Escape Room CTF – Question-Based Solving Guide

Created by: Varun S (21PC26), Vishnupriya R (21PC39)

Overview

This CTF is designed as a mobile *escape room* where each challenge provides a riddle or vulnerability hint. Solvers must identify the vulnerability and then exploit it to reveal a flag.

FLAG 1: Hardcoded Secrets

Prompt: Initial welcome screen with a flag input box.

- Are there hardcoded flags or secrets in strings.xml? If yes, find out the hardcoded flag that takes you to the next task.

FLAG 2: Insecure Data Storage

Prompt: Riddle — "In plain sight, your data I keep, No locks, no codes, just a careless heap."

Guiding Questions:

- Are the login credentials in the prompt hardcoded in the code? If yes, use them to proceed to the next Intent.
- Where is the flag stored? (Shared Preferences, SQLite DB, File Storage?)
- Can you decode any base64 strings from shared_prefs?
- What database is used, and which table contains flag data?
- Is XOR encryption used on file-stored data? What's the key?

FLAG 3: Insecure Deeplinks

Prompt: Riddle — “I’m a shortcut to a hidden place, but unchecked, I’m a hacker’s ace.”

Guiding Questions:

- What parameters are accepted by the Deeplink Handler?
- Can the key be guessed or found in the code or from hints in the UI?
- Can you construct and execute a malicious deep link using ADB?

FLAG 4: SQL Injection

Prompt: Riddle — “I speak the language of databases, but my words can access hidden places.”

Guiding Questions:

- Is there an SQL query in the login code vulnerable to input manipulation?
- Does the username/password field accept SQL payloads? If yes, can you construct a payload to bypass authentication?

FLAG 5: Frida – Bypassing PIN Validation

Prompt: 4-digit PIN entry screen

Guiding Questions:

- Where is the PIN validation logic located?
- Can you hook the necessary function and return true? If yes, document how you can use Frida to attach to the app and override functions?

FLAG 6: Frida – Bypassing License Verification

Prompt: License Invalid screen

Guiding Questions:

- Can you hook any function in code using Frida and override its return value to bypass the License Invalid Screen?
- Once bypassed, does clicking “Next Flag” proceed to success?