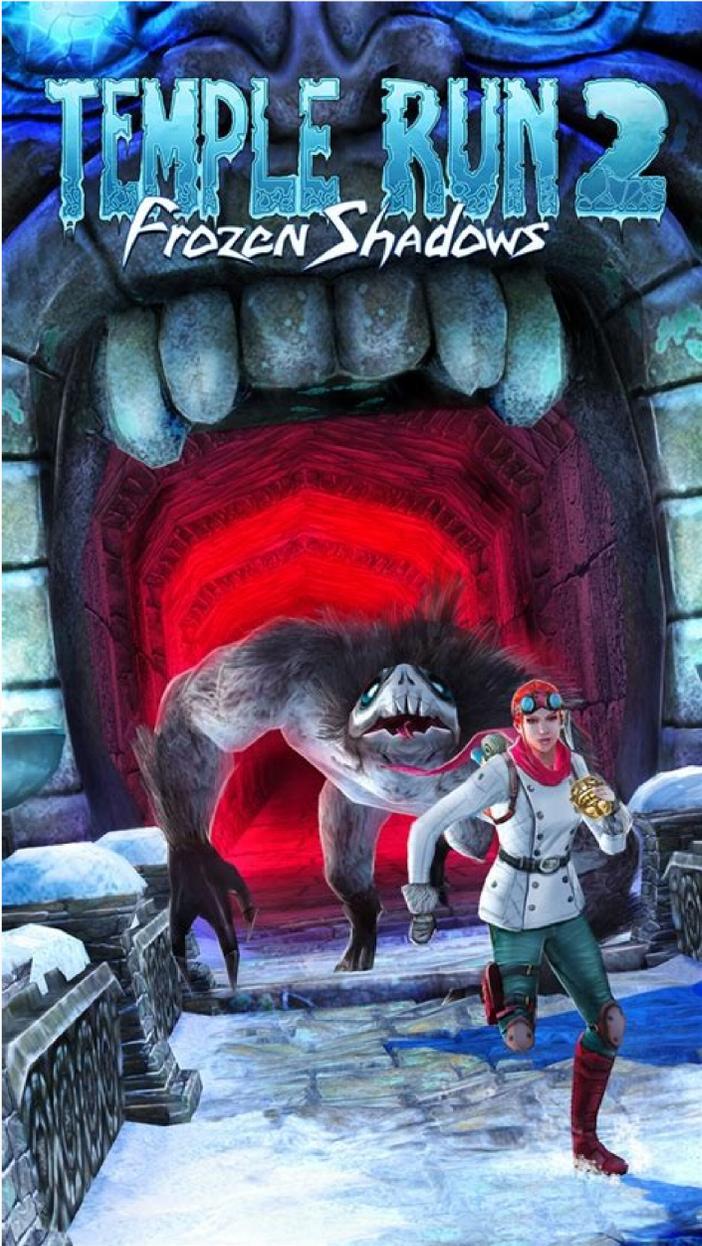


How to run android app on localhost

Continue



Today I will show you how you can convert your existing React js app to an android or ios app using ionic capacitor. So what exactly is Capacitor? According to documentation Capacitor is a cross-platform app runtime that makes it easy to build web apps that run natively on iOS, Android, Electron, and the web. We call these apps "Native Progressive Web Apps" and they represent the next evolution beyond Hybrid apps. So today we will build our android or ios app using the existing react app. Requirements Existing React Application Android Studio Xcode First, go to the root of your existing react app and create a file capacitor.config.json and inside that put the below code. 2. Now create another file name ionic.config.json and inside that insert the below code. Note: replace nameofyourapp in both files with the name of your app. 3. Now we need to build our react project. To build your react app open your terminal to the root of the project and run the below-mentioned command Note: this will create the build folder in your root project and the name of the folder should match the webDir name inside capacitor.config.json file. 4. Now we will install ionic globally in our machine. To install ionic globally in your machine open your terminal and run the below command. 5. Now install the capacitor core in our project. Android 6. After that, we will first create an android app with our existing react app. Open your terminal and type This will create the android folder in your root project and install all the required dependencies. 7. Now run the below command to open your android project in android studio. Wait some time and then it will ask you to update the Gradle. Just update the Gradle to the latest version and run the project in the emulator. You can also connect your mobile to run the project live on your mobile phone. 8. Now open the build menu from the android studio and build your apk file. iOS 9. To create ios app run the below command This will install all the required dependencies and ios folder to your project. 10. Now run the below command to open your ios project in Xcode. 11. Now open the app in emulator or physical device and build the app. Visit the capacitor homepage for detailed information and documentation. Here is the git repository for reference Arthur Shevtsov/Shutterstock.com You may be surprised to learn that Android is the most popular operating system on the planet—even bigger than Windows. That makes it a target for malicious attacks. But do you actually need antivirus apps on your Android phone? That's a fair question to ask. Antivirus software has been recommended for Windows users for many years. Thankfully, Microsoft has built-in better tools to combat malware—Windows has come with a built-in antivirus since Windows 8—but what about Android? Let's talk about some of the ways Android is protecting you. Google Play Protect Android's biggest built-in defense against malware is Google Play Protect. There are a few different components to Play Protect—including the Find My Device tools—but a big part of it is malware scanning. Every Android device that included the Google Play Store has Play Protect. You may have noticed the "No Harmful Apps Found" message at the top of the apps you download from the Play Store. Play Protect doesn't just work in the Play Store, though. It keeps an eye on everything outside of the store as well. Even apps that have been sideloaded from outside the Play Store are scanned by Play Protect. Sideloaded is still inherently riskier, but it's nice to know Play Protect is watching. In addition to scanning apps, Play Protect can protect you when browsing with Google Chrome too. Just like on Chrome for desktop, if you visit a site with malicious code, Chrome will warn you and take you back to safety. RELATED: What is Google Play Protect and How Does it Keep Android Secure? Monthly Security Updates Another big thing that protects your Android device is monthly security updates. These are smaller updates that don't typically have shiny new features, but they're very important. New vulnerabilities and exploits are popping up all the time. If your Android phone was only updated once a year, these things would pile up and become dangerous. It's critically important to routinely squash these things as they come up. That's why monthly security updates are necessary. Sadly, not all Android devices receive these updates in a timely manner or at all. Google releases the security updates every month and it's up to its partners (Samsung, OnePlus, etc.) to approve the fixes, add any of their own, and release them to devices. If you want the most secure Android phone, your best bet is a Google Pixel or Samsung Galaxy device. Both Google (unsurprisingly) and Samsung are the most

