OAuth 2.0: Authorization Code Flow Demonstration

INTRODUCTION

As general web applications being server-side applications where the source code is not public mostly using the authorization code flow (OAuth 2.0 RFC 6749, section 4.1), which exchanges an authorization code for a token. As mentioned above the application must be server-side since during the exchange the application's App Secret will transfer to the user account or the requested party where it will store on that end for further use.
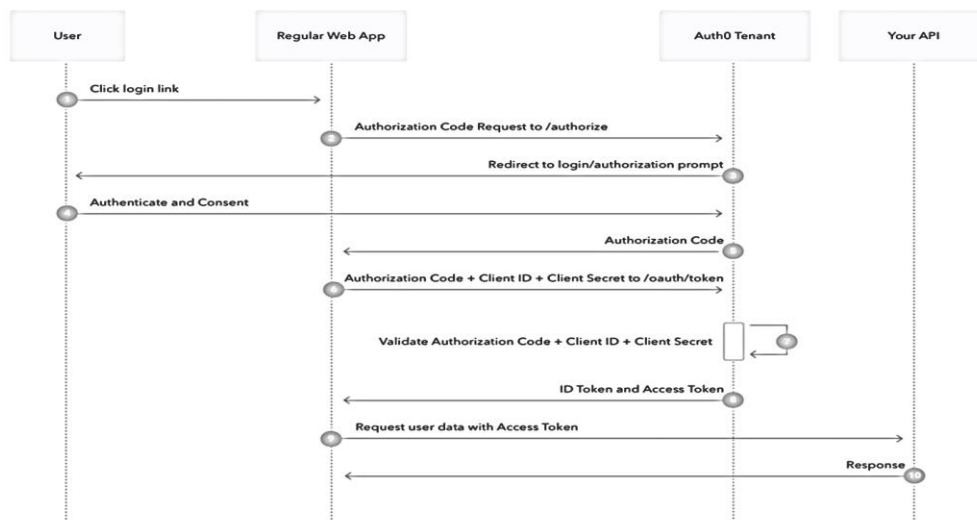
HOW IT WORKS

Fig 1. Authorization Code Flow [2]

1. User logs in to the application as usual [Fig. 2].

2. User is redirected to the authorization server (/authorize endpoint) by OAuth's software development kit.

3. User needs to log in resulting in an authorization prompt where it is redirected by the authorization server.

4. User authentication is done by a configured login option and prompts a consent with permissions requested where the web application can use it future when needed.
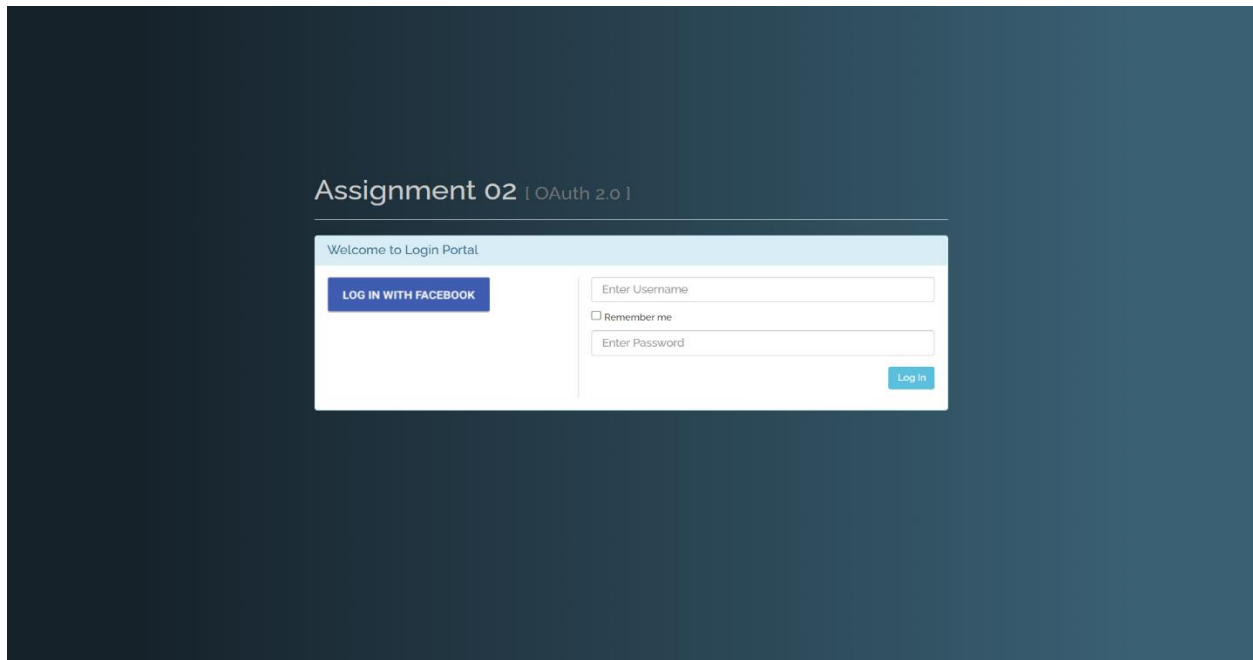
Fig 2. User Log in Page

