OAuth 2.0: Authorization Code Flow

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

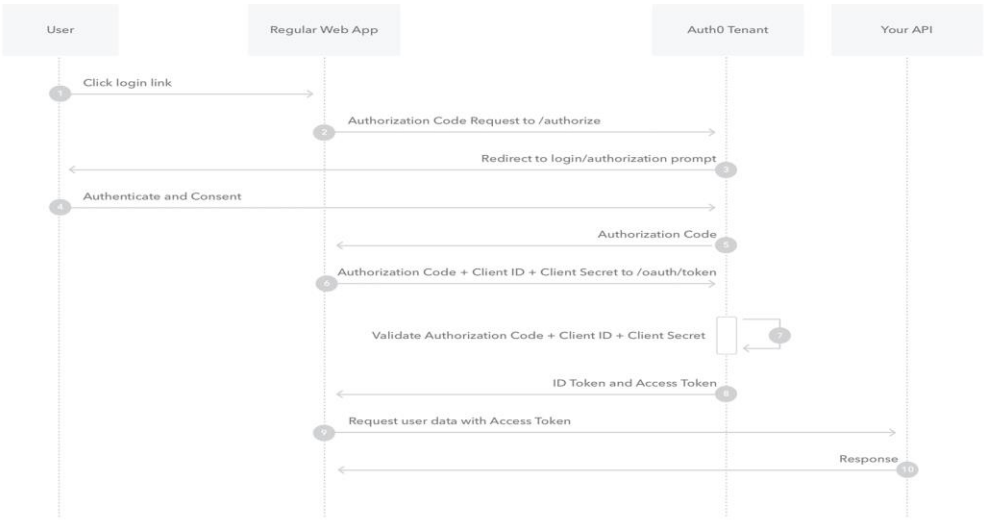


Fig 1. Authorization Code Flow [2]

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.

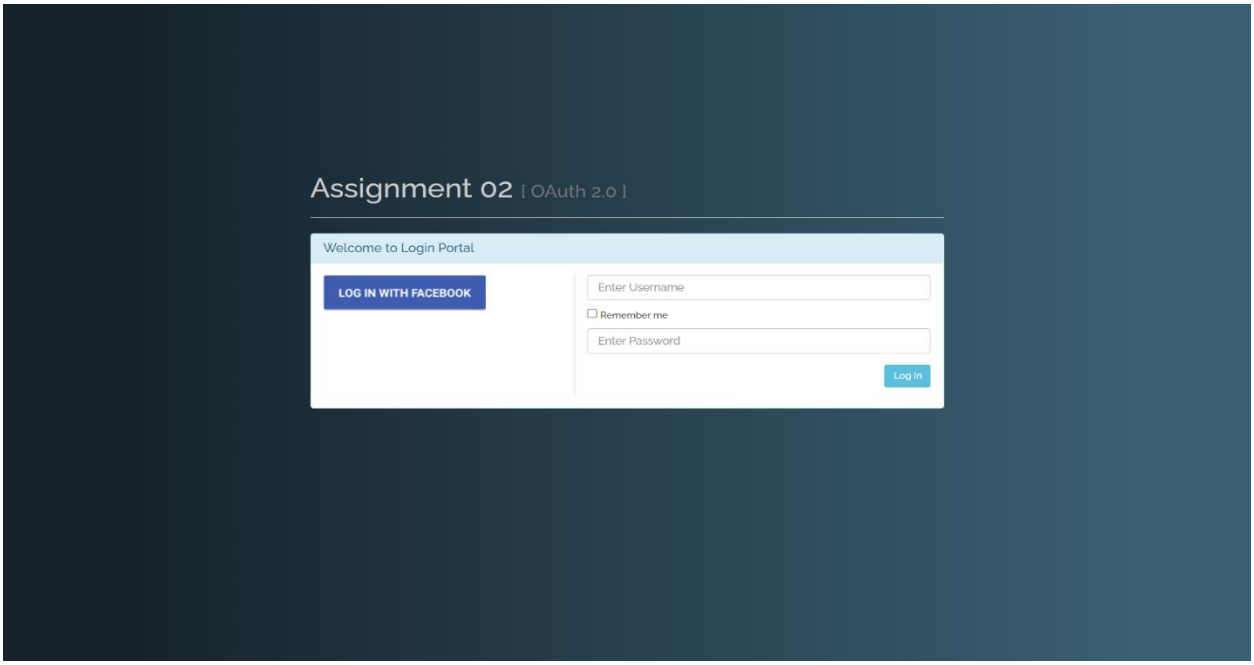


Fig 2. User Log in Page

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].

