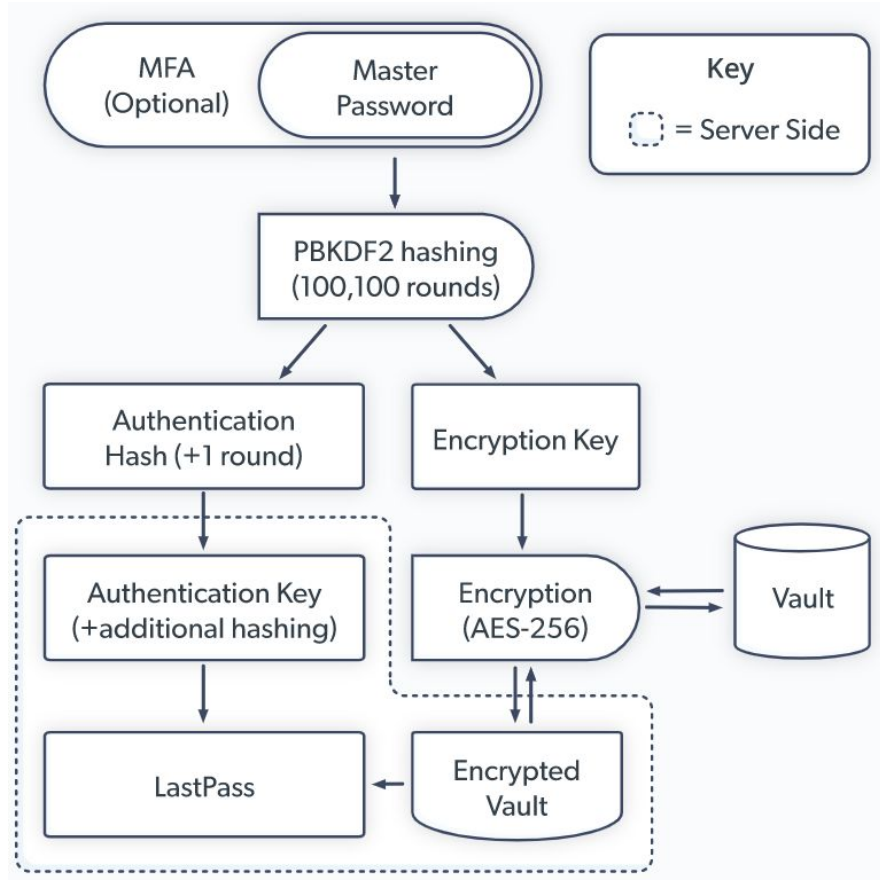# LastPass Clone Output

Manali Bagwe (1711003), Netra Ghaisas (1711016), Bhagyashree Phadnis (1711040)

Implementation Architecture

- Master password used to create the user account was hashed using PBKDF2-SHA256 algorithm (100100 rounds). This was used as the key for encryption / decryption of the password vault and for authentication after additional client-side (JavaScript) and server-side (PHP) hashing. Master password is not directly stored in the database.
- Encryption key so obtained was used to encrypt the vault, a Javascript object with entries having site name as key and password as value. AES-256 was used for encrypting and decrypting the vault on client-side using Javascript
- After login, the client makes AJAX calls to the server to get the encrypted vault and decrypt it using the key stored in session storage. The session storage gets cleared after the user logs out or closes the tab.
- Client-side JavaScript was used to randomly generate and test passwords. No data was sent over the Internet to the server

