Summer internship programme by upskill

Final Progress report

The secure password manager

Sairaj prakash rajput

B.tech

Upskill campus

In today's world, security is the main concern. If a user has created his multiple accounts then there should be a kind of application that will manage the passwords of that user.otherwise he loses his progress in the case it forgets his password.password manager application is to become an essential tool for storing the user password and managing user passwords, and retrieve them when needed. This report provides the purpose, working mechanism, benefits, and potential concerns.

The purpose of password secure manager:

1] Security: The password secure manager stores the password of the user. If the user has stored the password which is difficult to remember then he can retrieve it using this application. It increases the security of his user accounts.

2] Time saving: If someone is using this application then there will be no need to go for OPT verification or mail verification.verification is a useful method but it fails in some cases.that's why a secure password manager will remember the password to the user.

3] Strong password generation: this application also helps users to generate strong passwords and retrieve them when needed.

Working mechanism:

There will be UI which will contain 2 option:

1] Store password: The password will be stored by the user into the database.it will store the account name, password of that account and user ID.it will display the security of the password in the form of ratting while retrieving the password. All information will be stored in the database.

2] Generating password: There will be another option of generating the strong password.which will be below the ratings.

3] Retrieve password: It will first ask the user about the website on which the account has been created. then it will ask the account user name and then will show the password.

Benefits of secure password manager:

It provides several advantage including following:

1] There is no need for good memory: The main benefit of using a password manager to boost your cyber security is that you don't need to have a good memory. That means everyone can incorporate the latest recommendations for secure passwords, including using long phrases, symbols, punctuation, and capitalization.

2] You can secure your passwords: Without having to remember complicated passwords, your team will be able to not only use stronger

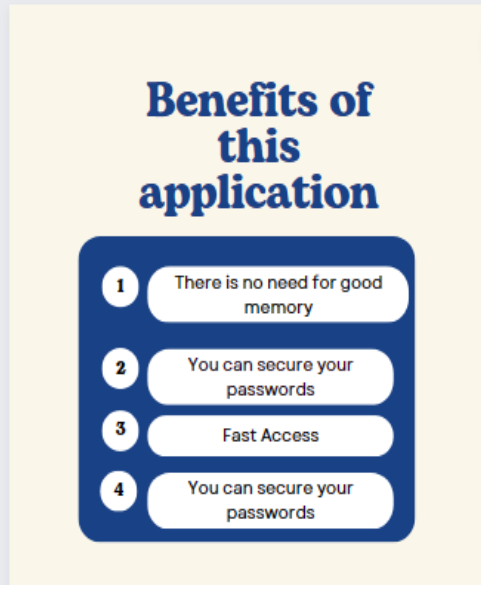
passwords, but also use a different password for every access point. That way, in the event of a breach, there will not be a cascading effect as each account becomes compromised. The result is a stronger password for each account and increased security across the board.

3] Fast Access

Password managers allow people to type a single password, and then have each access point automatically populated with a username and password. Your team will spend less time fumbling with login screens and password recovery and spend more time doing what matters.

4] More than one passwords:

Many password manager apps allow users to store and manage more than logins and passwords. For example, some provide secure access to credit card information. Others make multi factor authorization--or using a second test like answering a question once the correct password is entered--simple and effective. And, like complicated passwords, when multi factor authorization is simple to use, it's more likely for users to participate.



Potential concern:

1] All sensitive data in one place: You've probably heard about keeping your eggs in one basket. That's exactly what you'll be doing with a password manager. That basket will likely include credit card details and secure notes too. In case of a breach, blocking all payment options and changing passwords for all accounts might take enough time for the attacker to do damage.

2] Backup is not always possible: If the server breaks down, your only hope is that your provider has made a backup copy. This risk increases multi-fold if you decide to keep your vault offline on one of your devices. Naturally, keeping your own backup on an unprotected disk drive or poorly protected cloud service won't help either. Luckily, both NordPass and Keeper have your back – they keep backup copies for you in case of a server breakdown.

3] Forgetting your master password: Are you the only person who knew it, and your password manager doesn’t have a reset feature? In this case, you may already start recovering each login one-by-one. Alternatively, you may want to store your master password (or a hint) in some physically secure place, such as a safe.

4] Not all devices are secure enough. Hackers exploit the same vulnerability to get all of your logins in one attack. Password managers can be hacked if your device is infected with malware. In this case, typing the master password will get it recorded, and cybercriminals will gain full access to the data stored. That’s why password manager users

should invest in a trustworthy antivirus that will secure all of their devices first and reduce the risks.

Lessons learned:

Following things i have learned while tackling above challenges:

1] How to prepare for an internship level project?

2] problem solving:

3] Be consistent in work:

4] How to do operations with mysql database.

Overview: Thank you for your continued support and mentorship throughout my internship. I remain committed to delivering high-quality work and exceeding expectations.

Best regards,

Sairaj rajput, intern upskill