

CS35L Project Proposal - Shrine

Team Members

- Alan Yu azy7@g.ucla.edu 505538781
- Chentyi Zhang chriszhang09@g.ucla.edu 805582503
- Randy Gu rgu855@163.com 305592076
- Jin Zhang jinzhang2001@g.ucla.edu 405503937
- Hanry Xu hanryxu@ucla.edu 005583257

Overall Idea:

The idea of the project for our team is to implement a password vault/manager. It will facilitate users to store and organize their passwords in a more convenient and accessible way.

Motivation:

Major password managers list TOTP passcode as a paid-feature (here we exclude Authenticator apps e.g. Google Authenticator from password managers), and none implement HOTP passcode as a feature. With this project, users may copy and fill one time passcode directly from their browser, without the trouble of going to their mobile app, read and remember the one-time passcode, and submit to the website.

Features:

- Upload data from Client to Back-end
Username and passwords provided by users will be saved in the server database.
- Display Dynamic Data to the User
Added username and passwords will be displayed on the website, available for viewing, copying, and editing.
- Meaningfully search through server-side data
Users may search for website name or username to retrieve certain passwords.
- Unique Feature #1
Aside from the basic website name, username, and password, store two factor authentication (TOTP and HOTP) keys and dynamically generate dynamic codes.
- Unique Feature #2
Provide a random password generator to create stronger and safer passwords.
- Unique Feature #3
Notify users of repeated and unsafe (breached) passwords.