

IE5042

Software Security

Assignment 2

MSc. Cyber Security  
Ashini Devindi Thirimavithana  
**MS22905154**

## Table of Contents

|  |                                      |           |
|--|--------------------------------------|-----------|
| <b>1.0.</b>  | <b>Introduction .....</b>            | <b>3</b>  |
| <b>2.0.</b>  | <b>What is OAuth .....</b>           | <b>3</b>  |
| <b>3.0.</b>  | <b>Integrating OAuth.....</b>        | <b>3</b>  |
| <b>3.1.</b>  | <b>Use Case .....</b>                | <b>3</b>  |
| <b>3.2.</b>  | <b>Implementation on OAuth .....</b> | <b>4</b>  |
| <b>Step 1 – Create the Facebook Application .....</b>  | <b>4</b>                             |           |
| <b>Step 2 – Creating the Web Application .....</b>     | <b>7</b>                             |           |
| <b>Step 3 – Retrieving resources using OAuth .....</b> | <b>8</b>                             |           |
| <b>3.3.</b>  | <b>Methodology .....</b>             | <b>10</b> |
| <b>References.....</b>                                 |                                      | <b>11</b> |
| <b>Appendix.....</b>                                   |                                      | <b>12</b> |
| <b>1.</b>  | <b>Login Page.....</b>               | <b>12</b> |
| <b>2.</b>  | <b>Index Page.....</b>               | <b>14</b> |
| <b>3.</b>  | <b>Config code.....</b>              | <b>15</b> |
| <b>4.</b>  | <b>Callback Code.....</b>            | <b>16</b> |

## **1.0. Introduction**

This report is on using OAuth 2.0 Authorization Framework and creating a web application that use the services of OAuth.

## **2.0. What is OAuth**

The OAuth 2.0 or else known as a Open Authorization is an authorization framework. This enables an application to access HTTP services. [1]

In Simple terms OAuth notify the resource Provider (ex: Facebook) that the resource Owner (ex: user) has grant permission to a third-party application to access information. (ex: Allows the friends lists in Facebook). Using OAuth, request to authorization server is sent for obtaining the access token. And using this token, calls can be made to get the necessary data until it expires.

The advantage is it allows users to access data from another application. However, the user is given the control to choose the data that can be access. The main feature is it doesn't use credential but Authorization codes which are expiring. This provides a certain level of protections to the user data.

## **3.0. Integrating OAuth**

### **3.1. Use Case**

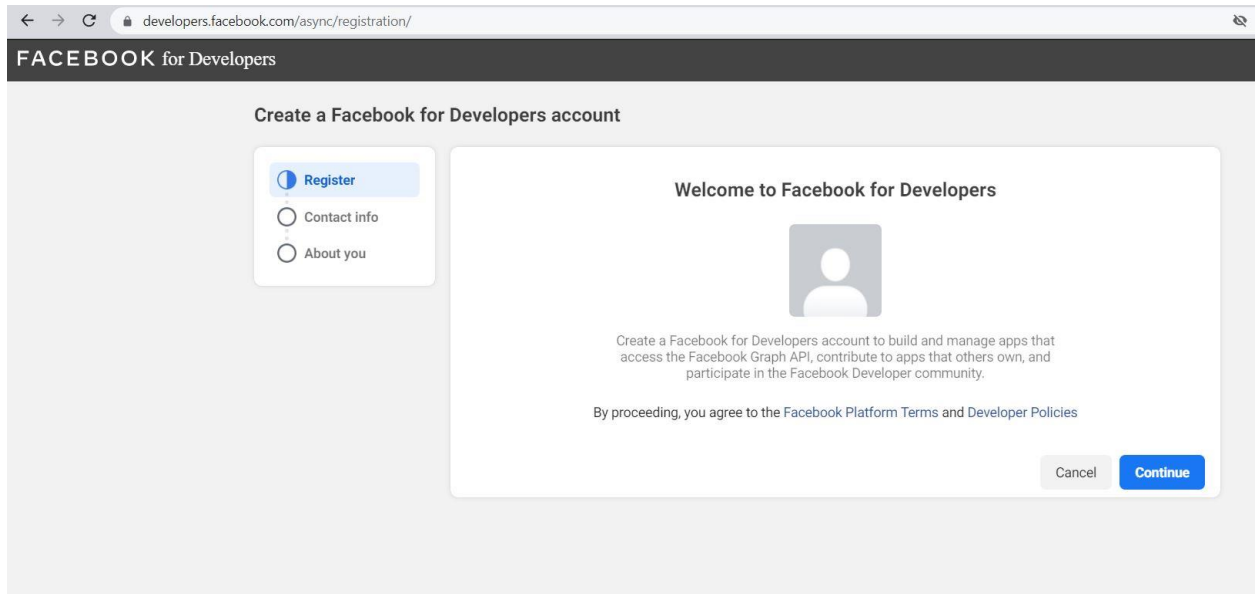
The use case selected is creating a web application to log in using Facebook. A Login with Facebook option is available when login to the web application along with the option to register. When the user clicks on the "login using Facebook" the user would get redirected to Facebook login page. After login, Facebook ask permission to share the necessary details. If the confirmation is given the application would obtain an Authorization code. And with this Authorization code an access token is requested from Facebook. Then the users profile information will be taken using the OAuth access token obtained and call the Facebook APIs.

