1. Used **ADB Shell** to access the app’s internal storage:

***adb shell***

***su***

***cd /data/data/com.sl.SLBiljetter/shared\_prefs/***

***ls***

***cat release\_remote\_config.xml***

1. Navigated to the app’s **Shared Preferences** directory and found

A black screen with white text

AI-generated content may be incorrect.

1. Found **API keys and tokens** inside the release\_remote\_config.XML.

A screen shot of a computer screen

AI-generated content may be incorrect.

1. Extracted **sensitive JSON data** from release\_remote\_config.xml (contained **API keys, secrets, tokens**). And The JSON contains multiple API keys and secrets, which, if valid, could allow unauthorized access to SL services.
2. If "psa\_auth" is an authentication key used for user authorization, an attacker could use it to gain unauthorized access to services.

A screen shot of a computer

AI-generated content may be incorrect.

1. Then **Validated JSON using Python script**

A screenshot of a computer

AI-generated content may be incorrect.

1. **test API keys and secrets** by sending requests to the **SL APIs**

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.