Android studio sqlite database update

I'm not robot

reCAPTCHA

Continue

I'm not robot

reCAPTCHA

S'Lite LogoRecently, I worked on the LinkedIn spy tool, I used the S'Lite database to store data, this tool should support the full text of the fonctionnality search for application. Googling on the Internet and I found that S'Lite already support a full text search in your native language. This is done through three evolutions of the complete ftS3/FTS4/FTS5 text search expansion. The original FTS3 code was included in the S'Lite project by Scott Hems of Google.FTS1, and THES2 are outdated full-bodied search modules for S'Lite. There are known problems with these old modules and should be avoided. Let's play with this extension, I choose this Moroccan beautiful Riad Riad Al Mamoun, the idea is to extract some reviews and search for them. Riad Al Mamuna - TripAdvisorTo manipulate the database S'Light, I use the sqlite3 command in ubuntu, but we have to update it as not supporting FTS5, so to update it run the following command lines on the terminal: sudo add-apt-repository ppa:jonathonf/backportssudo apt-get update sudo apt-get sq3 Then go into the workspace and create a S'Lite database file, taking out:sqlite3 hotels_reviews.dbNow, copy and paste every part of S'L on this essence and run it on the sqlite3 request, please read the comments to understand more:After you have correctly installed your database, we can now try to perform some search requests:SELECT rowid, review from hotels_reviews_index hotels_reviews_index You can also order by relevance, which is the rank score: SELECT rowid, rank, review from hotels_reviews_index WHERE hotels_reviews_index MATCH 'review:square and location' ORDER BY rank; Please check the official documentation for the syntax and operators supported by the FTS5 extension by following this link: can read more about this topic here:❤ If this post was helpful, please click a little green heart and follow me using the buttons below! Sign up to get a daily preparation of top tech history! Android: If you know or suspect that there is an update available for your Android device, but nothing appears when you check the system update in the device settings, here's an alternative method to get the check right now. Normally, you can go to the settings of the system update to check for available updates, but the problem is that operators often have step-by-step release cycles. Ghacks publishes an alternative method. Go to the settings of the apps (or apps) and choose to show everything. Then find the Google Services Framework and click Clean Data. Then click The Force Stop button. Note it may not work on the first try. Another alternative method we mentioned earlier is to type #checkin (using numbers on the letter dial). Cleaning up and forcing Google to shut down its service system is easier remember, but the registration code can be faster. You just read or heard that your phone is due to update, maybe just fixing bugs, or perhaps... Read moreTher method can help you get your bux fix or a larger version of the update faster. Note, however, that if no updates are available, it won't magically create one for your device. Making an Android device to find an update of Ghacks Most of us are still waiting for android 4.0 Ice Cream Sandwich on our phones, almost five months after the update was announced. Computerworld's blog summarizes which manufacturers follow through on their promises and which don't. Computerworld discussed this topic once when Andorid 2.2 Froyo came out, but things have changed a bit since then. Computerworld's current report card looks at tons of Android manufacturers and classes them when they promised their updates to Ice Cream Sandwich, and how well they followed through on those promises. Surprisingly, many tablet manufacturers like Acer, Archos, and Asus did a great job of updating quickly, while phone manufacturers like HTC, Samsung and Motorola are shrugging off promises or with the aim of upgrading in the second half of the year (with Motorola being the worst and HTC is the best, but still not a good enough winner). Hit the link for a complete rundown. Google's Android update make news, but if the manufacturer of your phone does nothing with... More Android 4.0 Report Maps: Which Manufacturers Fail? Computerworld You may have noticed that from time to time your Android smartphone encourages you to download and install a new version of its firmware. Maybe the first time this happened you thought you were getting an update to the latest version of Android, or maybe some neat new features were added. But in the end it turned out to be a boring Android security update! While Android security updates are really boring, they are very important. Let's take a look at these security patches, and Android security in general, to see what all the fuss is about! What are Android security updates? It is often said that making mistakes is a person, and although, as Alexander Pope says, forgive divinely, you will find that computers and hackers are not very forgiving! Whenever a software is written it inherently contains bugs, or bugs, as developers like to call them. Trying to reduce these errors is one of the key goals of software engineers. First, trying to catch bugs at a time when the software is written. Second, by correcting the bugs as soon as they have been found. There are two types of errors. First, the errors that make the software misbehave. Let's say you enter 001.300 and 02.7000 in calculator, and it gives you the answer of 2.51. Obviously something is wrong, maybe these extra zeros caused the software to behave Once the problem has been found the software can be fixed and the update sent out to users. These errors are usually a nuisance, and if serious enough can affect the sales/brand reputation, etc., but they are usually not dangerous (but more about it at the moment). The second category of errors is an error that affects the security of the software and the installed device. Thus, as a simple example, the app can request a username and password. The error can exist where if the user enters the correct name but leaves the password blank, the user is given access. It may sound silly, but it actually happened. Now there is an error that allows unauthorized access to private data. Most security bugs are much more complex and nuanced than this. But, in fact, an error in the program allows a third party to gain access that they should not have. Once these bugs are found, they need to be fixed quickly and deployed quickly to protect users. Sometimes first-category errors, unexpected behavior errors, can be manipulated in such a way that they become errors in the second category. Thus, the Android security update is a cumulative group of bug fixes that can be sent by air to Android devices to fix security bugs. Why are security patches important? Once you've installed a new security patch on your device, you'll see absolutely no difference in its functionality! It seems that nothing has been achieved. But this is, of course, the nature of fixing security errors. You don't notice them because they patch holes, often very small holes, in the safety of the device. For example, there may be a vulnerability where if you receive an SMS message in mixed Korean and Russian characters that is exactly 160 characters, then smart text creation in a message can cause an error that in turn can be used to open a hole in the protection of your device. I don't get many messages like that, so if the bug was found and fixed I would have no one the wiser. But here's the thing: when hackers learn about these esoteric bugs, they create special messages and send them to target people in order to gain access to their devices. Those who are targeted are vulnerable to the machinations of these cybercriminals. At the end you see a strange SMS message, frown a little and delete it. But you don't know that your phone has been compromised. Once you've installed a new security patch on your device, you'll see absolutely no difference in its functionality! So security patches are important because they protect your phone all hackers who want to gain access to your device. Just imagine all the data that is on your phone. Forget whatApps photos and messages. What

