# CV Builder Project: Security & Launch Readiness Checklist

## Environment & Sensitive Data Management

* ☐ Ensure .env files are properly excluded using .gitignore (confirmed).
* ☐ Create .env.example files to document required environment variables for development and deployment.

## Dependency & Code Security

* ☐ Run 'npm audit fix' and 'npm outdated' to identify and fix known vulnerabilities.
* ☐ Update critical dependencies related to authentication and encryption (e.g., jsonwebtoken, bcrypt).

## API & Input Validation

* ☐ Ensure express-rate-limit or similar middleware is used to prevent brute-force attacks.
* ☐ Verify that all API endpoints handling sensitive operations (login, register, password reset) have throttling in place.
* ☐ Validate and sanitize all user inputs, especially file uploads and AI processing inputs.
* ☐ Enforce allowed MIME types and size limits for file uploads.

## Payment Processing Security

* ☐ Confirm all payment processing is handled through Stripe’s hosted Checkout or Payment Intents API (confirmed).
* ☐ Ensure no card data is stored or processed on your servers.

## Application & Infrastructure Security

* ☐ Implement Helmet middleware in Express to set HTTP security headers.
* ☐ Enforce HTTPS site-wide through Cloudflare or web server configuration.
* ☐ Enable AWS RDS database encryption at rest.
* ☐ Verify AWS S3 buckets have AES-256 encryption and strict access policies (no public access).

## Monitoring & Logging

* ☐ Integrate Sentry or AWS CloudWatch for application error logging and monitoring.
* ☐ Ensure all critical errors are properly logged and not only printed to console.

## Compliance & Legal

* ☐ Draft and publish a clear Privacy Policy and Terms of Service on your website.
* ☐ Implement a Data Retention Policy outlining how long user data (CVs, job specs) is stored.
* ☐ Ensure GDPR compliance by providing users with options to delete their data.