- OAuth Authorization Server - Facebook
- OAuth grant type - Authorization Code
- OAuth Resource Server – Facebook

## 3.2. Implementation on OAuth

### Step 1 – Create the Facebook Application

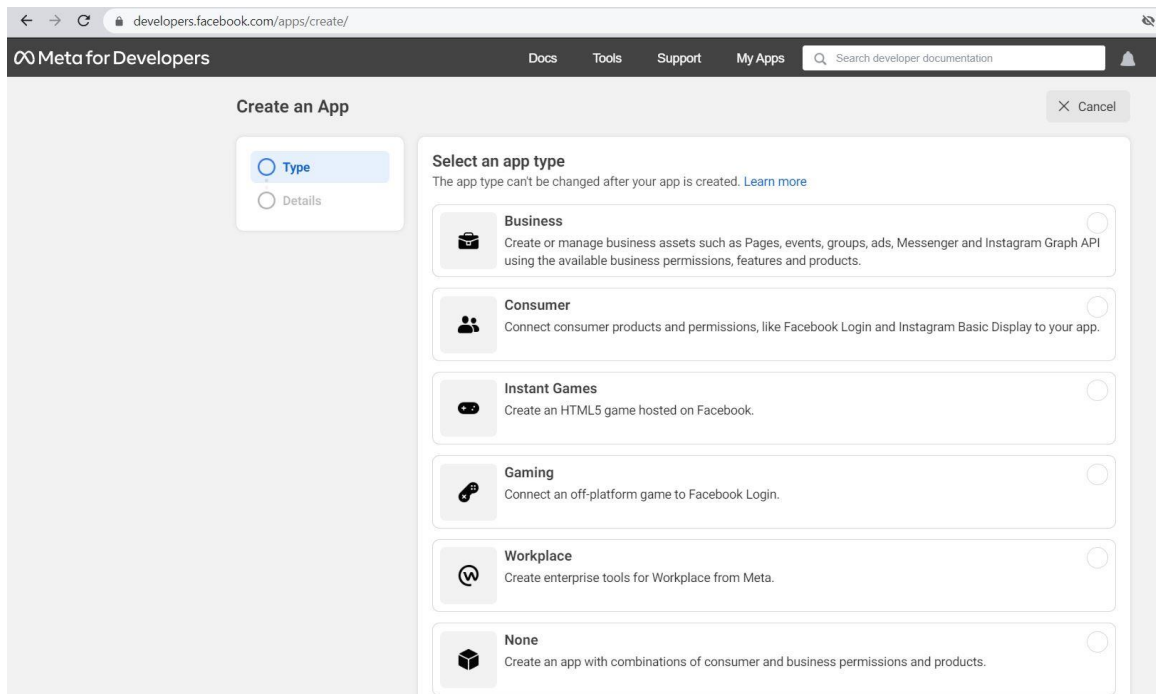
- 1.1. Visit <https://developers.facebook.com/> and create a developer account



The screenshot shows the 'Create a Facebook for Developers account' page. On the left, there is a sidebar with three steps: 'Register' (selected), 'Contact info', and 'About you'. The main content area has a heading 'Welcome to Facebook for Developers' above a placeholder profile picture. Below the picture, it says: 'Create a Facebook for Developers account to build and manage apps that access the Facebook Graph API, contribute to apps that others own, and participate in the Facebook Developer community.' At the bottom, it states: 'By proceeding, you agree to the Facebook Platform Terms and Developer Policies'. There are 'Cancel' and 'Continue' buttons at the bottom right.

- 1.2. Select Create a New App

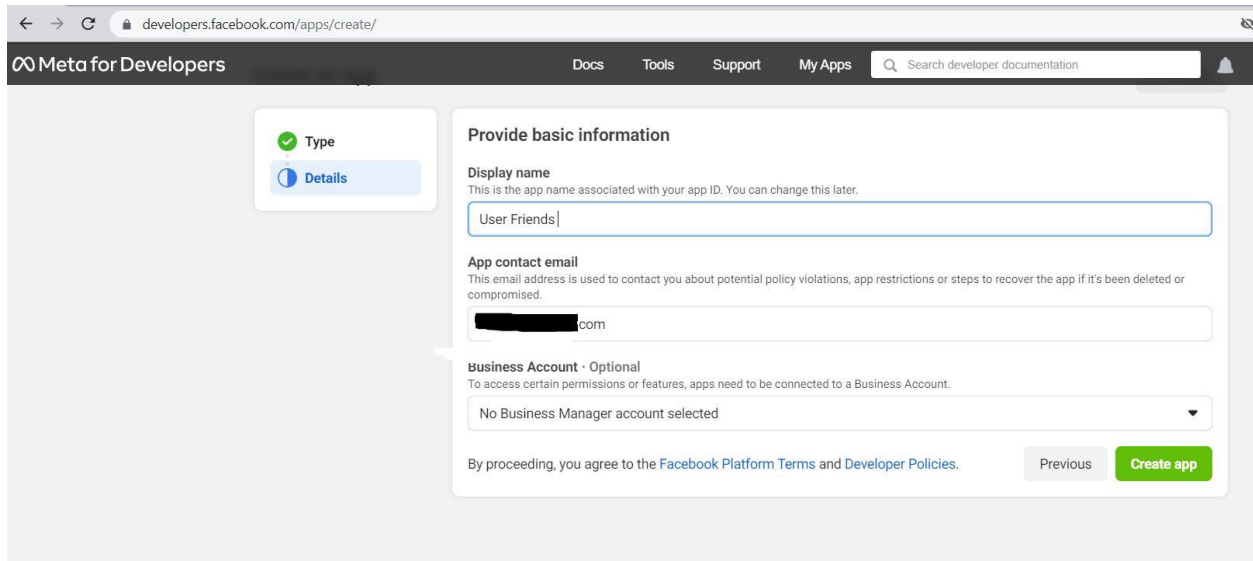
- 1.2.1. Select the required app type



The screenshot shows the 'Create an App' page. On the left, there is a sidebar with two options: 'Type' (selected) and 'Details'. The main content area has a heading 'Select an app type' with a note: 'The app type can't be changed after your app is created. [Learn more](#)'. Below this, there are six app type options, each with an icon and a description:

- Business**: Create or manage business assets such as Pages, events, groups, ads, Messenger and Instagram Graph API using the available business permissions, features and products.
- Consumer**: Connect consumer products and permissions, like Facebook Login and Instagram Basic Display to your app.
- Instant Games**: Create an HTML5 game hosted on Facebook.
- Gaming**: Connect an off-platform game to Facebook Login.
- Workplace**: Create enterprise tools for Workplace from Meta.
- None**: Create an app with combinations of consumer and business permissions and products.

### 1.2.2. Give a Display name, Email and create the app

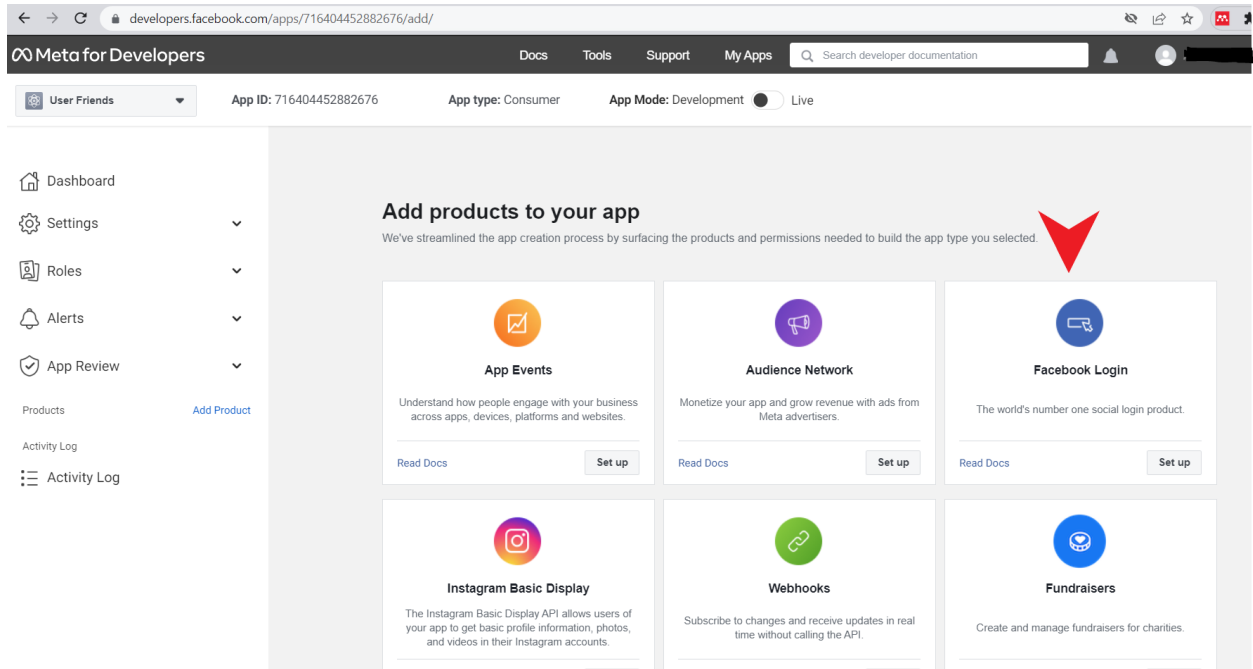


The screenshot shows the 'Provide basic information' step in the Facebook Developer console. On the left, there are two tabs: 'Type' (selected with a green checkmark) and 'Details'. The main form area contains the following sections:

- Display name:** A text input field containing 'User Friends'. Below it, a note states: 'This is the app name associated with your app ID. You can change this later.'
- App contact email:** A text input field containing a redacted email address followed by '.com'. Below it, a note states: 'This email address is used to contact you about potential policy violations, app restrictions or steps to recover the app if it's been deleted or compromised.'
- Business Account - Optional:** A dropdown menu showing 'No Business Manager account selected'. Below it, a note states: 'To access certain permissions or features, apps need to be connected to a Business Account.'

At the bottom of the form, there is a checkbox for 'By proceeding, you agree to the Facebook Platform Terms and Developer Policies.' and two buttons: 'Previous' and 'Create app'.

### 1.2.3. Once the app is created from app product chose Facebook Login



The screenshot shows the 'Add products to your app' page in the Facebook Developer console. The top navigation bar includes the 'Meta for Developers' logo, 'Docs', 'Tools', 'Support', 'My Apps', and a search bar. Below the navigation bar, the app's details are shown: 'User Friends' (selected), 'App ID: 716404452882676', 'App type: Consumer', and 'App Mode: Development' (selected over 'Live').

