



IE5042 – SOFTWARE SECURIT
ASSIGNMENT 2

H.W.R.R. Samarawickrama MS22904782
P.M.I.N. Kumara MS22910172
MSc in Information Technology (Cyber Security)

Introduction

Objective of this assignment is to develop a web application that makes use of the OAuth Authorization and Resource Server services. OAuth 2.0 is an authorization framework rather than an authentication method. As a result, it's designed primarily to provide access to a set of resources, such as external APIs or data of users. OAuth employs Access Tokens, which are pieces of data that act as the authorization mechanism to access certain resources on behalf of a user. To demonstrate OAuth token function, PHP based web App with Facebook Graph API is employed. App will request authorization from user and once user grants it, the authorization code will be used to get OAuth token and this token will be used to call Facebook basic profile details, profile picture and friend list.

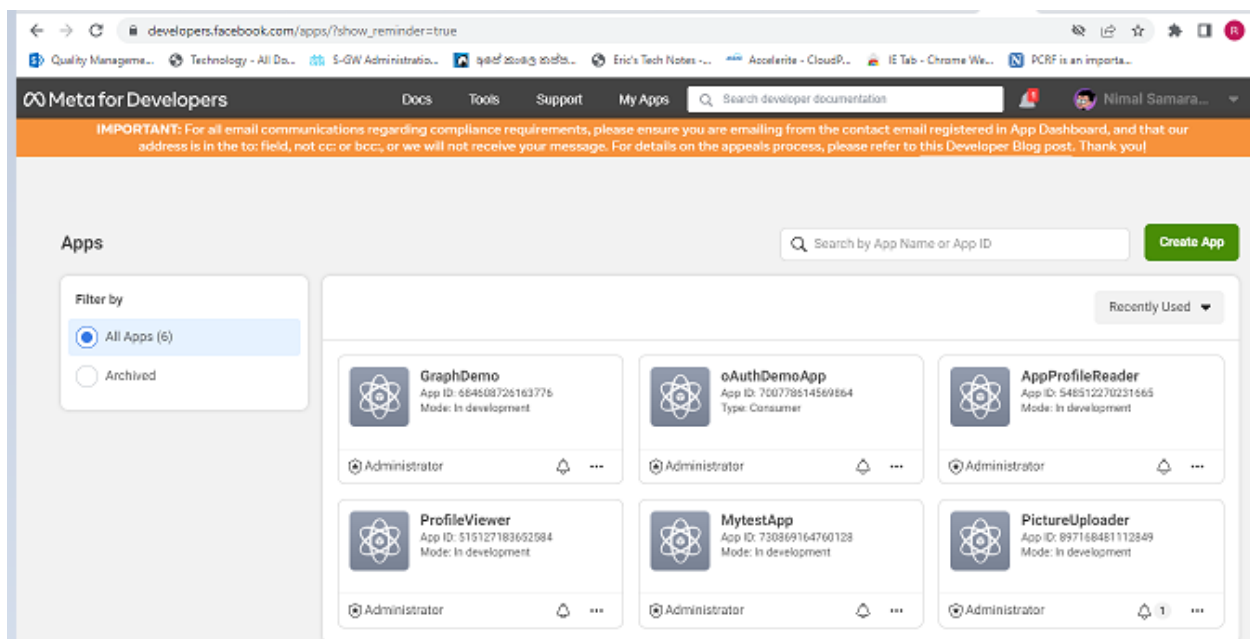
Registering Client (App)

If we need to use Facebook API, the App we are creating is the client and that needs to be registered in Facebook to acquire certain credentials. To do this we need to complete following steps,

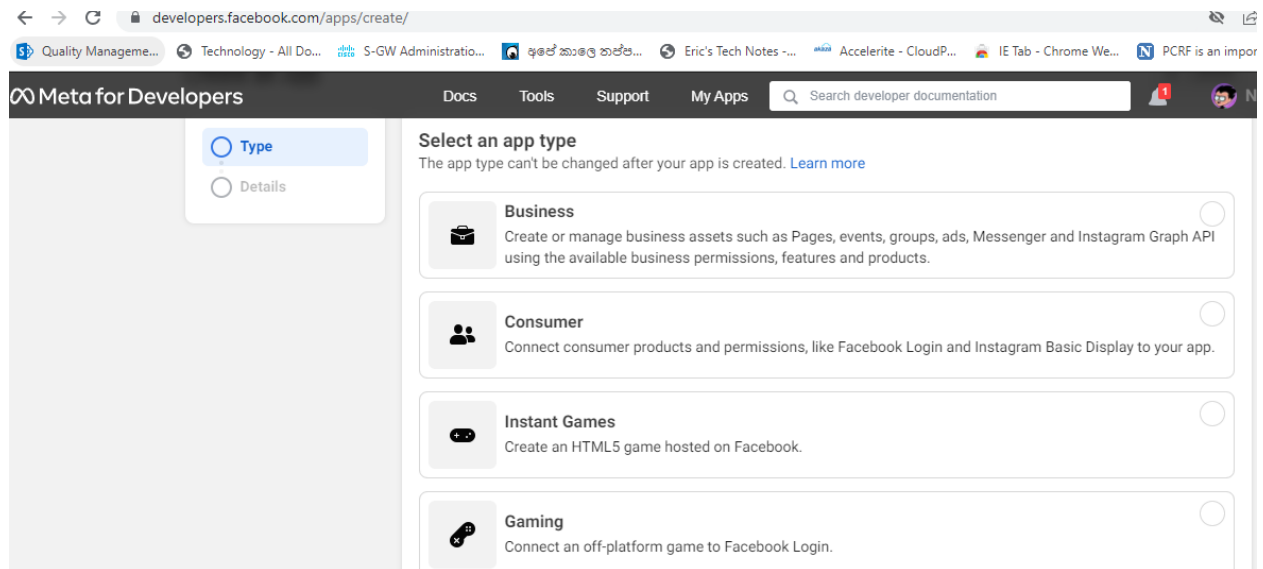
Client APP needs to be created by signing into Facebook Developer Account.

