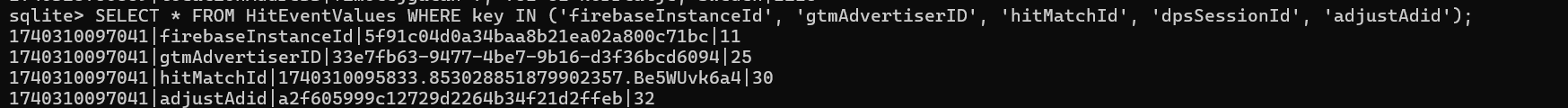
Foodora\_ App  
  
- generic\_x86:/data/data/se.onlinepizza/databases # sqlite3 /data/data/se.onlinepizza/databases/pandora.db.perseus

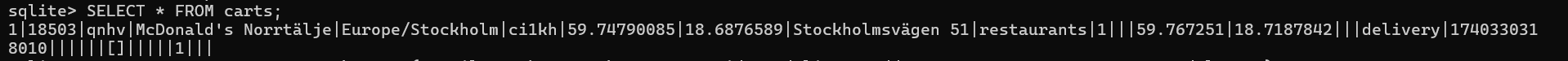
A computer screen with numbers and letters

AI-generated content may be incorrect.

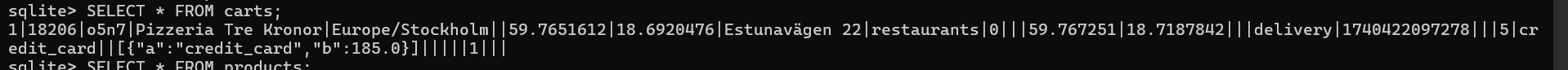
* Storing precise location data (latitude, address, city) could expose user privacy if leaked.



* These identifiers could be used to track users across sessions or devices.

  
  
**This is a security vulnerability**, particularly because **user location data is stored in plaintext**, potentially exposing users’ **movements and order history**.

**push Notification Token**: The registration\_id is a Firebase Cloud Messaging (FCM) token used for push notifications. If exposed, it could be used to send malicious notifications to the use

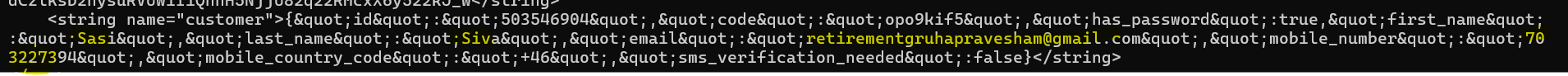


1. **Plaintext Storage of Payment Data**:
   * The carts table stores payment\_method (e.g., credit\_card) in plaintext.
2. **Exposure of Vendor Details**:
   * The carts table stores vendor\_address (e.g., Estunavägen 22) in plaintext.
3. **Lack of Encryption**:
   * Sensitive fields (e.g., payment\_method, vendor\_address, user\_id) are not encrypted.

A black screen with white text

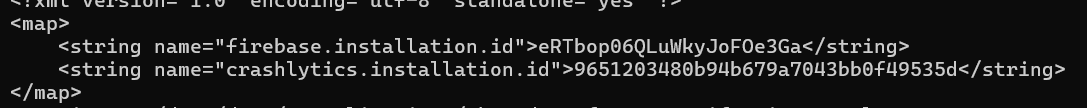
AI-generated content may be incorrect.

* OAuth tokens (access\_token, refresh\_token), FCM tokens, and push notification tokens are stored in plaintext.
* "id": "503546904",
* "code": "opo9kif5",
* "has\_password": true,
* "first\_name": "Sasi",
* "last\_name": "Siva",
* "email": "retirementgruhapravesham@gmail.com",
* "mobile\_number": "703227394",
* "mobile\_country\_code": "+46",
* "sms\_verification\_needed": false
* }



* Email,user\_id, mobile number, and full name are stored in plaintext.
* **Tracking IDs**:
  + Firebase, Crashlytics, and Google Ad IDs are stored in plaintext, enabling user tracking.

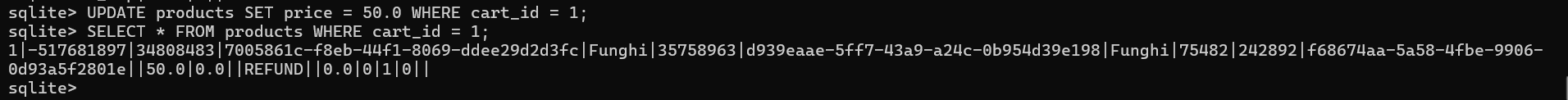






A screenshot of a phone

AI-generated content may be incorrect.



* + I set the price in the cart for that product is 50. So I added 3 in the cart and its updated to 150kr.

Despite utilizing various tools and techniques such as **Frida**, **Objection**, and **SSL pinning bypass scripts**, intercepting and modifying the **Foodora app** has proven to be highly challenging due to its robust security mechanisms. The app employs **certificate pinning**, a security feature that ensures it communicates only with trusted servers .