Vibe coding security applications checklists:

1. **CORS Configuration:** Restrict Cross-Origin Resource Sharing (CORS) to permit requests exclusively from my specified domain.
2. **Redirect URL Validation:** Before redirecting a user, validate all redirect URLs against a predefined allowlist.
3. **Supabase Storage RLS Policy:** Implement Row-Level Security (RLS) policies in Supabase Storage. The policy must ensure that users can only access files they personally uploaded.
4. **Pre-Deployment Clean-up:** Prior to deployment, eliminate all `console.log` statements and replace them with a robust error logging mechanism.
5. **Webhook Signature Verification (Stripe):** Explicitly instruct the AI to use Stripe's SDK to verify the webhook signature before processing any payment data.
6. **Admin Role Check:** For every protected route, perform a server-side check to confirm that `user.role` is equal to `'admin'` before executing the route's logic.
7. **Post-Build Security Audit:** After the build process, execute `npm audit fix`. Subsequently, query the AI for known breaking changes in the latest library versions.
8. **Rate Limiting (Password Reset):** Apply rate limiting to the password reset route, restricting it to a maximum of 3 requests per email address per hour.
9. **Error Handling and Logging:** Implement comprehensive error catching. Return generic error messages to end-users while logging detailed, server-side errors internally only.
10. **JWT and Refresh Token Management:** Set the JSON Web Token (JWT) expiration to 7 days and implement a system for refresh token rotation.