By using your facebook account credentials, you can log in to the developer.facebook.com.

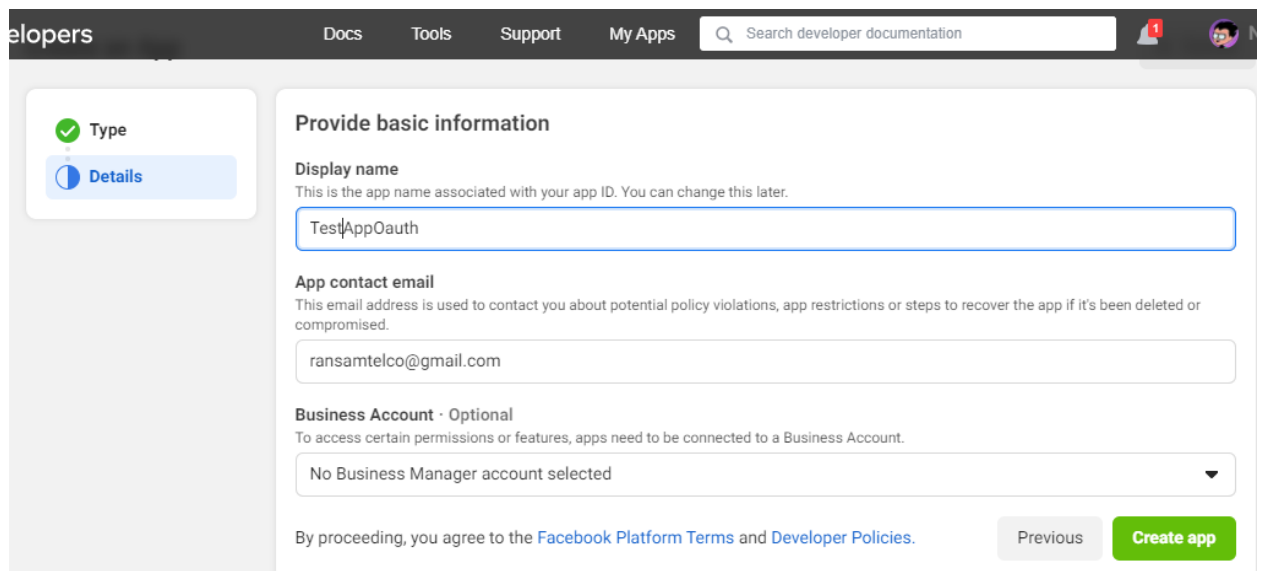
Then you need to click [Create App](#) button on the top right-hand corner.



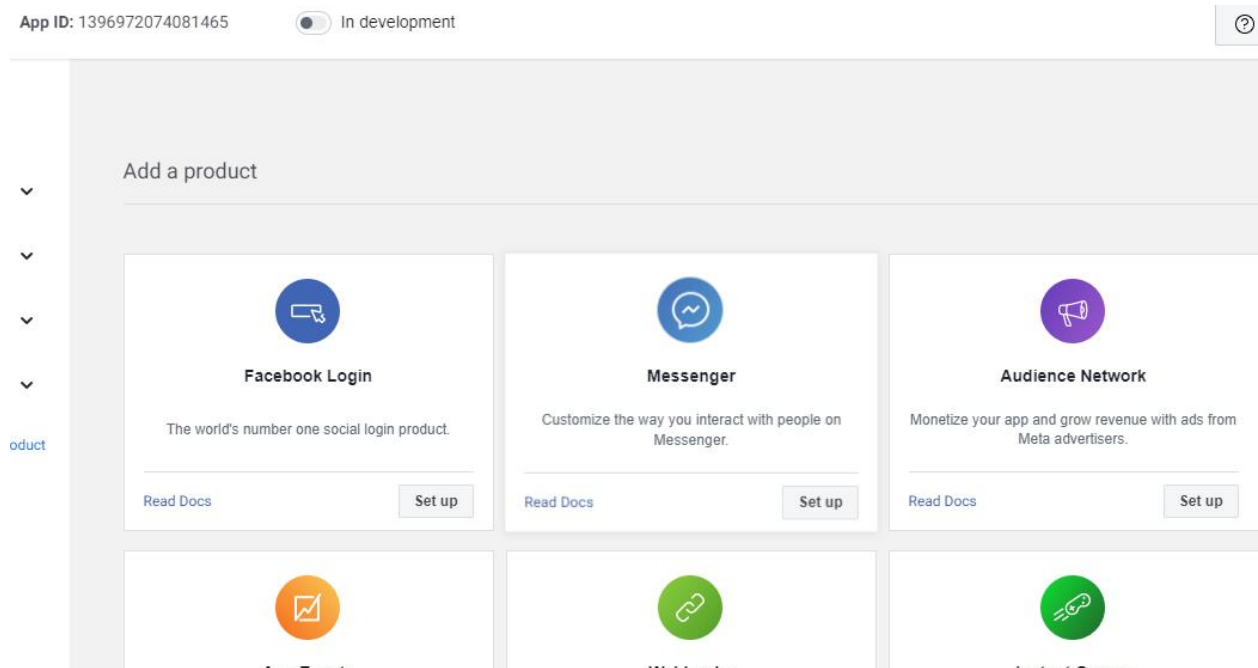
Then select any app type and click [Next](#).