Execution Screenshots

Landing Page
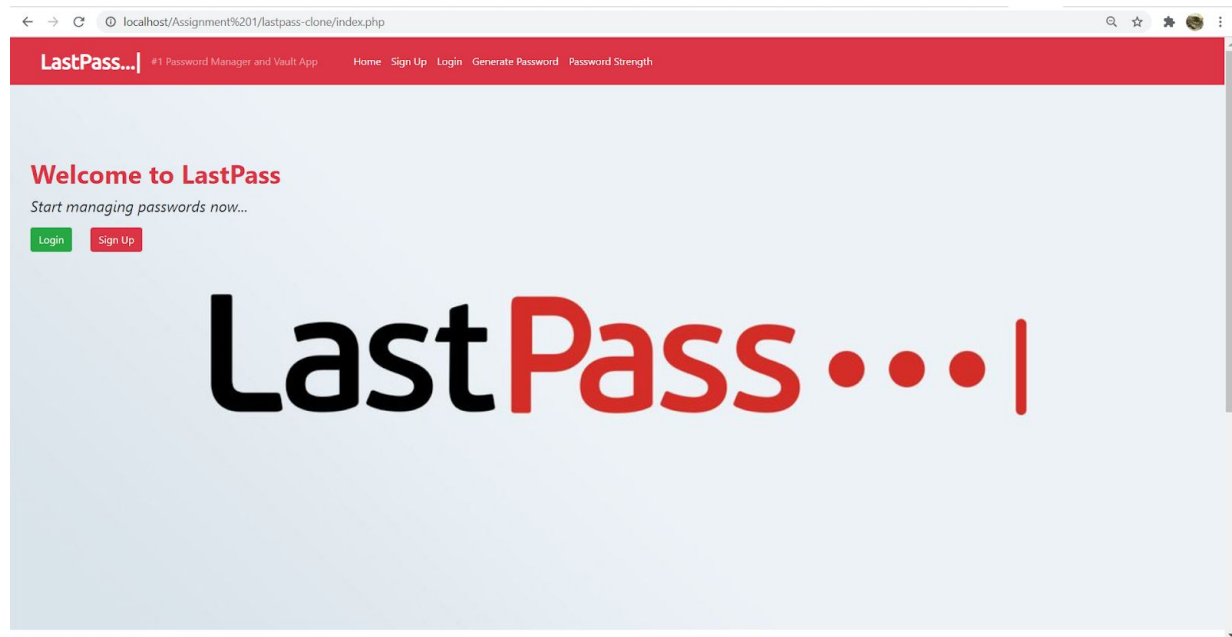
Sign up page
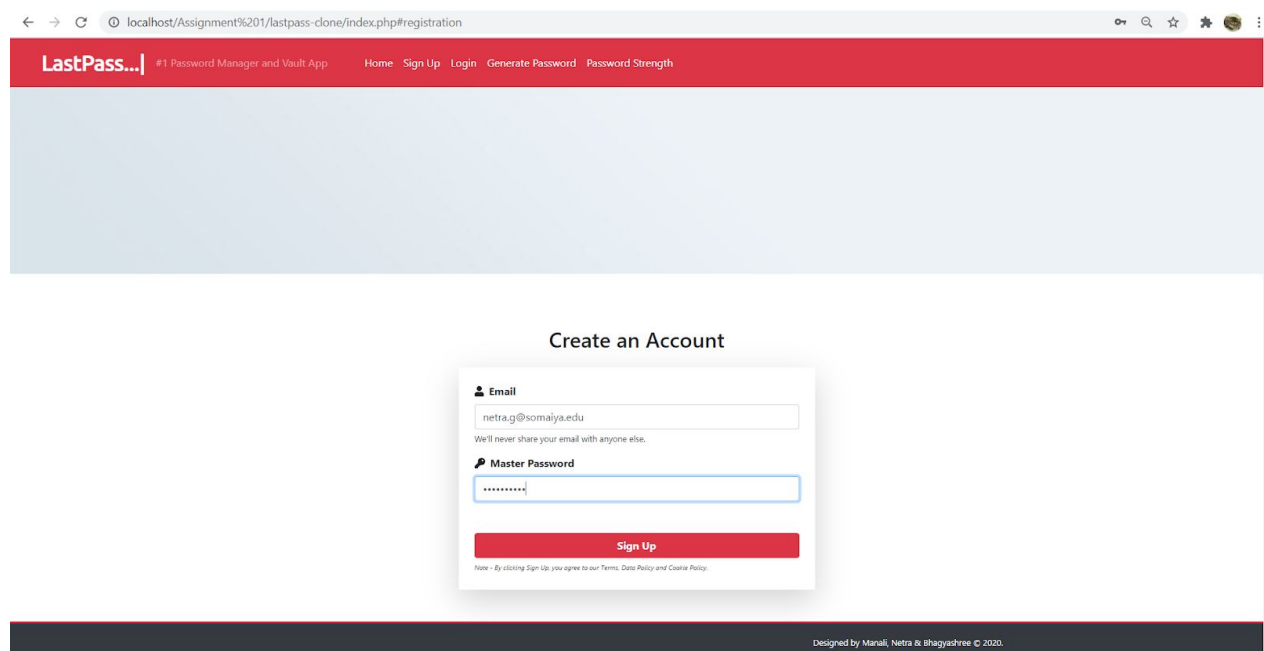
Login page

