Application Security Lab3 Report

In this lab session, I create a database named learningflask by Postgresql, meanwhile, I create three tables inside the database to record user actions which are Table users, Table logging, and Table pictures.

For Table users, the information that I want to store are when users sign up for this app, their first names, last names, emails, and passwords could be safely stored here（Figure 1）. For passwords, unlike first names, last names, and emails, it is not a good idea to simply store passwords as is in plain text in the database. The reason for this is that if someone breaks into my database, they would be able to see all my users' passwords. Therefore, I defend against by encrypting passwords first and then store that encrypted password into the database.

Figure 1. Table users

图片包含 人员, 屏幕截图



自动生成的说明

In Table logging, I will record all successful and failed login attempts. Users can type in any email address for username or any numbers/letters for password. No matter the information they provide is correct or not, it will be accurately documented in Table logging as shown in Figure 2. Similarly to Table users, passwords are also encrypted before they being stored inside the database.

Figure 2. Table logging

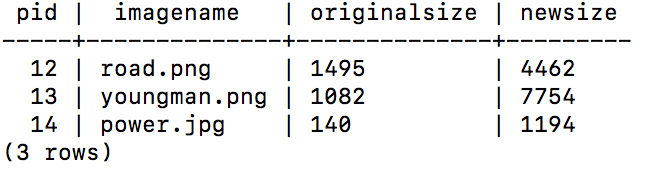
图片包含 文字, 报纸, 屏幕截图



自动生成的说明

After users successfully signing up or logging in the app, they will be redirected to the home page, this allows them to upload images and resize those images. In order to trace this kind of information, I create Table pictures storing uploaded image names, their original sizes as well as the new sizes of them in KB after being resized.

Figure 3. Table pictures



In conclusion, by adding Table users, Table logging, and Table pictures to my application database so that there is an audit trail of my user actions. This sort of data is useful when troubleshooting app performance and investigating suspicious behavior in the event of a breach.