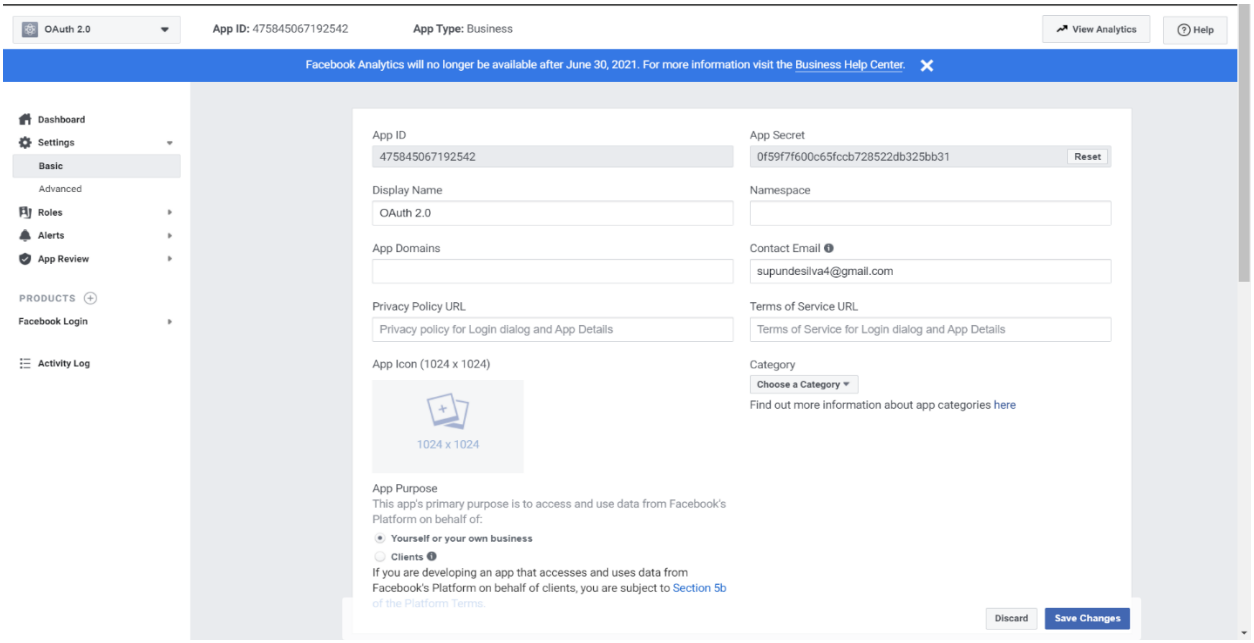


Fig 3. Application Properties

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.

