CSE 312 Project

Ishaan Roychowdhury, Dannen Roberts, Manthan Vasavada

Passlib Report

For this project, when dealing with user account registration, authentication, and storage, we used passlib. This is a library that is specifically designed to generate a secure hash for your password to store in your database. There is also functionality to verify the password when it comes to authenticating the user. This library is very similar in function to the Bcrypt library we used in homework 8 for this class. The library has several common cryptographic algorithms implemented in the form of functions. These algorithms are specifically designed to generate a random hash for the text input you give it. Additionally, when the hash function in the library is called, the library generates a completely random and arbitrary string called a salt with varying degrees of entropy. Only the library knows this random string. This string is attached to the hashed input to make the hash even more secure. The Passlib's verify function keeps track of the random salt generated and the password hash and can verify if the password is correct. Since the library handles salt and hash generation, we did not have to worry about generating random strings to encrypt the passwords. It supports the common SHA-256 hash and all other modern hashes for our purposes of ensuring that the user passwords were completely secure. Since all of the algorithms are abstracted away into functions, we can easily use them without having to implement these algorithms ourselves. One interesting note thing to note is that the Passlib library seems to import the Bcrypt library so it even abstracts away a lot of the algorithms to the

Bcrypt library. The passlib library makes use of Bcrypt to abstract things like generating salts. This makes it even easier to generate a hash(and a salt) with fewer lines of code.

When it comes to licensing and copyright, Passlib comes under the 2 clause BSD License. The library is open source and that means anyone can use it freely. They are not liable for the consequences of any third party's usage of the library. You can use the code in any way you see fit.

Links to Documentation:

1. **Link to Github Repo**
    a. https://github.com/efficks/passlib/tree/master/passlib
2. **Link to Documentation**
    a. https://passlib.readthedocs.io/en/stable/index.html
3. **Link to the implementation of their MD-4 hash(Not all hashes are clearly implemented but this one is)**
    a. https://github.com/efficks/passlib/blob/master/passlib/crypto/_md4.py
4. **Link to a list of functions they use to generate the hash for passwords:**
    a. https://github.com/efficks/passlib/blob/master/passlib/pwd.py