**PASSWORD MANAGER**

**INTRODUCTION**

First and foremost, password managers are a good thing. All password managers add value to the security posture of secrets management. An active security researcher once wrote, “Password managers don’t have to be perfect; they just have to be better than not having one”. Aside from being an administrative tool to allow users to categorize and better manage their credentials, password managers guide users to avoid bad password practices such as using weak passwords, common passwords, generic passwords, and password reuse. The tradeoff is that users’ credentials are then centrally stored and managed, typically protected by a single master password to unlock a password manager data store.

**ABSTRACT**

Password managers allow the storage and retrieval of sensitive information from an encrypted database. Users rely on them to provide better security guarantees against trivial exfiltration than alternative ways of storing passwords, such as an unsecured flat text file. We anticipated that password managers would employ basic security best practices, such as scrubbing secrets from memory when they are not in use and sanitization of memory once a password manager was logged out and placed into a locked state.

**PLATFORM/TOOLS**

Programming Language - JAVA

Database Connectivity - MYSQL

IDE - INTELLIJ IDEA, MYSQL 8.0

Operating System - WINDOWS 10

**CONCLUSION**

Remembering thousands of passwords is not possible for human beings. When it comes to a digital device, this task will be easy. Password Manager is that kind of software/application which memorizes our passwords with strong security features.