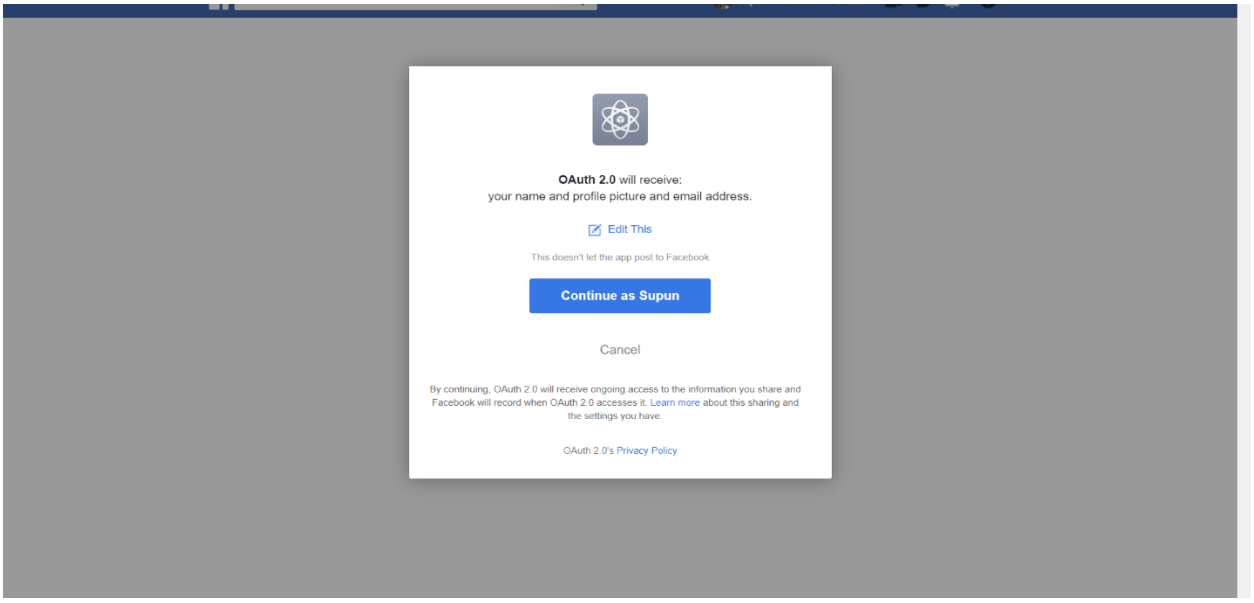
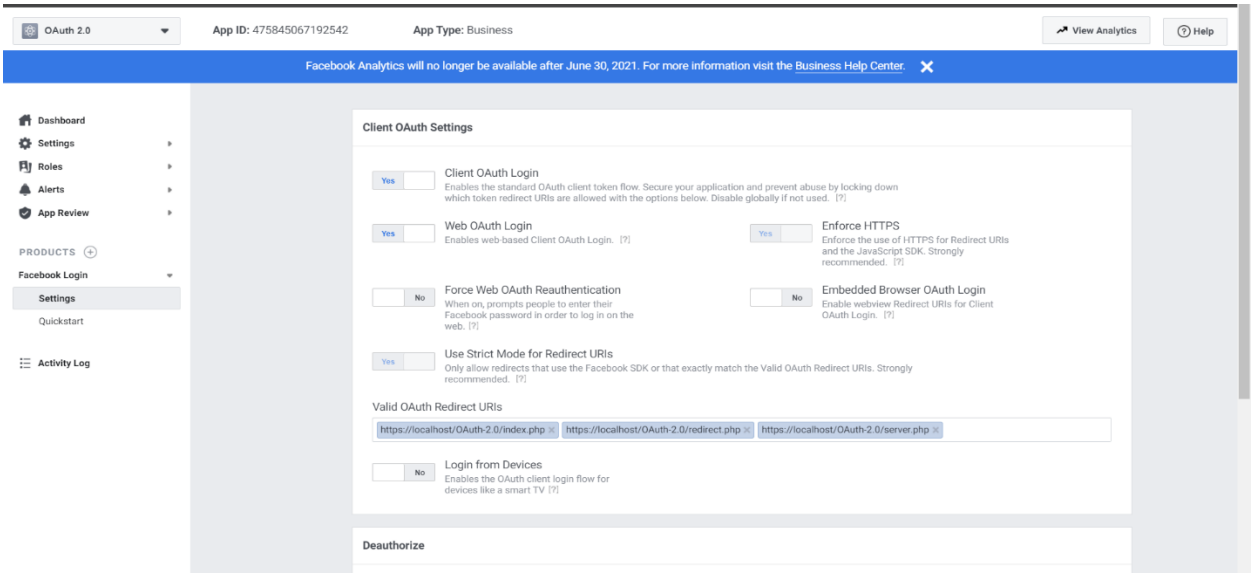


Fig 4. User Consent Prompt

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.



APPENDIX: Code Samples

Fig 5. Application URI Properties

Config.php

```
<?php

//function to get Access token
   function get_auth_code($client_id, $redirect_uri, $auth_code, $appID_secret_base64)
   {
      //define parameter using array
      $data = array('grant_type'=>'authorization_code', 'client_id'=>$client_id,'redirect_uri'=>$redirect_uri,'code'=>$auth_code);

      //build http query
      $query = http_build_query($data);

   //create http contex details
   $contex_data = array(
                  'method'=>'POST',
                  'header'=>'Authorization:Basic '.$appID_secret_base64,
                  'content'=>$query
                 );

   //create contex resource for POST request
   $contx = stream_context_create(array('http'=>$contex_data));

   //store resuts in variable
   $access_token = file_get_contents('https://graph.facebook.com/oauth/access_token',false,$contx);

return $access_token;
```

```
    }

    //change this according to your need * ex :- scope *
    function AUTH_URL($client_id,$redirect_url)
    {
        $url = "https://www.facebook.com/dialog/oauth?response_type=code&client_id=$client_id&redirect_uri=$redirect_url&scope=public_profile%20email";

        return $url;
    }

    //function to get user ID
    function get_user_id($access_token)
    {
        $parameters = array('fields'=>'id');
        $buildParam = http_build_query($parameters);
        $requestContent = array('method'=>'GET','header'=>'Authorization:Bearer '.$access_token,'content'=>$buildParam);
        $reqcontex = stream_context_create(array('http'=>$requestContent));
        $result = file_get_contents('https://graph.facebook.com/v3.0/me?',false,$reqcontex);

        return $result;
    }

//functions to get basic info of account
```

```
   function get_user_basics($access_token,$user_id)
   {
      $parameters = array('fields'=>'id,email');
      $buildParam = http_build_query($parameters);
      $requestContent = array('method'=>'GET','header'=>'Authorization:Bearer '.$access_token
,'content'=>$buildParam);
      $reqcontex = stream_context_create(array('http'=>$requestContent));
      $resultmail =
file_get_contents('https://graph.facebook.com/v3.0/'.$user_id.'?fields=email,picture',false,$re
qcontex);

      return $resultmail;

   }

   function post_fb($access_token, $message, $user_id)
   {
      $requestContent = array('method'=>'POST','header'=>'Authorization:Bearer
'.$access_token ,'content'=>$buildParam);
      $reqcontex = stream_context_create(array('http'=>$requestContent));
      $postMessage =
file_get_contents('https://graph.facebook.com/'.$user_id.'/feed?message='.$message.'&access
_token='.$access_token,false,$reqcontex);

      return $postMessage;
   }

   function foo()
{
```

```
    return "Coded with Love";
  }

?>
```