5. Users are redirected back to the web application with an authorization code by the authorization server.

6. Authorization server (/oauth/token endpoint) catches this code when it is sent by the OAuth's software development along with the application's App ID and App Secret [Fig. 3].
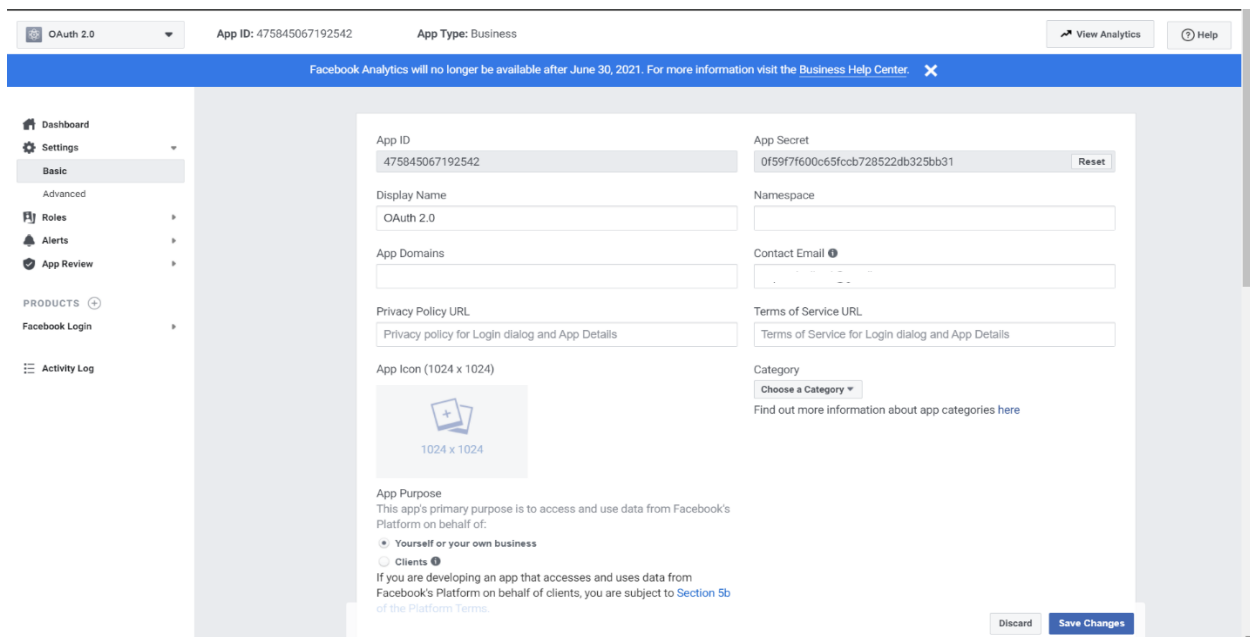

