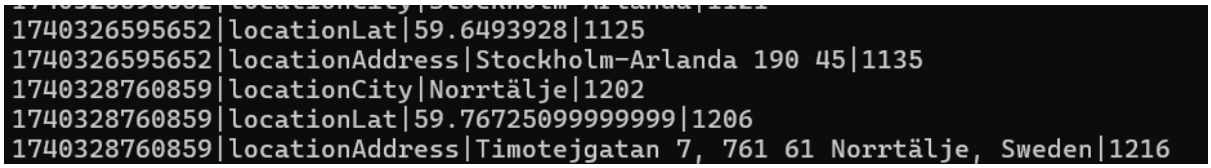
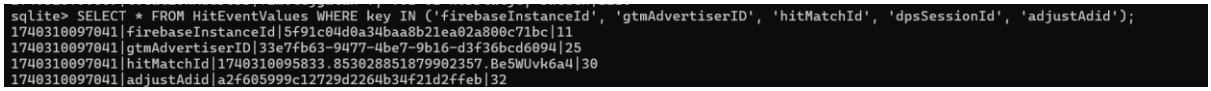
Foodora_ App

- generic_x86:/data/data/se.onlinepizza/databases # sqlite3 /data/data/se.onlinepizza/databases/pandora.db.perseus



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

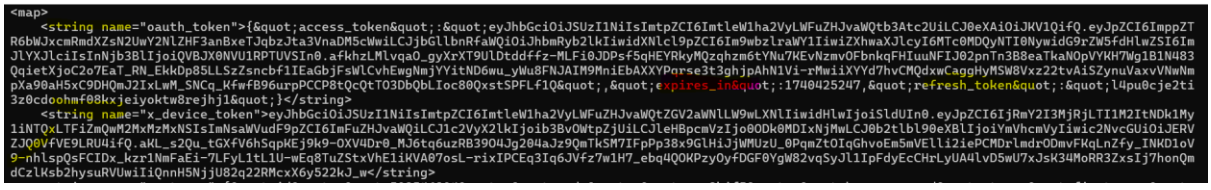


- These identifiers could be used to track users across sessions or devices.

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.



- 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
}
```



```
<string name="customer">{&quot;id&quot;:&quot;503546904&quot;,&quot;code&quot;:&quot;opo9kif5&quot;,&quot;has_password&quot;:true,&quot;first_name&quot;:&quot;Sasi&quot;,&quot;last_name&quot;:&quot;Siva&quot;,&quot;email&quot;:&quot;retirementgruhapravesham@gmail.com&quot;,&quot;mobile_number&quot;:&quot;703227394&quot;,&quot;mobile_country_code&quot;:&quot;+46&quot;,&quot;sms_verification_needed&quot;:false}</string>
```


- 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.

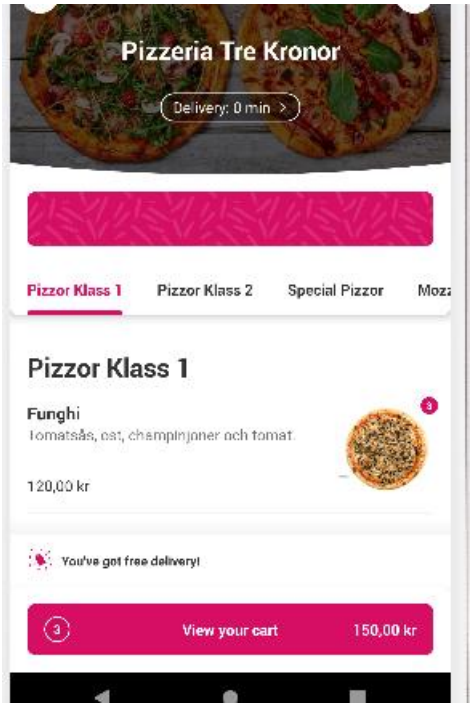

```
<string name="app_instance_id">0a7fbe1cef3af15ea108356e0ed971eb</string>
```



```
<map>
    <string name="firebase.installation.id">eRTbop06QLuWkyJoFOe3Ga</string>
    <string name="crashlytics.installation.id">9651203480b94b679a7043bb0f49535d</string>
</map>
```



```
google_ad_id&quot;:&quot;33e7fb63-9477-4be7-9b16-d3f36bcd6094&quot;
```

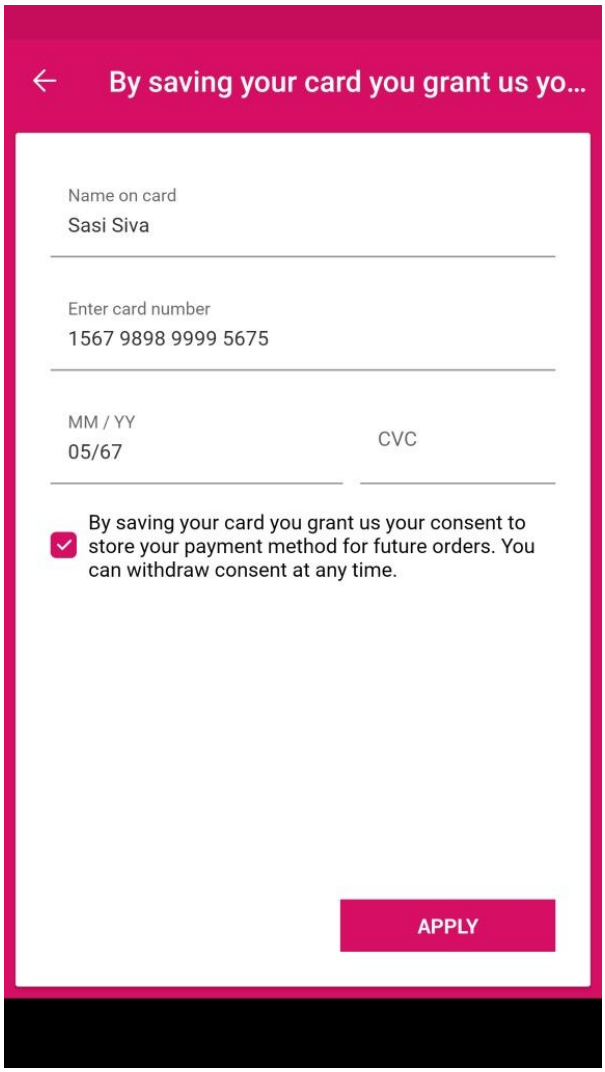




```
sqlite> UPDATE products SET price = 50.0 WHERE cart_id = 1;
sqlite> SELECT * FROM products WHERE cart_id = 1;
1|-517681897|34808483|7005861c-f8eb-44f1-8069-ddee29d2d3fc|Funghi|35758963|d939eaae-5ff7-43a9-a24c-0b954d39e198|Funghi|75482|242892|f68674aa-5a58-4fbe-9906-0d93a5f2801e||50.0|0.0||REFUND||0.0|0|1|0||
sqlite>
```

- 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 .

- During my analysis, I found that sensitive payment card details (including card number, expiry date, and CVV) are being stored in plaintext within the /data/system_ce/0/snapshots/ directory on the device/emulator. This allows unauthorized access to payment information, violating security best practices and compliance regulations.




```
PS C:\Users\yamin\AppData\Local\Android\Sdk\platform-tools> adb pull /data/system_ce/0/snapshots/
/data/system_ce/0/snapshots/: 9 files pulled, 0 skipped. 6.3 MB/s (306029 bytes in 0.046s)
PS C:\Users\yamin\AppData\Local\Android\Sdk\platform-tools>
```