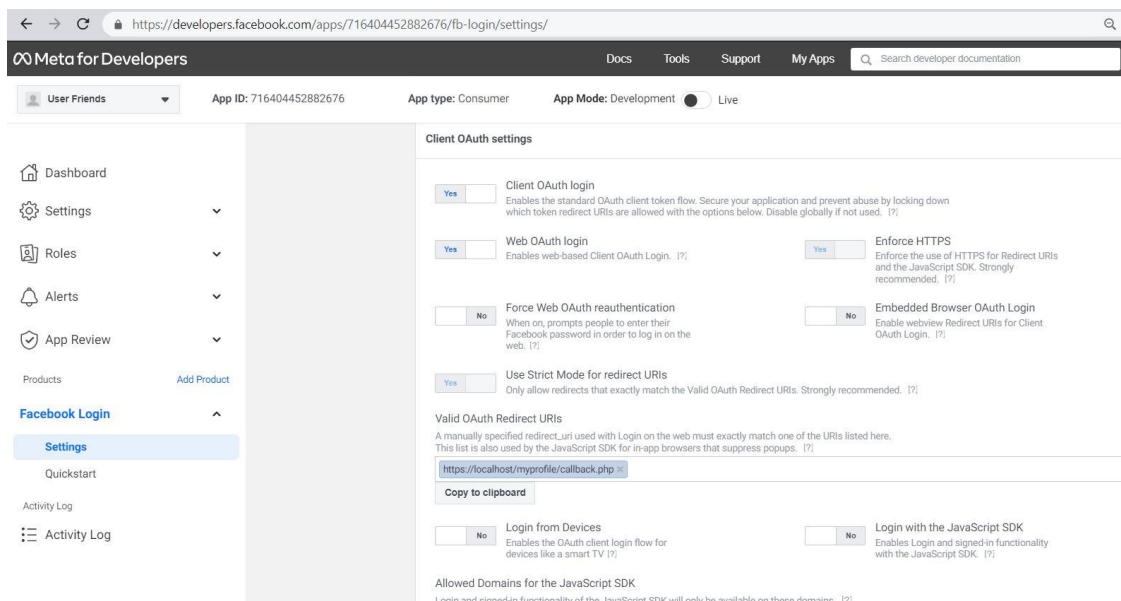
The main content area is titled 'Add products to your app' with a subtitle: 'We've streamlined the app creation process by surfacing the products and permissions needed to build the app type you selected.' A red arrow points to the 'Facebook Login' product card.

The page displays six product cards in a 2x3 grid:

- App Events:** Understand how people engage with your business across apps, devices, platforms and websites. Includes 'Read Docs' and 'Set up' buttons.
- Audience Network:** Monetize your app and grow revenue with ads from Meta advertisers. Includes 'Read Docs' and 'Set up' buttons.
- Facebook Login:** The world's number one social login product. Includes 'Read Docs' and 'Set up' buttons. A red arrow points to this card.
- Instagram Basic Display:** The Instagram Basic Display API allows users of your app to get basic profile information, photos, and videos in their Instagram accounts. Includes 'Read Docs' and 'Set up' buttons.
- Webhooks:** Subscribe to changes and receive updates in real time without calling the API. Includes 'Read Docs' and 'Set up' buttons.
- Fundraisers:** Create and manage fundraisers for charities. Includes 'Read Docs' and 'Set up' buttons.

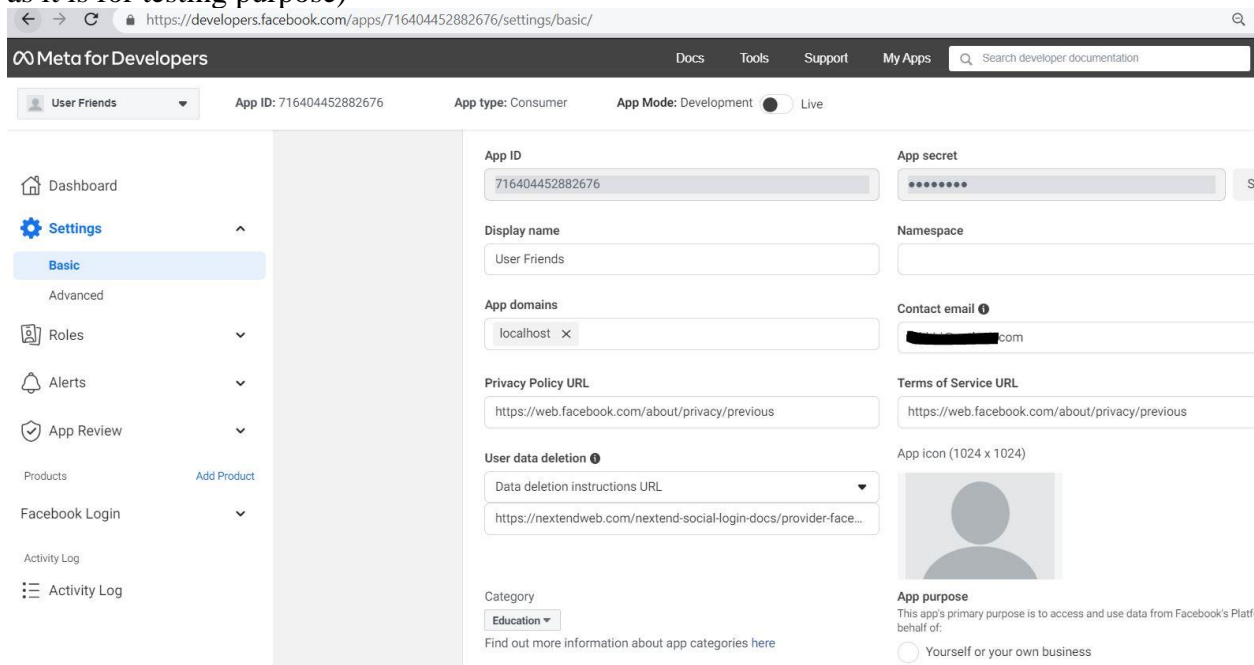
On the left side of the page, there is a sidebar with navigation links: 'Dashboard', 'Settings', 'Roles', 'Alerts', 'App Review', 'Products' (with an 'Add Product' link), 'Activity Log', and 'Activity Log'.