User profile page with password vault

Case 1: No password entries yet

Case 2: Passwords added to vault
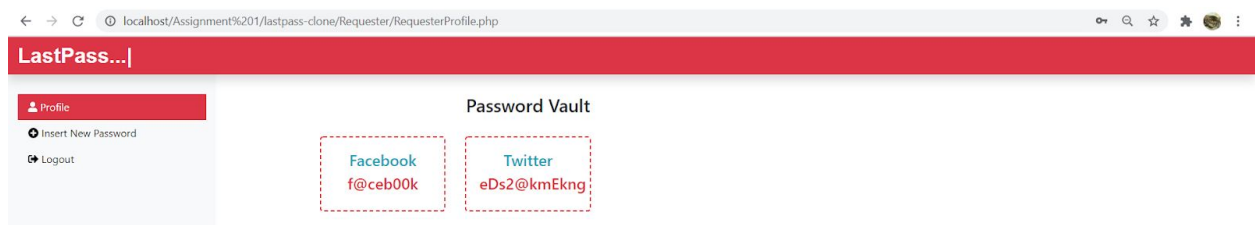
Adding a new entry to password vault

Features:

Show password toggle

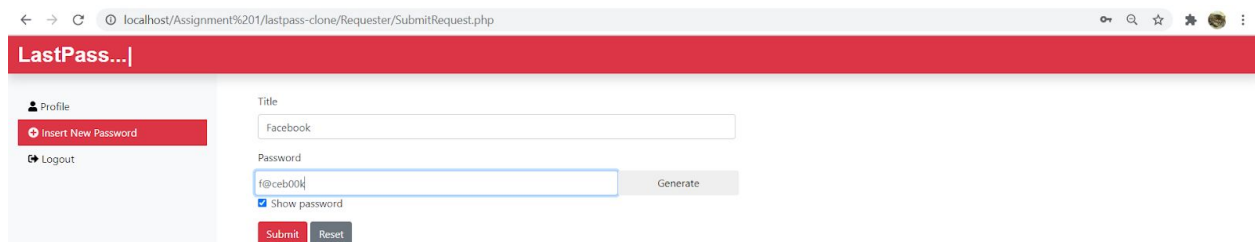# Randomly generate password during entry creation

Random Password Generator

← → C ⓘ localhost/Assignment%201/lastpass-clone/passgen.php   ⊕ ☆ ✦ 🌰 ⋮

LastPass...|

hGulchaw

Generate

Random Password Generator

A Strong Password
A strong password is key for protecting your personal info and assets online. Using a different password for every website that is long and has multiple types of characters (numbers, letters, and symbols) will help protect you from someone hacking into your accounts.

How it Works
Password generation is done client-side, on your computer, with Javascript. These passwords are never shared with us.

A Password Solution
Tired of remembering passwords? A password manager helps you store your passwords in one secure place, where they are encrypted and accessible only to you. A built-in password generator also helps you create strong passwords when you need them.