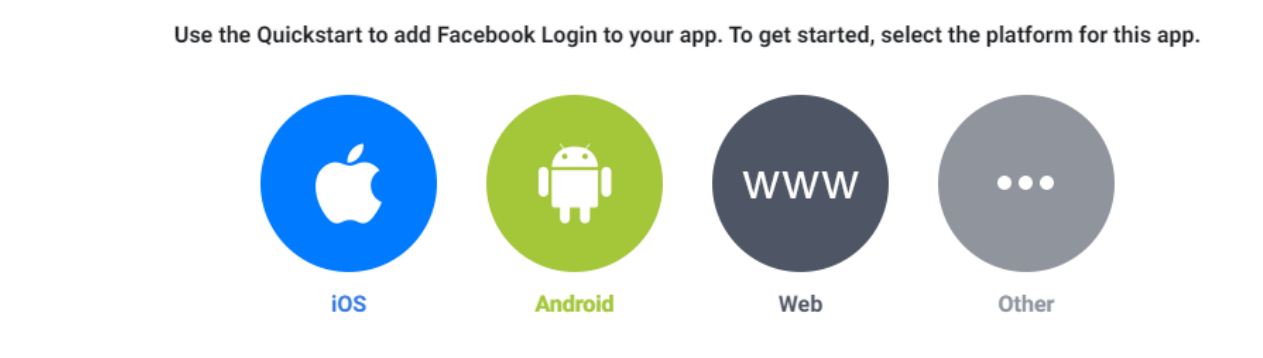
Then you need to enter **App Display** name. After that click **Create app**. Then you need to provide your facebook credentials to create the app.



Then App will be created with **App ID** appearing on the top left-hand corner. Then you need to **Add a product** to your App from the list of products. For this App, **Facebook Login** product is used. You need to click **Set up** button in Facebook **Login product**.

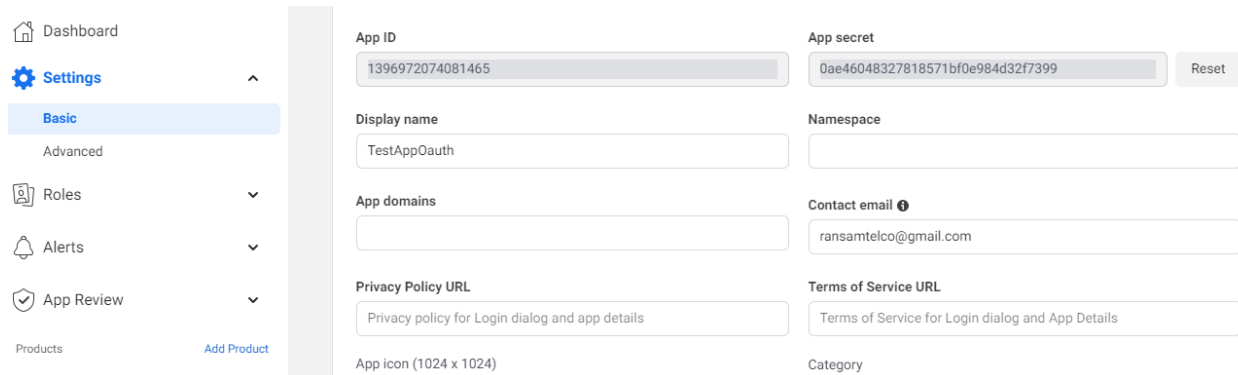


Then you need to add [platform for this app](#). Since this is the App used to demonstrate is a web App, [WWW](#) is selected.



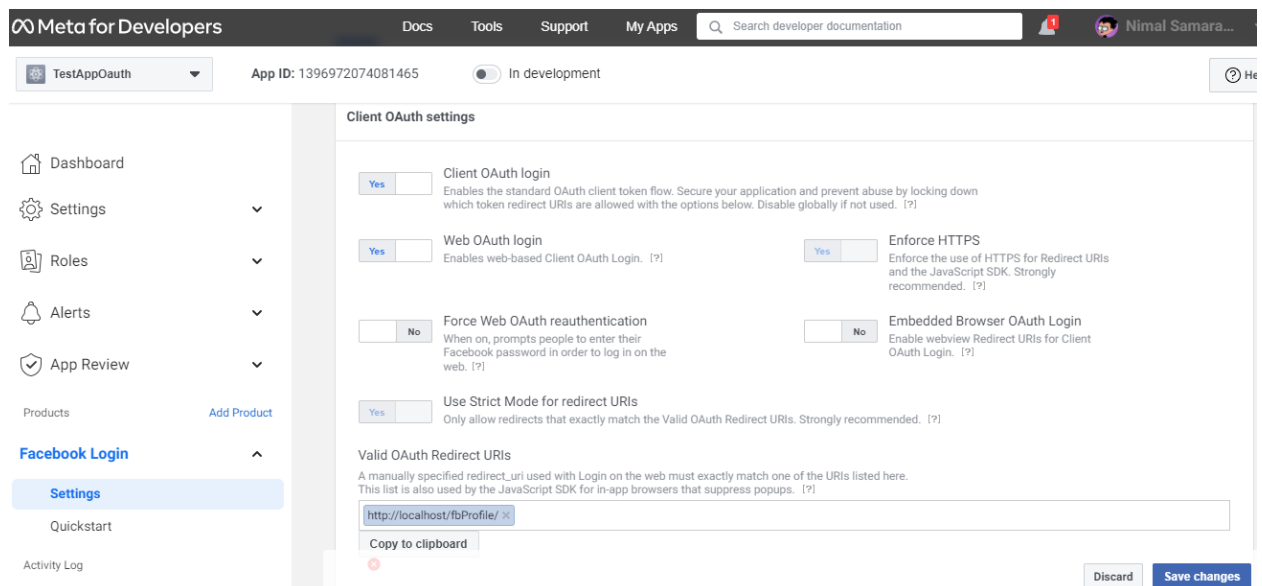
Then you need to give a [Site URL](#). Since this is only used for testing, [localhost](#) is used. Then need to [Save](#) and [Continue](#).

On the left pane, click **Basic** and you can find basic App parameters. For the Application we are going to implement, **App ID** and **App secret** are the most important parameters since they will be used in the App,



The screenshot shows the 'Basic' settings page for a Facebook application. The left sidebar contains navigation links: Dashboard, Settings (selected), Roles, Alerts, App Review, and Products. The main content area is divided into two columns. The left column contains fields for App ID (1396972074081465), Display name (TestAppOAuth), App domains, Privacy Policy URL (Privacy policy for Login dialog and app details), and App icon (1024 x 1024). The right column contains fields for App secret (0ae46048327818571bf0e984d32f7399), Namespace, Contact email (ransamtelco@gmail.com), Terms of Service URL (Terms of Service for Login dialog and App Details), and Category. A 'Reset' button is located next to the App secret field.

