

OAuth/Authlib Report

OAuth is an open standard protocol used to authenticate users by granting data to websites that other websites hold with the user's permission. Most commonly, this technology is used for single sign-on login by logging in to other websites using information such as Google Mail. For our project, we use OAuth to solve the login issues as OAuth helps abstract away security issues with login and passwords. In addition, OAuth makes it more accessible and convenient as a majority of users already have an email account as opposed to registering for an account on our website. Since we are using python framework as a backend, our choice of OAuth implementation is an open source library called Authlib.

Authlib first creates an authorization url using the client id and client key provided by the developer, this code can be seen at <https://github.com/lepture/authlib/blob/169c7dcfc47478c8d55553cc95fb0f5578162b77/authlib/oauth2/client.py#L123>. After creating the url link, we redirect the user to this link to go through the single-sign on flow, in our case we used Google OAuth. After the user finishes the sign-on flow, the url link redirects the user back to our own website where we begin the authentication process. The authorization process begins by authorizing the access token which will verify that the access token is verified and has been fetched. This code can be seen at https://github.com/lepture/authlib/blob/169c7dcfc47478c8d55553cc95fb0f5578162b77/authlib/integrations/flask_client/apps.py#L79. After verifying the token, we will take the same token and parse the token in order to get the authorized user information out of the token. This is done through the `parse_id_token` function as seen from https://github.com/lepture/authlib/blob/169c7dcfc47478c8d55553cc95fb0f5578162b77/authlib/integrations/base_client/sync_openid.py#L32. With this, we now have the authorized user information from Google and can now create an account that the user can login with to access the features within our website.

The license attached to our project is the BSD license as we are using our project as an open-source project. If our project was closed-source, there would be a different commercial license. The BSD license places minimal restrictions on the distribution of our software meaning we are free to publish the work we've done with the contribution of the Authlib library.