Password Length:
8

Password Formula:
○ All Characters
◉ Easy to Say
○ Easy to Read

☑ A-Z ☑ a-z ☐ 0-9 ☐ !$%@#

5 Minimum Numeric Characters

← → C ⓘ localhost/Assignment%201/lastpass-clone/passgen.php   ⊕ ☆ ✦ 🌰 ⋮

LastPass...|

cA43yB224@

Generate

Random Password Generator

A Strong Password
A strong password is key for protecting your personal info and assets online. Using a different password for every website that is long and has multiple types of characters (numbers, letters, and symbols) will help protect you from someone hacking into your accounts.

How it Works
Password generation is done client-side, on your computer, with Javascript. These passwords are never shared with us.

A Password Solution
Tired of remembering passwords? A password manager helps you store your passwords in one secure place, where they are encrypted and accessible only to you. A built-in password generator also helps you create strong passwords when you need them.

Password Length:
10

Password Formula:
○ All Characters
○ Easy to Say
◉ Easy to Read

☑ A-Z ☑ a-z ☑ 0-9 ☑ !$%@#

5 Minimum Numeric Characters

Password Strength Checker

How secure is your password?

Test Your Password		Minimum Requirements
Password:	••••••••	• Minimum 8 characters in length
Hide:	☑	• Contains 3/4 of the following items:
Score:	79%	- Uppercase Letters
Complexity:	Strong	- Lowercase Letters
		- Numbers
		- Symbols

Disclaimer

This application is designed to assess the strength of password strings. See if your password is strong enough to keep you safe. This tool runs locally. No data is sent data over the internet. This tool is for personal testing purposes only. Nothing you enter is sent or recorded anywhere.

LastPass...|

How secure is your password?

Test Your Password		Minimum Requirements
Password:	3nH3244!Clth	• Minimum 8 characters in length
Hide:	☐	• Contains 3/4 of the following items:
Score:	100%	- Uppercase Letters
Complexity:	Very Strong	- Lowercase Letters
		- Numbers
		- Symbols

Disclaimer

This application is designed to assess the strength of password strings. See if your password is strong enough to keep you safe. This tool runs locally. No data is sent data over the internet. This tool is for personal testing purposes only. Nothing you enter is sent or recorded anywhere.

Database snapshot

Database: lastpass
Table: users

r_login_id	r_email	r_password	enc_vault
7	netra@netra.com	$2y$10$5UC.CRbgsinqGrrA6PQPFuTHO8k.Q87dj0luvXenj3r...	[BLOB - 156 B]
9	qwerty@qwerty.com	$2y$10$49QHZ462.kjc65Tx2yZyCOt43gP33orrlyu/Vy8YvmX...	[BLOB - 292 B]
13	netra.g@somaiya.edu	$2y$10$IlqUdCyuiNghnq4tJndkKu5tsOVMhMcKvnE.GiZuXlf...	[BLOB - 316 B]

Encrypted vault blob file

users-enc_vault - Notepad

File Edit Format View Help

{"iv":"yqq7TJVXA4P1cTQ/7eFzhg==","v":"1","iter":10000,"ks":128,"ts":64,"mode":"ccm","a
data":"","cipher":"aes","salt":"auF8jFCZwxo=","ct":"O/laRh+91vSlyxp5c
+Jagl0NhhpS6FbsvPlFAGrm1xoGgnZJPrCNhxy0NRYV7dOaHcaGVprcUBLQcoTOtWzg1Pd/XAL6EuLAPzG5FkZ
De/VCr1O2xne/kOsLSgO00lDUzZMpn8Yw66LaR5vcmaK6wRzs5o3PvBQEvxyEaJWLtdFwwQ=="}

Additional implementation pictures and videos are present in the outputs/ folder in the GitHub code repository

Output Video Links:
- **Password Manager:**
  https://drive.google.com/file/d/1DywtGY5LnAqcI_UMECeJ27ib_QNN0sIY/view?usp=sharing
- **Password strength checker:**
  https://drive.google.com/file/d/1gHNyZsJ-adJyFjALqkKNGz9Hagley1ml/view?usp=sharing
- **Random password generator:**
  https://drive.google.com/file/d/1sfAERDNdiz4FVMcSzqJkhLHjvugV4B23/view?usp=sharing