies but no refresh rotation, weak session expiry	Token refresh, CSRF tokens, role-based access on API routes	Short-lived JWTs, server-side session validation, MFA available	Zero-trust middleware, device binding, session anomaly detection
Dependency security	No lock file, outdated deps with known CVEs, no audit process	Lock file exists but `npm audit` warnings ignored	Regular audits, critical CVEs patched within a week	Automated Dependabot/Renovate, audit gate in CI pipeline	SBOM tracked, zero known vulnerabilities, license compliance
Secrets management	API keys hardcoded in source, .env committed to git	.env in .gitignore but secrets shared via chat, no rotation	Env vars via hosting platform, server-only access enforced	Vault/KMS for secrets, automatic rotation, least-privilege scoping	Secret scanning in CI, no long-lived credentials, audit trail