Fig 3. Application Properties

7. The code, App ID, and App Secret are verified by the authorization server.

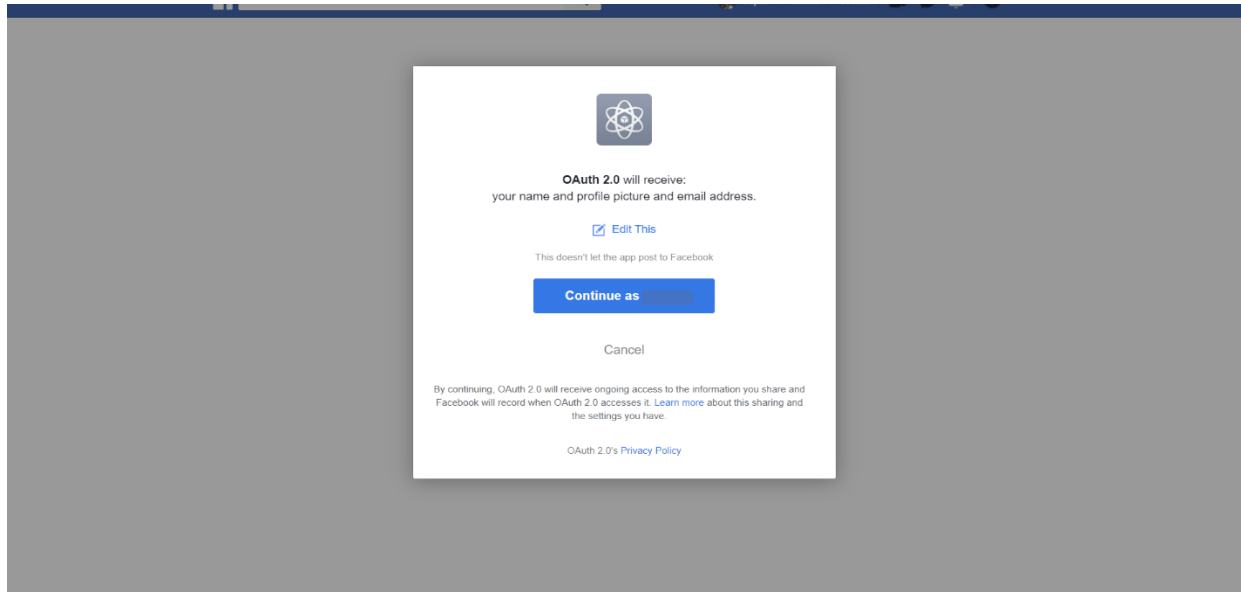8. A response with an ID and access token will be sent by the authorization server.

Fig 4. User Consent Prompt

9. Your application can use the Access Token to call an API to access information about the user.

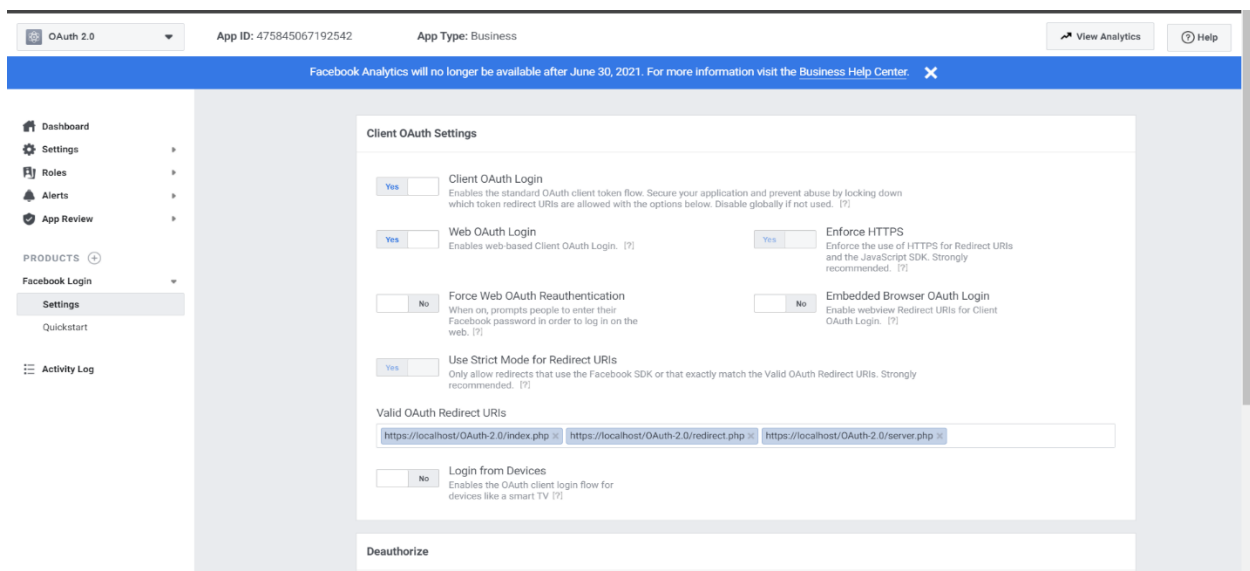10. A response from the application programming interface with requested data.

Fig 5. Application URI Properties

REFERENCES

[1] The OAuth 2.0 Authorization Framework. [Online]. Available: https://tools.ietf.org/html/rfc6749.

[2] Authorization Code Flow. [Online]. Available: https://auth0.com/docs/flows/authorization-code-flow

[3] Permissions Reference. [Online]. Available: https://developers.facebook.com/docs/permissions/reference/

[4] Permissions with Facebook Login. [Online]. Available: https://developers.facebook.com/docs/facebook-login/permissions/overview/

[5] Retrieving User Resources from Facebook over the OAuth 2.0 Authorization Code Grant Type. [Online]. Available: http://www.securityinternal.com/2017/04/retrieving-user-resources-from-facebook.html.