Index.php

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

  session_start();




?>



<!DOCTYPE html>
<html>
<head>
<title> Assignment 02 </title>
<meta charset="utf-8"/>
<link rel="stylesheet" href="//maxcdn.bootstrapcdn.com/bootstrap/3.3.0/css/bootstrap.min.css" id="bootstrap-css" />
<script src="//maxcdn.bootstrapcdn.com/bootstrap/3.3.0/js/bootstrap.min.js"> </script>
<script src="//code.jquery.com/jquery-1.11.1.min.js"></script>
<link href='http://fonts.googleapis.com/css?family=Raleway:500' rel='stylesheet' type='text/css'>
<script type="text/javascript" src="config.js"> </script>
```

```
<style>

body {
   width:100px;
        height:100px;
 background: -webkit-linear-gradient(90deg, #16222A 10%, #3A6073 90%); /* Chrome 10+, Saf5.1+ */
 background:   -moz-linear-gradient(90deg, #16222A 10%, #3A6073 90%); /* FF3.6+ */
 background:    -ms-linear-gradient(90deg, #16222A 10%, #3A6073 90%); /* IE10 */
 background:     -o-linear-gradient(90deg, #16222A 10%, #3A6073 90%); /* Opera 11.10+ */
 background:       linear-gradient(90deg, #16222A 10%, #3A6073 90%); /* W3C */
font-family: 'Raleway', sans-serif;
}

.middlePage {
        width: 780px;
   height: 500px;
   position: absolute;
   top:0;
   bottom: 0;
   left: 0;
   right: 0;
   margin: auto;
}

p {
```

```
        color:#CCC;
}

.spacing {
        padding-top:7px;
        padding-bottom:7px; }

.logo {
        color:#CCC;
}

</style>




</head>
<body>

<div class="middlePage">
<div class="page-header">
   <h1 class="logo">Assignment 02 <small> [ OAuth 2.0  ] </small> </h1>
</div>

<div class="panel panel-info">
   <div class="panel-heading">
<h3 class="panel-title"> Welcome to Login Portal </h3>
```

```
  </div>

  <div class ="panel-body">
    <div class="row">
      <div class="col-md-5">
      <a href="<?php echo AUTH_URL("475845067192542","https%3A%2F%2Flocalhost%2FOAuth-2.0%2Fredirect.php"); ?>" onclick="return getCount();"><img src="fb.png" width="200" heigt="100"/></a>
      </div>

      <div class="col-md-7" style="border-left:1px solid #ccc;height:160px">
        <form class="form-horizontal" method="POST" action="server.php" >
          <input name="user_name" type="text" placeholder="Enter Username" class="form-control input-md">
          <div class="spacing"><input type="checkbox" name="checkboxes" id="checkboxes-0" value="1"><small> Remember me</small></div>
          <input name="user_pswd" type="password" placeholder="Enter Password" class="form-control input-md">
          <div class="spacing"><input type="hidden" id="csToken" name="CSR"/></div>
          <input type="submit" name="sbmt" value="Log In" class="btn btn-info btn-sm pull-right">
        </form>
      </div>

    </div>
  </div>

</div>
<?php
```

```
?>

</div>

</body>
</html>
```

Redirect.php

```
<!--Temporary page for redirect results-->
<?php

   require 'config.php';

   session_start();

   echo "Fetching data, Keep Calm for a Suprise";