1.3 Under “Facebook Login” select settings. Provide the OAuth Redirection URL. (This is the URL of the web application where response from Facebook is captured.) For testing this web application is hosted in localhost hence the URL is provided here is on localhost.



The screenshot shows the 'Client OAuth settings' page in the Facebook Developer console. The left sidebar contains navigation links: Dashboard, Settings, Roles, Alerts, App Review, Products, Facebook Login (expanded), and Activity Log. The 'Facebook Login' section is active, showing 'Settings'. The main content area is titled 'Client OAuth settings' and includes several toggle switches and text fields. The 'Valid OAuth Redirect URIs' section contains a text field with the value 'https://localhost/myprofile/callback.php' and a 'Copy to clipboard' button. Other settings include 'Client OAuth login', 'Web OAuth login', 'Enforce HTTPS', 'Force Web OAuth reauthentication', 'Embedded Browser OAuth Login', 'Use Strict Mode for redirect URIs', 'Login from Devices', and 'Login with the JavaScript SDK'.

1.4 Now go to Setting > basic and provide the required information. (Dummy data is provided as it is for testing purpose)



The screenshot shows the 'Basic' settings page in the Facebook Developer console. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Basic' and contains various fields for app configuration. The 'App ID' field is filled with '716404452882676'. The 'App secret' field is filled with a masked value. The 'Display name' field is filled with 'User Friends'. The 'App domains' field is filled with 'localhost'. The 'Privacy Policy URL' field is filled with 'https://web.facebook.com/about/privacy/previous'. The 'Terms of Service URL' field is filled with 'https://web.facebook.com/about/privacy/previous'. The 'User data deletion' section has a dropdown menu for 'Data deletion instructions URL' and a text field for 'https://nextendweb.com/nextend-social-login-docs/provider-face...'. The 'App icon' field shows a placeholder image. The 'App purpose' section has a radio button selected for 'Yourself or your own business'.

Now the Facebook app is configured. The App ID, APP Secret and the OAuth Redirest URI should be note down as its required to mention these information in the web application.

## **Step 2 – Creating the Web Application**

The Web application is created using PHP. Facebook PHP SDK is used to access the Facebook Platform from the web app without any manual configurations.

There will be two front end HTML/CSS coded pages as login page and index page where the results will be shown. And two server-side PHP codes as config.php and callback.php.

### **2.1 Creating the Login Page. (Refer Code in Appendix)**

In the login Page there is an option to login with Facebook and Register as well.

### **2.2. Code the config.php**

Here the App ID, App secret which was given by the Facebook is mentioned and this is accessed by the callback.php page. The Facebook PHP SDK is also defined here.

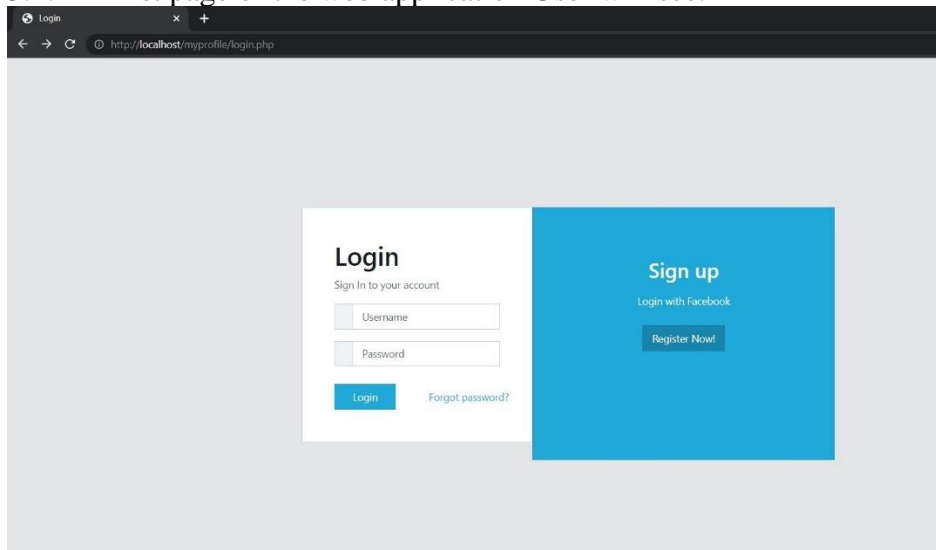
### **2.3 Coding the Callback**

The callback.php file contains the code to get the access token by sending the Authorization code, App ID and APP secret.

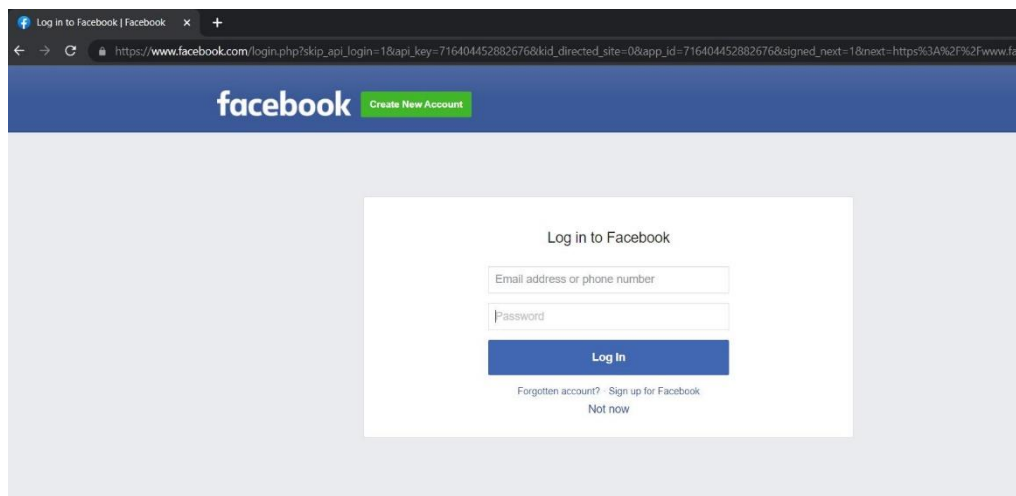
Then with the use of the access token the required user details are retrieved.