about banking? Amazon shopping? Ebay? Google Pay? There is a long list of things that will be of interest to the hacker. Which Which Get security updates? Theoretically, all Android smartphones should get about two years of security updates. However, the reality is often very different. How it should work this way: Google fixes an Android security bug. Google places these changes on AOSP and/or notifies its partners (each OEM that has a certified Android device from Google). Google actually does this on a monthly basis. Smartphone manufacturers then incorporate these fixes into their firmware and, if necessary, give a copy to the carriers. Carriers then approve the fixes and finally the release is sent to the devices by air. This works very well on Google phones like the Pixel range. It also works well on Android One devices, which are mostly supported by Google. It also works well for big brands. For example, the Samsung Galaxy Note 8 was launched in August 2017. I have one and can confirm that it has received regular (almost monthly updates). In fact, it has also been updated to Android 9.0 Pie.But for some medium-sized brands, updates can be more sporadic, whereas for smaller brands they often don't exist! Lack of security updates can be a real problem. It seems that some smartphone manufacturers have to sell it and forget its mentality. This means that there are millions of current (less than 2 years) Android phones in the hands of consumers who don't get any security updates, causing them to potentially be exposed to all sorts of attacks. On the other hand, Google knows it's a problem and wants to fix it! Android Security is a best practiceregardless on how often the device gets security patches, it's worth noting the following best Android security practices: Don't click on links in email, WhatsApp, Facebook Messenger, or SMS unless you're sure of the source of the link and where it will get you. Make sure you keep your apps up to date, including Chrome and other Google apps. Use unique passwords: Don't use the same password in multiple accounts. It's like using the same key to multiple homes: it increases the risk to your security. If this sounds like too much hassle, then use a password manager. Protect your accounts with 2-step Verification: Even if your username and password are stolen with a 2-step check with the help of intruder protection. Check Google's security: It's easy to do (g.co/securitycheckup) and analyzes the security status of your Google account. What about zero-day vulnerabilities and zero-day exploits? There is one aspect of Android security that is not covered by monthly security updates. A zero-day vulnerability. mistakes that Google doesn't know about, but someone does. They have security bugs that Google has zero days to try to fix. What's going on here, so-called security research companies, or cyber criminals, try to find bugs in Android and then once found found Don't tell anyone. They become a secret arsenal that can be used for nefarious means. Since this arsenal is secret and difficult to acquire, these zero-day vulnerabilities are highly valued. They get used to one of two ways. They are either sold to organizations with a lot of money as a national state security force, or they are used directly by cybercriminals in a massive attack to try to trick people into money. In any case, they can be deadly, literally, as we saw recently with the death of Jamal Khashoggi. Once these zero-day vulnerabilities start to be used publicly (in the wild), it is often not long before google is able to isolate the problem and issue a patch. Again, emphasizing the need to keep your phone up to date with monthly security patches. Wrap-upSecurity, as backups, can be boring. The problem with backups is that most people don't think about them until they've lost all their data. Similarly, most people don't think about security until their email account has been hacked, or fraudulent accusations have been made through their online banking. There will always be an element of risk, but Android security updates provide a way to reduce this risk as well as improve the stability and reliability of your device. Bottom line, whenever your phone says it has an update, install it. This is.