Then go to **Facebook Login** on the left pane and select **Settings**. Under **Valid OAuth Redirect URIs**, enter a redirect URI. Here we have used <https://localhost/fbProfile/>. [/rbProfile](#) is the folder in which all site files are contained. This is URI of our App and the redirected endpoint.



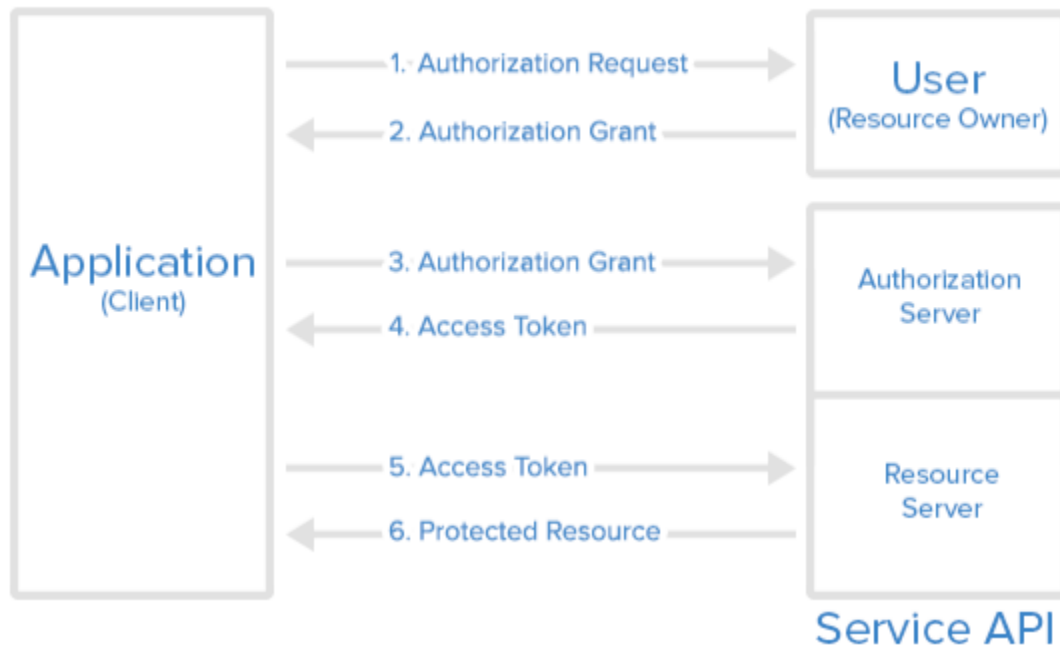
The screenshot shows the 'Facebook Login' settings page for the same Facebook application. The left sidebar is similar to the previous screenshot, but 'Facebook Login' is selected. The main content area is titled 'Client OAuth settings' and contains several toggle switches: 'Client OAuth login' (Yes), 'Web OAuth login' (Yes), 'Enforce HTTPS' (Yes), 'Force Web OAuth reauthentication' (No), 'Embedded Browser OAuth Login' (No), and 'Use Strict Mode for redirect URIs' (Yes). Below these toggles is the 'Valid OAuth Redirect URIs' section, which includes a text input field containing 'http://localhost/fbProfile/' and a 'Copy to clipboard' button. At the bottom right, there are 'Discard' and 'Save changes' buttons.

Once this is completed, the app creation and configuration is completed.

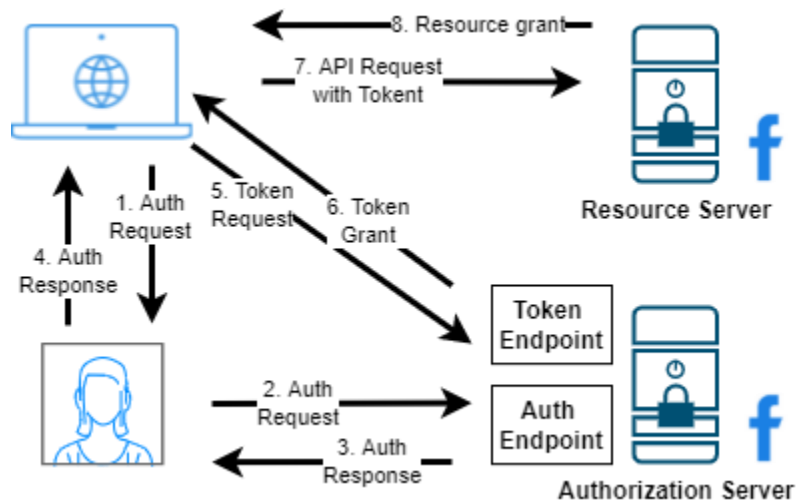
Message Flow

The basic message flow of the App is illustrated in in following Abstract Protocol Flow.

Abstract Protocol Flow



A high level message flow of the App is illustrated in following diagram,



The user will be asked to press a button if he needs to get Facebook basic profile details, Profile picture and Friend List.

Once he the click the button, he will be redirected to Facebook for login/grant authorization for the App to use profile details.

When the user grants his/her consent, Auth server will issue an Authorization code, and this code is employed by app to request OAuth token from Auth server.

Once OAuth token is granted to App, App will use it to call relevant Facebook APIs.