## Step 3 – Retrieving resources using OAuth

### 3.1. First page of the web application User will see.

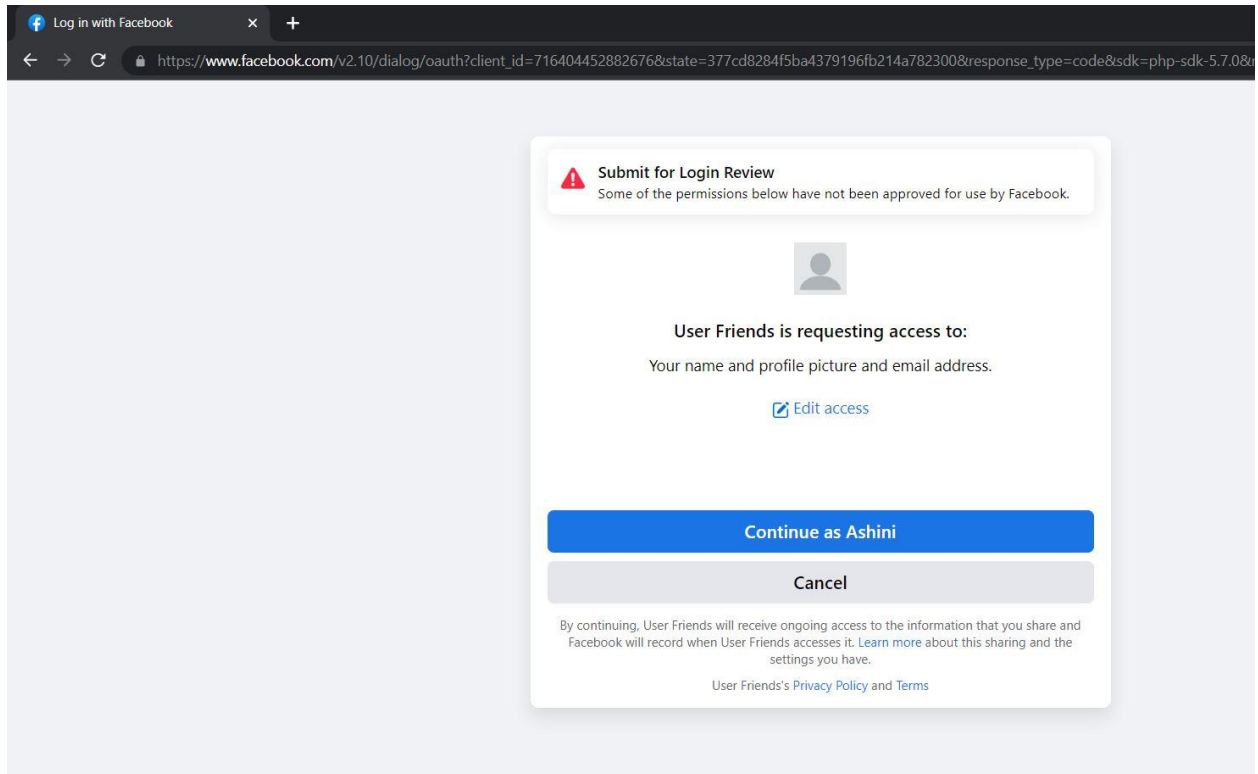


### 3.2. When the user clicks on the “login with Facebook” button the user is redirected to login page of Facebook

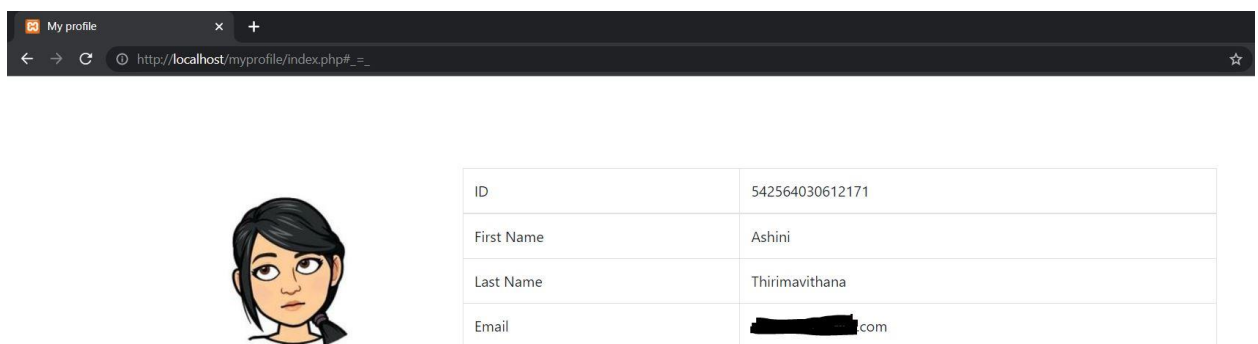




### 3.3. After log in user will be asked to give permission

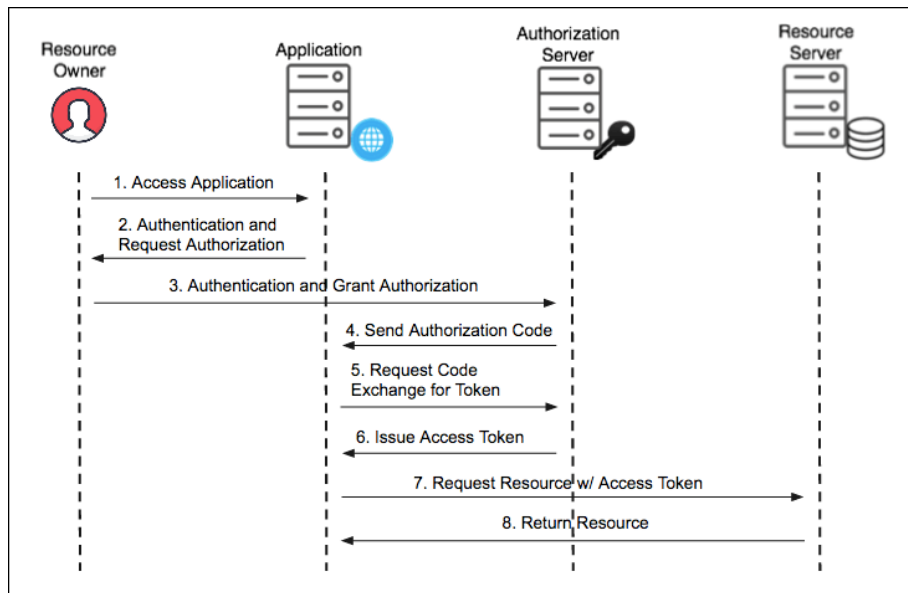


### 3.4. Displaying Retrieved User Details



### 3.3. Methodology

Let's go in details on how these resources were retrieved using the below diagram.



The Diagram shows how the Resources are retrieved which will be shown in the below steps.

1. Resource owners (User) access the application in this scenario 'my profile' application and clicks on the login with Facebook option.
2. Then the Facebook login page come asking for Authentication and Request Authorization
3. Then the user Provides the Authentication (login credential) and grant Authorization (permission for the app)

#### ***Sample Request:***

[https://www.facebook.com/v2.8/dialog/oauth?client\\_id=CLIENT\\_ID&scope=public\\_profile,email&response\\_type=code&redirect\\_uri=REDIRECT\\_URI&state=STATE\\_TOKEN](https://www.facebook.com/v2.8/dialog/oauth?client_id=CLIENT_ID&scope=public_profile,email&response_type=code&redirect_uri=REDIRECT_URI&state=STATE_TOKEN)

