Foodora_App

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

```
1740326595652|locationLat|59.6493928|1125
1740326595652|locationAddress|Stockholm-Arlanda 190 45|1135
1740328760859|locationCity|Norrtälje|1202
1740328760859|locationLat|59.76725099999999|1206
1740328760859|locationAddress|Timotejgatan 7, 761 61 Norrtälje, Sweden|1216
```

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

```
sqlite> SELECT * FROM HitEventValues WHERE key IN ('firebaseInstanceId', 'gtmAdvertiserID', 'hitMatchId', 'dpsSessionId', 'adjustAdid');
1740310097041|firebaseInstanceId|5F91c04d0a34baa8b21ea02a800c71bc|11
1740310097041|gtmAdvertiserID|33e7fb63-9477-4be7-9b16-d3f36bcd6094|25
1740310097041|hitMatchId|1740310095833.85815895902357.8e5WUvk6a4|30
1740310097041|adjustAdid|a2f605999c12729d2264b34f21d2ffeb|32
```

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

```
sqlite> SELECT * FROM carts;
1|18503|qnhv|McDonald's Norrtälje|Europe/Stockholm|ci1kh|59.74790085|18.6876589|Stockholmsvägen 51|restaurants|1||59.767251|18.7187842|||delivery|174033031
8010|||||||||||||||
```

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

```
sqlite> SELECT * FROM carts;
1|8286|567|Pizzeria Tre Kronor|Europe/Stockholm||59.7651612|18.6920476|Estunavägen 22|restaurants|0||59.767251|18.7187842|||delivery|17404422097278|||5|credit_card||[{*a":"credit_card","b":185.0}||||||||||
```

1. Plaintext Storage of Payment Data:

• The carts table stores payment_method (e.g., credit_card) in plaintext.

2. Exposure of Vendor Details:

o 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.

<map>
<map
<map>
<map
<map>
<map
<map>
<map

• 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",

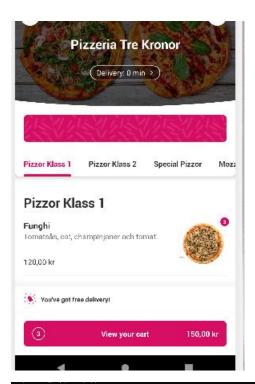
"mobile_country_code": "+46",

"sms_verification_needed": false
}
```

string name="oustomer">[Equot;idEquot;idEquot;:Equot;idSquot;idequot;idsquot;i

- 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.

google_ad_id":"33e7fb63-9477-4be7-9b16-d3f36bcd6094"



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.