For the demonstration, following parameters will be used,

App ID: 684608726163776 (client_id)

App Secret: 803444823b90348911b468c1aac8a8ed (client_secret)

Encoded OAuth Redirected URI: <https%3A%2F%2Flocalhost%2FfbProfile> (Encoded <http://localhost/fbProfile> isong <https://www.urlencoder.org/>) – redirect_uri

Getting Authorization Code



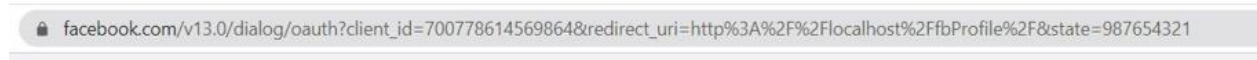
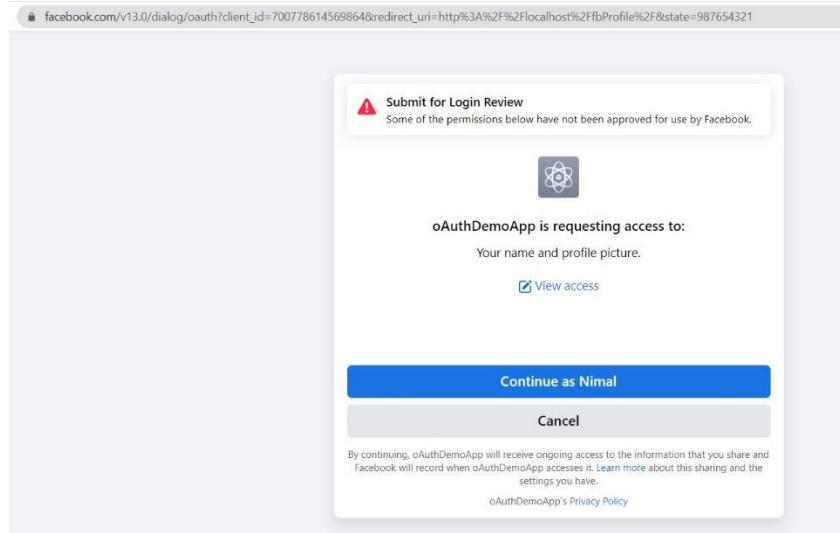
To call Authorization endpoint in the browser, following sample URI is used,

[https://www.facebook.com/v13.0/dialog/oauth?client_id=clientId&redirect_uri=URLENCODE\(redirectURI\)&state=](https://www.facebook.com/v13.0/dialog/oauth?client_id=clientId&redirect_uri=URLENCODE(redirectURI)&state=)

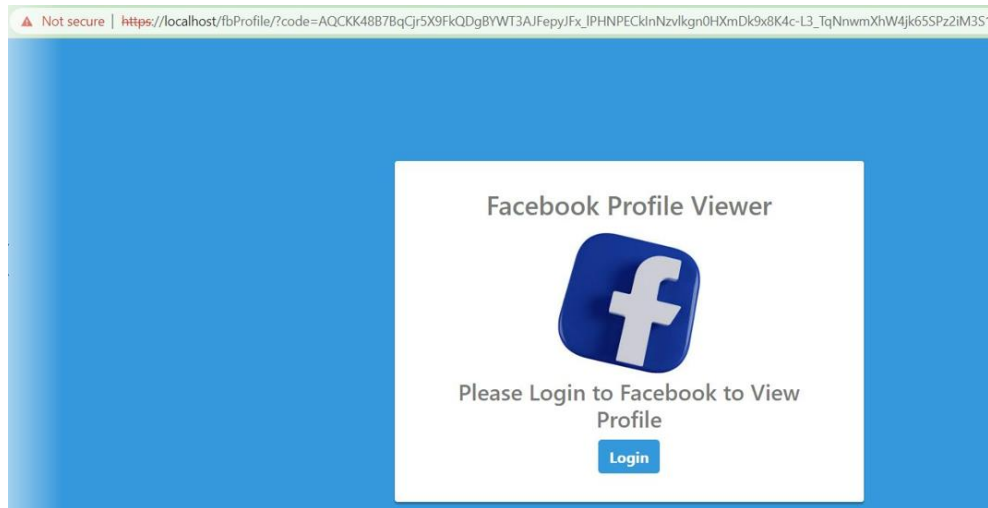
After substituting App values to URI gives following,

https://www.facebook.com/v13.0/dialog/oauth?client_id=684608726163776&redirect_uri=https%3A%2F%2Flocalhost%2FfbProfile&state=987654321

After executing this, we can get following screen. If the user logs into App, he needs to authenticate with Facebook. Since I am already login to Facebook, I don't need to login again. Instead, it will generate following to request for Sharing data from Facebook to our sample App which is OAuthDemoApp. By clicking "Continue as Nimal" I can give the consent to data sharing.



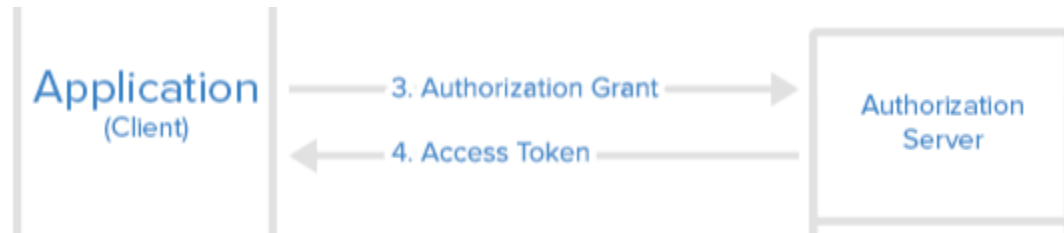
Now user will be redirected to Redirect URI we have already configured for this App with authorization code. From the URI we can get the code.



