botCTF - Mobile Security Challenge

Vishal Ram V A (21PC38), Yamuna Shree P (21PC40)

Flag Format: bot{...}

Challenge 1: Broken Authentication

Guiding Questions:

1. Can you locate any hardcoded credentials inside the APK?
2. Which class or method is handling the login process?
3. What happens when you try submitting dummy credentials?
4. What response or activity is triggered upon successful login?

Tools: Jadx, apktool

Challenge 2: Conditionally Yours

Guiding Questions:

1. What boolean condition governs flag access?
2. Can you override this value at runtime without modifying the APK?
3. How can Frida be used to alter variable values during execution?
4. Is there any log output or toast message triggered when condition is met?

Tools: Frida, Jadx

Challenge 3: Location Spoofing

Guiding Questions:

1. Where in the app is the location retrieved or validated?
2. Are there any hardcoded latitude/longitude values?
3. Can you identify location APIs being used in Smali or Java?
4. What value needs to match to reveal the flag?

Tools: Frida, Jadx

Challenge 4: BotCoded Cipher

Guiding Questions:

1. Is there any encoded string or obfuscated logic in the app?
2. What kind of cipher might be used?
3. Can you reverse-engineer the decoding logic in Smali/Java?
4. Does a correct decoded input unlock the flag?
5. What's the expected decoded value to submit?

Tools: Python, Jadx

Challenge 5: Intercept & Execute

Guiding Questions:

1. Which broadcast receiver is exported in AndroidManifest.xml?
2. Can you send a custom broadcast via ADB to trigger an action?
3. What happens when you inspect the WebView through DevTools?

Tools: ADB, Chrome DevTools

Challenge 6: Arbitrary Code Execution

Guiding Questions:

1. What method is used to load and execute code in the app?
2. Can you inject a .dex file containing your own class?
3. How does HiddenDebugActivity trigger arbitrary execution?

Tools: NDK, javac, jar, d8, ADB

Using the CTFBot

Available Bot Commands:

- /list – View all challenges
- /help – Syntax help
- /hint "<challenge_name>" – Get a hint
- /flag "<challenge_name>" "<flag>" – Submit a flag

Track your progress with the “View Progress” button in the bot interface.