#### ***Actual Request:***

[https://www.facebook.com/v2.10/dialog/oauth?client\\_id=716404452882676&state=ddd70a0a538b8e56a020d727f9acd45f&response\\_type=code&sdk=php-sdk-5.7.0&redirect\\_uri=http%3A%2F%2Flocalhost%2Fmyprofile%2Fcallback.php&scope=email&ret=login&fbapp\\_pres=0&logger\\_id=17e8ddeb-8d9c-44ff-a467-3da67c0c9609&tp=unspecified&cbt=1651319576810](https://www.facebook.com/v2.10/dialog/oauth?client_id=716404452882676&state=ddd70a0a538b8e56a020d727f9acd45f&response_type=code&sdk=php-sdk-5.7.0&redirect_uri=http%3A%2F%2Flocalhost%2Fmyprofile%2Fcallback.php&scope=email&ret=login&fbapp_pres=0&logger_id=17e8ddeb-8d9c-44ff-a467-3da67c0c9609&tp=unspecified&cbt=1651319576810)

4. Then the Authorization Server Facebook provide with the Authorization Code.

***Authorization Code Generated:***

[http://localhost/myprofile/callback.php?code=AQAdtPRGqw3tN2tL6ONDKnNRjaPI6\\_0pqmm08R7ISHxQdvoxGsCgaFa69XewzP1UoQ2Nx6o15siq9IJLK9JoabMVPKqfz9mmQmfGfz04Eu8jKJtVv2nHRMO1bTbJ5utChrxGOdlZ\\_h8Q-agQXIL\\_KCtQP3kYITecuDcEEpsePUI7upft2o4uK6o5-tBvd-nL7BMxurfkTDgxRuYbhWC3hG6SVcxO6hGmEgkQF3A53crLS9NA83bgv6a-qHvY8oPKa3tv67eqlPKjfGlqtxPuXhB9P6s6WDp5H50CIANGOSqqawqY8eONVnQITvCHyvJ6OJa83uNZ\\_zbEXBGVG-7Xz8hk-oEmLFhWGMOQRsBIOmDQk8aYyytaebE00Fr3vIZ0aM&state=ddd70a0a538b8e56a020d727f9acd45f#](http://localhost/myprofile/callback.php?code=AQAdtPRGqw3tN2tL6ONDKnNRjaPI6_0pqmm08R7ISHxQdvoxGsCgaFa69XewzP1UoQ2Nx6o15siq9IJLK9JoabMVPKqfz9mmQmfGfz04Eu8jKJtVv2nHRMO1bTbJ5utChrxGOdlZ_h8Q-agQXIL_KCtQP3kYITecuDcEEpsePUI7upft2o4uK6o5-tBvd-nL7BMxurfkTDgxRuYbhWC3hG6SVcxO6hGmEgkQF3A53crLS9NA83bgv6a-qHvY8oPKa3tv67eqlPKjfGlqtxPuXhB9P6s6WDp5H50CIANGOSqqawqY8eONVnQITvCHyvJ6OJa83uNZ_zbEXBGVG-7Xz8hk-oEmLFhWGMOQRsBIOmDQk8aYyytaebE00Fr3vIZ0aM&state=ddd70a0a538b8e56a020d727f9acd45f#) =