https://localhost/fbProfile/?code=AQCKK48B7BqCjr5X9FkQDgBYWT3AJFepyJFx_IPHNPECKInNzvlkgn0HXmDk9x8K4c-L3_TqNnwmXhW4jk65SPz2iM3S1QHxXMblprCHIsAI3YUX9pyb7N8cKTMLkxdoZq1KwXPOVE5VorbMs0SVQ71knPXhMeIN4lQmP8FTw8vBVqkTXdLW5sT1CRggHpBWoyapV9eaWnlwva2-ddzufQC8PMoqEp9ga-0LzJlKdy5Xq6TIwbZtrV5WceBnEF9BX8NCbcEhkxvP5FoTktETPFEiUG2qfyGocKX9n9jvxsHMX5Z9eIEsidTY9f2o6D7wbbbgDJ2UJTAeayKvLjWbaUfjRjvR7tzOtwctjacNjgOWpR8gN7qioHbx1fjT_nwhMp_J3EfawY5O6a88jDNjXMKf8OfQhlynKyHAizleOMFRUG&state=987654321# =


```
Code {AQCKK48B7BqCjr5X9FkQDgBYWT3AJFepyJFx_IPHNPECKInNzvlkgn0HXmDk9x8K4c-
L3_TqNnwmXhW4jk65SPz2iM3S1QHxXMBIprCHIsAI3YUX9pyb7N8cKTMIkxdoZq1KwXPOVE5VorbMs0SV
Q71knPXhMeIN4IQmP8FTw8vBVqkTXdLW5sT1CRggHpBWoyapV9eaWnlwva2-ddzufQC8PMoqEpf9ga-
0LzJIKdy5Xq6TIwbZtrV5WceBnEF9BX8NCbcEhkvP5FoTkETPFEiUG2qfyGocKX9n9jvxsHMX5Z9eIEsidTY9f2
o6D7wbbbgDJ2UJTAeayKvLjWbaUfjRjvR7ztOtwctjacNJgOWpR8gN7qioHbx1fjT_nwhMp_J3EfawY5O6a88j
DNjXMKf8OfQhlynKyHAizleOMFRUg}
```

Using Authorization code to get OAuth User Token



For Token Endpoint, following URI is used,

[https://graph.facebook.com/v13.0/oauth/access_token?redirect_uri=URLENCODE\(redirectURI\)&client_id=clientId&client_secret=clientSecret&code=code](https://graph.facebook.com/v13.0/oauth/access_token?redirect_uri=URLENCODE(redirectURI)&client_id=clientId&client_secret=clientSecret&code=code)

After substituting relevant parameters, we can get following

https://graph.facebook.com/v13.0/oauth/access_token?redirect_uri=https%3A%2F%2Flocalhost%2FfbProfile&client_id=684608726163776&client_secret=803444823b90348911b468c1aac8a8ed&code=AQB9lYqdF5foSZ_ubsv4OOJVCvgOI9KAdwMxsrwcePZVBKwsQE0fx-

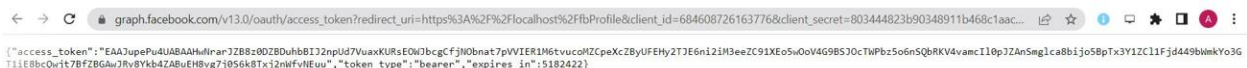
After running this in the browser, we can get following,

```
{ "access_token": "EAAJuPePu4UABABdqbhgqO9b4Dm23c7sCykHe1ZCiuJeh5Ye8qnRZBdTrhKJ7zMvLdkR203abNyVqJLBjdMA8ZAxHSi62HmIqZA5mZAQrxS5R338hTcI4CrIuvE9VB1GkAxEnxGsNKxtqDAF2DBSBPD7zvAfsWVK2gYwFdHS2r5k3DGQ1PLge2ojni6f7RN7gqVE7Osaw1qAjVLHPbBrrG69VZC6ZBAiZCLZCnpUeNwtNRt9ls6P7J9Omd", "token_type": "bearer", "expires_in": 5180051 }
```

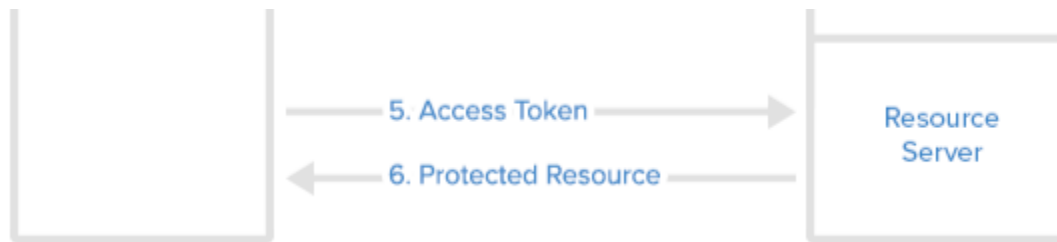
From this we can get OAuth Access Token,

Access Token,

```
{EAAJuPePu4UABABdqbhgqO9b4Dm23c7sCykHe1ZCiuJeh5Ye8qnRZBdTrhKJ7zMvLdkR203abNyVqJLBjdMA8ZAxHSi62HmIqZA5mZAQrxS5R338hTcI4CrIuvE9VB1GkAxEnxGsNKxtqDAF2DBSBPD7zvAfsWVK2gYwFdHS2r5k3DGQ1PLge2ojni6f7RN7gqVE7Osaw1qAjVLHPbBrrG69VZC6ZBAiZCLZCnpUeNwtNRt9ls6P7J9Omd}
```



Using Token to call APIs



Now we can use above token to call the APIs. We will use it to call Graph API from Facebook using “me”. For this curl is used with following sample format,

```
curl -H "Accept: application/json" -H "Authorization: Bearer access_token"  
"https://graph.facebook.com/me --ssl-no-revoke
```

After substituting the above access token we can get following,

```
C:\Users\asus> curl -H "Accept: application/json" -H "Authorization: Bearer  
EAAJupePu4UABAAHwNrarJZB8z0DZBDuhbBIJ2npUd7VuaxKURsEOWJbcgCfjNObnat7pVVIER1M6  
tvucoMZCpeXcZByUFEHy2TJE6ni2iM3eeZC91XEo5wOoV4G9BSJOcTWPbz5o6nSQbRKV4vamcI10p  
JZAnSmglca8bijo5BpTx3Y1ZC11Fjd449bWmkYo3GT1iE8bcQwjt7BfZBGAWJRv8Ykb4ZABuEH8vg  
7j0S6k8Txj2nWfvNEuu" "https://graph.facebook.com/me" --ssl-no-revoke
```

