Team Name: HashPass Password Manager
Team Number: 4
Team Members: Samarth Girish, Shivam Sharma, Xavier Callait

Product Overview:
Over the course of the project this team accomplished all goals that were set forth. We developed a password generator and manager application which creates passwords with over 300 bits of entropy using custom salt calculation logic as well as the Argon2 hashing algorithm. The user creates a strong yet simple “passphrase” to use to unlock the password manager. Initially, we aimed for a minimum of 60 bits of entropy, but achieved better than expected results. Additionally, the extension automatically pops up whenever a login or a sign up field is detected to make the product easier to use. This results in the user not having to take extra steps to enable the extension. Another accomplished goal is that the limited information stored in the database is encrypted using AES and not stored in plaintext. This prevents attackers from gaining user information if the database is compromised. The application also has a feature which allows users to opt out of HashPass for select websites. This feature is in place for users who already have an account with a certain site and do not want to use HashPass for. Finally, this application never stores the generated passwords and is always calculated live. This prevents passwords from leaking in case the database is compromised. Even the user’s simple passphrase is not stored anywhere as it is used as the encryption and decryption key. AES encryption and decryption are run using that key on predetermined UUID values to authenticate a user.