Security & Data Privacy Policy

Table des matières

1. Overview

Trips & Roads is committed to protecting user data through a "Privacy by Design" approach. Since this is an educational project at IUT Lyon 1, we prioritize transparency regarding how data is stored, processed, and secured.

2. Security Architecture

A. Authentication & Hashing

- **Password Encryption:** We never store plain-text passwords. We use CakePHP's built-in DefaultPasswordHasher, which utilizes the **bcrypt** algorithm.
- **Security Salt:** Every installation uses a unique Security.salt defined in app_local.php to secure the generation of hashes and tokens.

B. Data Protection

- **SQL Injection Prevention:** By using the CakePHP ORM (as seen in RoadtripsController.php), all database queries are prepared, effectively neutralizing SQL injection risks.
- **CSRF Protection:** We enable Cross-Site Request Forgery (CSRF) middleware to ensure that all form submissions (Contact, Roadtrip creation) originate from our domain.

3. Data Privacy (GDPR Compliance)

A. Collected Information

We limit data collection to what is strictly necessary for the service:

- **Mandatory:** Email, Name, and encrypted Password for account creation.
- **Optional:** Profile picture, birthdate, and residence city.
- **Usage Data:** Trip plans, waypoints, and shared comments.

B. Data Retention & Deletion

- **Retention:** Data is kept as long as the user account is active.
- **Right to Erasure:** In accordance with the GDPR, users can request the permanent deletion of their account and all associated road trips via the contact form.

C. Cookie Management

We do **not** use tracking or advertising cookies. Our cookies are strictly functional:

- PHPSESSID: Maintains the user session.
- csrfToken: Ensures security for form submissions.
- remember_me: Optional cookie for persistent login.

4. API Security

- **Gemini API:** The API key is stored server-side in app_local.php. It is never exposed to the frontend (client-side), preventing unauthorized use of our AI quotas.
- **Nominatim & OSRM:** We respect the "Usage Policy" of OpenStreetMap by implementing client-side throttling to avoid overwhelming their free tier servers.