5. Then the Application request code exchange for token. (Refer Appendix code in callback.php)

```
$oAuth2Client = $FBObject->getOAuth2Client();  
$accessToken = $oAuth2Client->getLongLivedAccessToken($accessToken);
```

6. Then the Authorization Server (Facebook) issue the access Token
7. Application Request the resources with the access token from the resource Server ( Also Facebook) (Refer Appendix code in callback.php)

```
8. $response = $FBObject->get("/me?fields=id, first_name, last_name, email,  
picture.type(large)", $accessToken);
```

Here the resources requested from facebook are ID, First name, Last name, Email and Picture.

9. Facebook return the Resources.

## References

- [1] Internet Engineering Task Force (IETF), “The OAuth 2.0 Authorization Framework.” <https://tools.ietf.org/html/rfc6749> (accessed Apr. 08, 2022).

## Appendix

### 1. Login Page

```
<?php
include('configuration.php');

if(isset($_SESSION['accesstoken'])){
    header("Location: index.php");
    exit();
}

$redirectTo = "http://localhost/myprofile/callback.php";
$data = ['email'];
$fullURL = $handler->getLoginUrl($redirectTo, $data);
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <title>Login </title>
    <link href="css/styledoc.css" rel="stylesheet">
</head>

<body class="app flex-row align-items-center">
<div class="container">
<div class="row justify-content-center">
<div class="col-md-8">
<div class="card-group">

    <form method="post" action="">
        <div class="card p-4">
            <div class="card-body">
                <h1>Login</h1>
                <p class="text-muted">Log In to your account</p>
                <div class="input-group mb-3">
                    <div class="input-group-prepend">
                        <span class="input-group-text"><i class="icon-user"></i></span>
                    </div>
                    <input type="text" id="txtUser" placeholder="Enter Username"
class="form-control" >
                </div>
                <div class="input-group mb-4">
                    <div class="input-group-prepend">
```

```

        <span class="input-group-text"><i class="icon-lock"></i></span>
    </div>
    <input type="password" id="txtPass" placeholder="Enter Password"
class="form-control" >
    </div>
    <div class="row">
        <div class="col-6">
            <button type="submit" name="btn_login" class="btn btn-primary
px-4">Login</button>
        </div>
        <div class="col-6 text-right">
            <button type="button" class="btn btn-link px-0">Forgot
password?</button>
        </div>
    </div>
</div>
</div>
</div>
</div>
</form>

<div class="card text-white bg-primary py-5 d-md-down-none"
style="width:44%">
    <div class="card-body text-center">
        <div>
            <h2>Sign up</h2>
            <input type="button" value="Login with Facebook onclick="window.location
= '<?php echo $fullURL ?>' " class="btn btn-primary active mt-3" " >
            <br>
            <button type="button" class="btn btn-primary">Register Now!</button></a>
        </div>
    </div>
</div>

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

```

## 2. Index Page

```
<?php
session_start();

if(!isset($_SESSION['accesstoken'])){
    header("Location: login.php");
    exit();
}
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <title>My profile</title>
    <link href="css/styledoc.css" rel="stylesheet">

<body>
<div class="container" style="margin-top: 100px">
    <div class="row justify-content-center">
        <div class="col-md-3">
            
        </div>

        <div class="card-body">
            <table class="table table-striped">
                <thead>
                    <tr>
                        <th>ID</th>
                        <th>First Name</th>
                        <th>Last Name</th>
                        <th>Email</th>
                    </tr>
                </thead>
                <tbody>

                    <tr>
                        <td><?php echo $_SESSION['userData']['id'] ?></td>
                        <td><?php echo $_SESSION['userData']['first_name']
?></td>

                        <td><?php echo $_SESSION['userData']['last_name'] ?></td>
                        <td><?php echo $_SESSION['userData']['email'] ?></td>
                    </tr>
                </tbody>
            </table>
```

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

### 3. Configuration code

```
<?php
session_start();
include('FacebookPHPSDK/autoload.php');

$FBObject = new \Facebook\Facebook([
    'app_id' => '716404452882676',
    'app_secret' => '3187403ef3ae6088d4ea076f7f3c2a62',
    'default_graph_version' => 'v2.10'
]);

$handler = $FBObject -> getRedirectLoginHelper();
?>
```

#### 4. Callback Code

```
<?php
include("configuration.php");

try {
    $accessToken = $handler->getAccessToken();
} catch(\FacebookPHPSDK\Exceptions\FacebookResponseException $excep){
    echo "Response Exception: " . $excep->getMessage();
    exit();
} catch(\FacebookPHPSDK\Exceptions\FacebookSDKException $xcepe){
    echo "SDK Exception: " . $excep->getMessage();
    exit();
}

if(!$accessToken){
    header('Location: login.php');
    exit();
}

$oAuth2Client = $FBObject->getOAuth2Client();
if(!$accessToken->isLongLived())
    $accessToken = $oAuth2Client->getLongLivedAccessToken($accessToken);
$response = $FBObject->get("/me?fields=id, first_name, last_name, email,
picture.type(large)", $accessToken);
$userData = $response->getGraphNode()->asArray();
$_SESSION['userData'] = $userData;
$_SESSION['accesstoken'] = (string) $accessToken;
header('Location: Index.php');
exit();
?>
```