?>



<?php



  if(isset($_GET['code']))
  {
//get Access token and store it inside $result variable
```

```
   $result = get_auth_code("475845067192542", "https://localhost/OAuth-2.0/redirect.php",
$_GET['code'],
"NDc1ODQ1MDY3MTkyNTQyOjBmNTlmN2Y2MDBjNjVmY2NiNzI4NTIyZGIzMjViYjMx");

   //jason array to fetch token
   $token_json = json_decode($result);


   //set cookie including access token
   if(!isset($_COOKIE['access_token']))
   {
     echo "cookie setting! Please Wait!";
     setcookie("access_token",$token_json->access_token,time()+3600,"/","localhost");
     echo '<script> window.location.assign("https://localhost/OAuth-2.0/server.php") </script>';
   }

   echo '<script> window.location.assign("https://localhost/OAuth-2.0/server.php") </script>';

 }



?>
```

Server.php

```
<?php
```

```
   require 'config.php';


   session_start();




?>


<!DOCTYPE html>

<html>

<head>

   <title> Assingment 02 </title>

   <meta charset="UTF-8"/>

   <link                                                                    rel="stylesheet"
href="//maxcdn.bootstrapcdn.com/bootstrap/3.3.0/css/bootstrap.min.css"   id="bootstrap-css"
/>

   <script src="//maxcdn.bootstrapcdn.com/bootstrap/3.3.0/js/bootstrap.min.js"> </script>

   <script src="//code.jquery.com/jquery-1.11.1.min.js"></script>

   <link          href='http://fonts.googleapis.com/css?family=Raleway:500'          rel='stylesheet'
type='text/css'>


   <style>


      body{

         background: linear-gradient(to left, #5499c7, #2471a3);

}
```

```
    h3{
        color:white;
        border-bottom:1px solid red;
        padding-bottom:3px;
    }

    h4{
        padding:6px;
        border-radius:6px;
    }

    .fbdet{
        border-right: 2px solid black;
        padding-right: 7px;
    }

    .well{
        background: linear-gradient(to left,#d4e6f1,#e8daef );
    }

    .btns{
        padding-top:7px;
    }

    .bg-info{
padding:4px;
        border-radius:8px;
```

```
        }

        .msg_head{
            border-bottom:1px solid white;
            color: #e5e7e9;
        }

        .form-group{
            padding: 6px;
            background: #884ea0;
            color:white;
        }

    </style>

<script>

        function open()
        {
            alert("Save?");
        }

</script>

</head>
<body onbeforeunload="return open()">
<div class="container-fluid">
```

```
 <div class="row">


   <!-- Right side tab -->


  <div class="col-md">
  <div class="fbdet">
    <div class="row">
      <div class="col-md-12">
        <h3> Facebook - OAuth 2.0 </span> </h3> <br/>
        <div class="well well-sm"> <?php user(); ?> <p> <img src="<?php echo userBasics()->picture->data->url;?>" width="60" height="60" /> </p>
                        <p> Name : <?php echo user()->name; ?> </p>
                        <p> E-Mail : <?php echo userBasics()->email; ?> </p>
        </div>



      </div>
    </div>
  <!-- End of right side first block -->


      <div class="row">
        <div class="col-md-12">
          <div class="well well-sm"> Logout <a href="http://localhost/OAuth-2.0/login.php" target="_self">Save Cookies </a> Now </div>
        </div>
</div>
```

```
  </div>
  </div>

  <!-- Body -->

 </div>
  <div class="footer">
   <p><?php echo foo(); ?></p>
  </div>

</div>

<?php

  //php intraction functions

  //set user ID to session variable. this function should be called first
  function user()
  {
     $result=get_user_id($_COOKIE['access_token']);
     $jason = json_decode($result);
     $_SESSION['id'] = $jason->id;

     return $jason;
  }
function userBasics()
     {
```

```
        if(isset($_SESSION['id']))
        {
        $rsult = get_user_basics($_COOKIE['access_token'],$_SESSION['id']);
        $jason = json_decode($rsult);
        //echo $rsult;
        return $jason;
        }
        else
        {
           echo "Session ID Not Detected";
        }
      }

   if(isset($_POST['sbmt']))
   {
      $msg = $_POST['comment'];
     echo post_fb($_COOKIE['access_token'], $msg, $_SESSION['id']);

   }

?>
<script>

window.onbeforeunload = function() {
  var dialogText = 'Keep Calm & Enjoy Coding';
  alert(dialogText);
};
```

```
</script>

</body>

</html>
```

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.