This will be run using Windows command prompt. The output is as follows,

```
{"name": "Nimal Samarawickrama", "id": "105821992126497"}
```

Similarly, we can run other API calls as well.

```
C:\Users\asus> curl -H "Accept: application/json" -H "Authorization: Bearer  
EAAJupePu4UABAAHwNrarJZB8z0DZBDuhbBIJ2npUd7VuaxKURsEOWJbcgCfjNObnat7pVVIER1M6  
tvucoMZCpeXcZByUFEHy2TJE6ni2iM3eeZC91XEo5wOoV4G9BSJOcTWPbz5o6nSQbRKV4vamcI10p  
JZAnSmglca8bijo5BpTx3Y1ZC11Fjd449bWmkYo3GT1iE8bcQwjt7BfZBGAWJRv8Ykb4ZABuEH8vg  
7j0S6k8Txj2nWfvNEuu"
```

```
"https://graph.facebook.com/me/picture?redirect=false&width=300&height=300" --ssl-no-revoke
```

```
{"data": {"height": 168, "is_silhouette": false, "url": "https://platform-  
lookaside.fbsbx.com/platform/profilepic/?asid=105821992126497&height=300&  
width=300&ext=1654320705&hash=AeSSXCwIhGcoHz5N-as", "width": 168}}
```

Facebook has restricted getting certain information from the public profile after 2018. Therefore, information like age and gender cannot be acquired from the profile.

```

C:\Users\asus>curl -H "Accept: application/json" -H "Authorization: Bearer EAAJupePu4UABAAHwNrarJZB8z0DZBDuhbBIJ2npUd7
VuaxKURsEOWJbcgCfjNObnat7pVVIER1M6tvucoMZCpeXcZByUFEHy2TJE6ni2iM3eeZC91XEo5w0oV4G9BSJOcTWpbz5o6nSQbRKV4vamcI10pJZAnSmg
lca8bijo5BpTx3Y1ZC11Fjd449bWmkYo3GT1iE8bcQwjt7BfZBGAWJRv8Ykb4ZABuEH8vg7j0S6k8Txj2nwfvNEuu" "https://graph.facebook.com
/me?fields=id,name,first_name,last_name,middle_name,email,name_format,cover,gender,birthday,timezone,picture,link" --s
sl-no-revoke
{"id":"105821992126497","name":"Nimal Samarawickrama","first_name":"Nimal","last_name":"Samarawickrama","name_format":
"{first} {last}","picture":{"data":{"height":50,"is_silhouette":false,"url":"https://platform-lookaside.fbsbx.com/p
latform/profilepic/?asid=105821992126497&height=50&width=50&ext=1654320618&hash=AeQMMJ4F1GPUJydL828","width":50}}}
C:\Users\asus>
C:\Users\asus>
C:\Users\asus>curl -H "Accept: application/json" -H "Authorization: Bearer EAAJupePu4UABAAHwNrarJZB8z0DZBDuhbBIJ2npUd7
VuaxKURsEOWJbcgCfjNObnat7pVVIER1M6tvucoMZCpeXcZByUFEHy2TJE6ni2iM3eeZC91XEo5w0oV4G9BSJOcTWpbz5o6nSQbRKV4vamcI10pJZAnSmg
lca8bijo5BpTx3Y1ZC11Fjd449bWmkYo3GT1iE8bcQwjt7BfZBGAWJRv8Ykb4ZABuEH8vg7j0S6k8Txj2nwfvNEuu" "https://graph.facebook.com
/me/picture?redirect=false&width=300&height=300" --ssl-no-revoke
{"data":{"height":168,"is_silhouette":false,"url":"https://platform-lookaside.fbsbx.com/platform/profilepic/?asid
=105821992126497&height=300&width=300&ext=1654320705&hash=AeSSXCwIhGcoH25N-as","width":168}}
C:\Users\asus>
C:\Users\asus>
C:\Users\asus>curl -H "Accept: application/json" -H "Authorization: Bearer EAAJupePu4UABAAHwNrarJZB8z0DZBDuhbBIJ2npUd7
VuaxKURsEOWJbcgCfjNObnat7pVVIER1M6tvucoMZCpeXcZByUFEHy2TJE6ni2iM3eeZC91XEo5w0oV4G9BSJOcTWpbz5o6nSQbRKV4vamcI10pJZAnSmg
lca8bijo5BpTx3Y1ZC11Fjd449bWmkYo3GT1iE8bcQwjt7BfZBGAWJRv8Ykb4ZABuEH8vg7j0S6k8Txj2nwfvNEuu" "https://graph.facebook.com
/me/friends?fields=name&limit=20" --ssl-no-revoke
{"data":[]}
C:\Users\asus>


```

After embedding information sent by facebook API to a HTML table in the actual App, we can get following,

Facebook – log in or sign up | php-graph-sdk/retrieve_user_profile | localhost/fbProfile/fbprofile.php | (3) Ruchira Ranga | Facebook

localhost/fbProfile/fbprofile.php#_=_

Your Facebook Profile



Facebook User ID	105274015514628
Facebook Profile Name	Ruchira Ranga
Facebook First Name	Ruchira
Facebook Last Name	Ranga
e-mail	ransamtelco@gmail.com
Name Format	{first} {last}

