SOftware security

Assignment 02

MS21908842

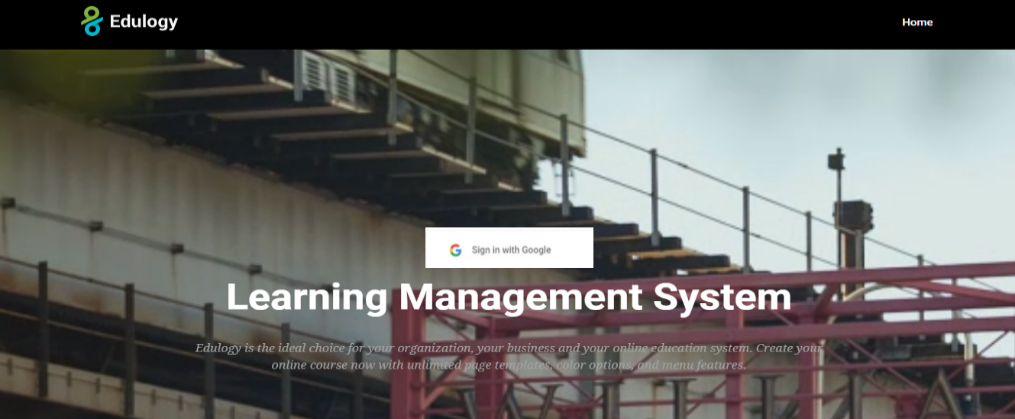
G.A.P Madubashana

1. Introduction

This report describes about the public oauth server details and other functionalities of the Learning Management System which is implemented to demonstrate the oauth authorization server. This, system is use google oauth server to validate the users and provide access to the system to perform their tasks. The system allows users to upload assignment to the google drive, view course details and register for courses after successfully login to the system using google authorizations.

