Secure Mobile Software Development Modules

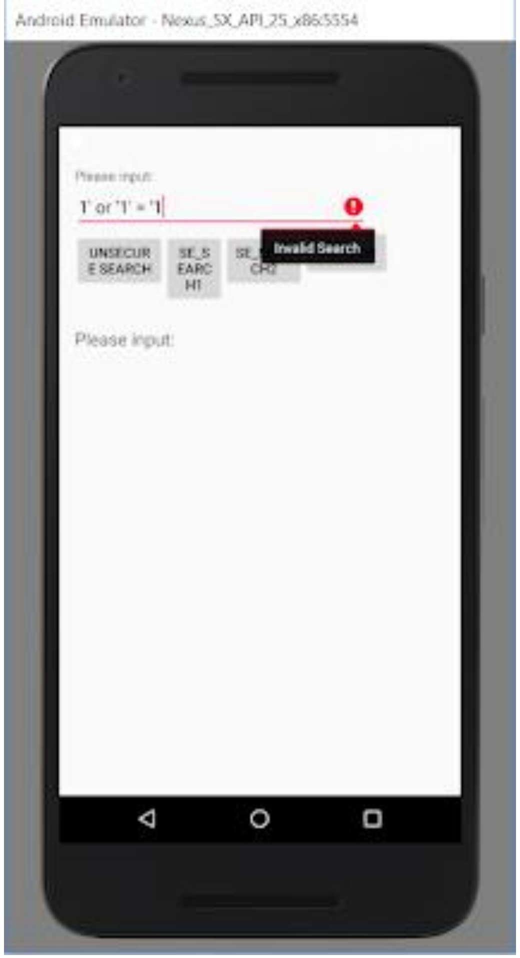
Introduction

- Many Android smartphones compromised because users download malicious software disguised as legitimate apps
- Malware vulnerabilities can lead to:
  - Stolen credit card numbers, financial loss
  - Stealing user’s contacts, confidential information
- Frequently, unsafe programming practices by software developers expose vulnerabilities and back doors that hackers/malware can exploit
- Examples:
  - Attacker can send invalid input to your app, causing confidential information leakage

Secure Mobile Software Development (SMSD)

- **Goal:** Teach mobile (Android) developers about backdoors, reduce vulnerabilities in shipped code

- SMSD:
  - Hands-on, engaging labs to teach concepts, principles
  - Android plug-in: Highlights, alerts Android coder about vulnerabilities in their code
  - Quite useful



Android Emulator - Nexus_5X_API_25_x86:5554

Please input:

1' or '1' = '1

Invalid Search

Please input:

SMSD: 8 Modules

- M0: Getting started
- M1: Data sanitization for input validation
- M2: Data sanitization for output encoding
- M3: SQL injections
- M4: Data protection
- **M5: Secure inter-process communication (IPC)**
- M6: Secure mobile databases
- M7: Unintended data leakage
- **M8: Access control**

- You should
  - Pre-Survey
  - **Lab:** Go through M5, M8
  - Post-survey afterwards

M5 & M8 Overview

- M5: Intra-app IPC vulnerabilities
- 2 security loopholes
  - **Intent Eavesdropping:** Malicious app can **receive** intent not meant for it
  - **Intent Spoofing:** Malicious app inserts (**send**) undesired behavior into a component using the implicit intent

- M8: Inter-App Secure IPC vulnerabilities
  - Malicious app can exploit security loophole in Broadcast Receivers to intercept valuable information

Important: This Lab REPLACES Worst Quiz

- Counts as quiz 6
- I will drop your worst quiz and replace it with score from SMSD
- Basically, I will use your best 5 scores
- Just do this lab online,
- Due 11.59, Friday, December 14, 2018