Appendix

appconf.php

```
<?php
    //This will be called by other pages when following App parameters are
required
    session_start();
    require 'Facebook/autoload.php';    // To use Facebook\Facebook namespaced
class methods
    $appId = '548512270231665'; // Replace value in '' with your app id
    $appSecret = '41fc77734d799260acc7951058f83209';    // Replace value in ''
with your app secret
    $defgraphVersion = 'v13.0'; // Replace value in '' with correct graph version
    $fb = new Facebook\Facebook([
        'app_id' => $appId,
        'app_secret' => $appSecret,
        'default_graph_version' => $defgraphVersion,
    ]);
?>
```

index.php

```
<!DOCTYPE html>
<html lang="en">
<head>
    <title>fb Profile Viewer</title>
    <link rel="stylesheet"
href="https://cdn.jsdelivrivr.net/npm/bootstrap@5.1.3/dist/css/bootstrap.min.css">
    <link rel="stylesheet" href="css/styles.css">
</head>
<body>
    <!-- This will provide user with an interface to start the App to get fb
profile details -->
    <div class="login-form">
        <div class="login-snippet">
            <h3 class="text-center">Facebook Profile Viewer</h3>
            
            <h4 class="text-center">Please Login to Facebook to View Profile</h4>
            <a href="fblogin.php"><button id="signin" class="btn btn-
primary">Login</button>
```

```
        </div>
    </div>
</body>
</html>
```

fblogin.php

```
<?php
    // Generates the login link
    require 'appconf.php';

    $helper = $fb->getRedirectLoginHelper();

    $optPermissions = ['email']; // Define Optional permissions
    $fbloginUrl = $helper->getLoginUrl('http://localhost/fbProfile/tokenget.php',
    $optPermissions);

    header("location:" . $fbloginUrl);
?>
```

tokenget.php

```
<?php
    require 'appconf.php';

    $fbuserId = '104491122259584'; // For validating Access Token

    $helper = $fb->getRedirectLoginHelper();

    try {
        $fbuseraccessToken = $helper->getAccessToken();
    } catch(Facebook\Exceptions\FacebookResponseException $e) {
        // Throw following errors if didn't get the Access Token
        echo 'Graph returned an error: ' . $e->getMessage(); // Output Message
        When Graph returns an error
        exit;
    } catch(Facebook\Exceptions\FacebookSDKException $e) {
        echo 'Facebook SDK returned an error: ' . $e->getMessage(); // Output
        Message When other local issues or if validation fails
        exit;
    }
}
```

```

if (! isset($fbuseraccessToken)) {
    if ($helper->getError()) {
        //If access Token is not set throw following errors
        header('HTTP/1.0 401 Unauthorized');
        echo "Error: " . $helper->getError() . "\n";
        echo "Error Code: " . $helper->getErrorCode() . "\n";
        echo "Reason for Error: " . $helper->getErrorReason() . "\n";
        echo "Description of the Error: " . $helper->getErrorDescription() .
"\n";
    } else {
        header('HTTP/1.0 400 Bad Request');
        echo 'Bad request';
    }
    exit;
}

// To manage access tokens, the client handler OAuth 2.0 is used
$oAuth2Client = $fb->getOAuth2Client();

// From /debug_token, acquire the access token metadata
$tokenMetadata = $oAuth2Client->debugToken($fbuseraccessToken);
echo '<h1>Metadata</h1>';
var_dump($tokenMetadata);

// Validation (If fail, these will throw FacebookSDKException)
$tokenMetadata->validateAppId($appId);
// If the user ID, to which this access token belongs is known, it can be
validated here
//$tokenMetadata->validateUserId('{your user id}');
$tokenMetadata->validateExpiration($fbuserId);

// After Logged in Generate token and set it into the session
// Redirect token to fbprofile.php
$_SESSION['fb_acc_token'] = $fbuseraccessToken->getValue();
header("location: fbprofile.php")

?>

```

fbprofile.php

```
<?php

require 'appconf.php';

try {
    // Set fields and that need to be retrieved from public profile
    // Set Access token already acquired to pass to facebook to get the profile
    details
    $fbprofRequest = $fb-
>get('/me?fields=id,name,first_name,last_name,middle_name,email,name_format,cover
,gender,birthday,timezone,picture,link', $_SESSION['fb_acc_token']);
    $fbprofImage = $fb->get('/me/picture?redirect=false&width=300&height=300',
$_SESSION['fb_acc_token']);    // To get Profile Picture
    $requestFriends = $fb->get('/me/friends?fields=name&limit=20',
$_SESSION['fb_acc_token']);    // To get friend list (currently not supported
with user access token)
} catch(Facebook\Exceptions\FacebookResponseException $e) {
    echo 'An error was returned by Graph API: ' . $e->getMessage();
    exit;
} catch(Facebook\Exceptions\FacebookSDKException $e) {
    echo 'An error was returned Facebook SDK: ' . $e->getMessage();
    exit;
}

$fbUser = $fbprofRequest->getGraphUser();

$profImage = $fbprofImage->getGraphUser();

//$fbFriends = $requestFriends->getGraphUser();

//echo "<pre>";
//print_r($fbUser);
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <title>fb Profile</title>
    <link rel="stylesheet" href="css/styles.css">
    <style>
        #fbProfile {
            font-family: Arial, Helvetica;
```

```

        border-collapse: collapse;
        width: 30%;
    }
    #fbProfile td, #fbProfile th {
        border: 2px solid #ddd;
        padding: 7px;
    }
    #fbProfile tr:nth-child(even){background-color: #FFE4C4;}
    #fbProfile tr:hover {background-color: #ddd;}
    #fbProfile tr {
        color: red;
        text-align: left;
        padding-top: 10px;
        padding-bottom: 10px;
    }
    img {
        border-radius: 45%;
    }
</style>
</head>

<body>
<!-- This will present User Profile information sent by Facebook API in a Table -
-->
<!-- Profile Picture is displayed as rounded image -->
<div class="container">
    <center></center>
    <br>
    <br>
    <center><table id="fbProfile">
        <tr>
            <td>Facebook User ID</td>
            <td><?=$fbUser['id']?></td>
        </tr>
        <tr>
            <td>Facebook Profile Name</td>
            <td><?=$fbUser['name']?></td>
        </tr>
        <tr>
            <td>Facebook First Name</td>
            <td><?=$fbUser['first_name']?></td>
        </tr>
        <tr>
            <td>Facebook Last Name</td>

```



```
        <td><?=$fbUser['last_name']?></td>
    </tr>
    <tr>
        <td>e-mail</td>
        <td><?=$fbUser['email']?></td>
    </tr>
    <tr>
        <td>Name Format</td>
        <td><?=$fbUser['name_format']?></td>
    </tr>
</table><center>
</div>
</body>
</html>
```