1. System Structure

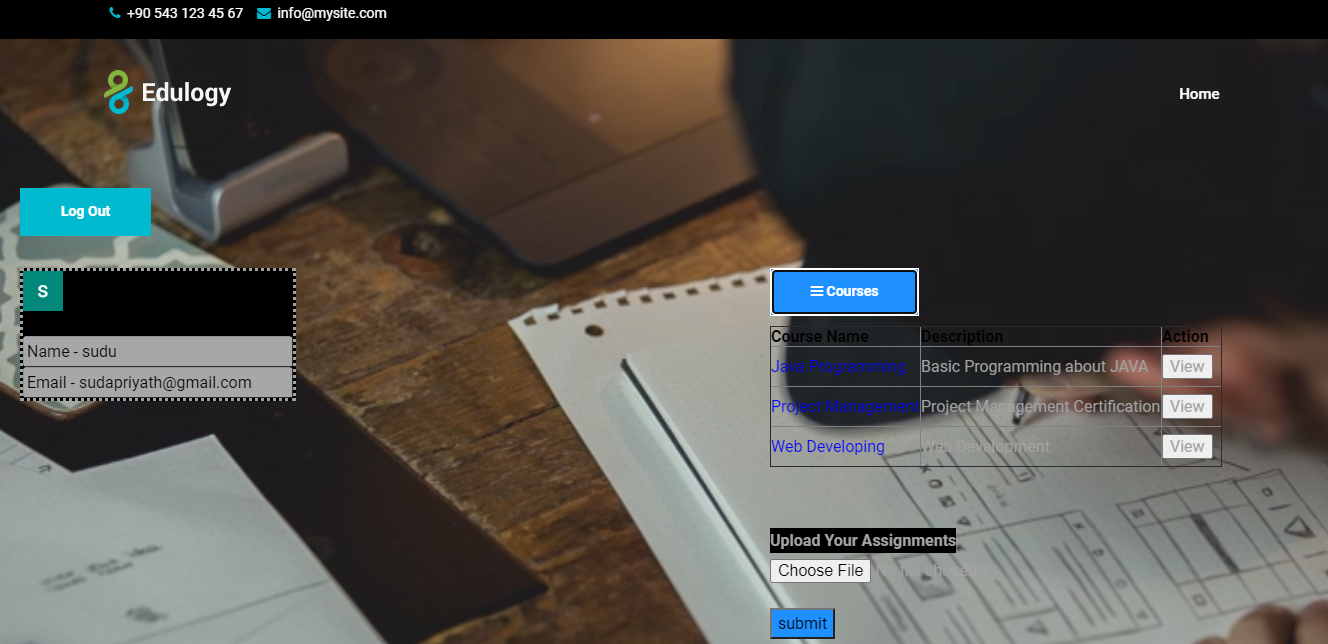
**Home page**



Click on ‘Sign in’ button to login to the web application

Figure : Home Page

**Registered users’ view**



Click to choose a file

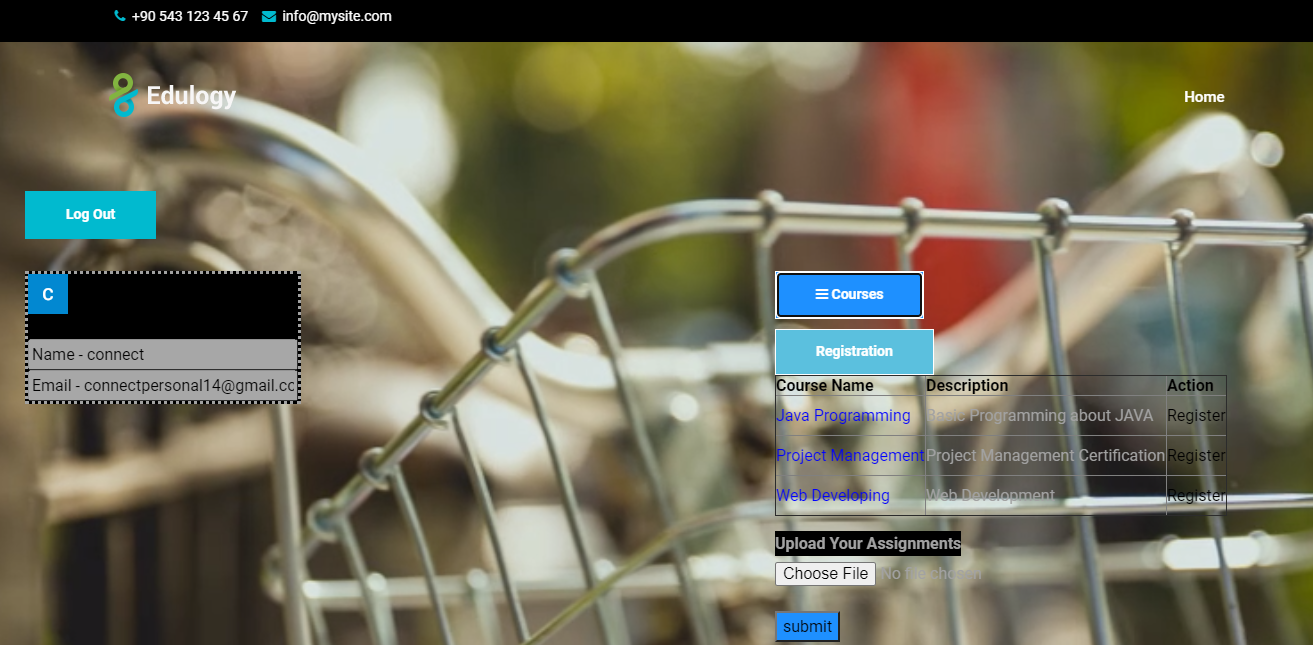
Click to submit the file to the google drive of the institute

Click to view course details

Click to view courses

Figure : Registered User's View

**Unregistered users’ view**



Click to register

Figure : Unregistered User's View

1. Integrating Google Sign-in

This Learning Management System use authorization credentials to provide google sign-in for user. Below are the steps that followed to create the google authorization credentials.

1. Create a Project in the Credentials page.

Create a project using the credentials page and select that project in order to create credentials.

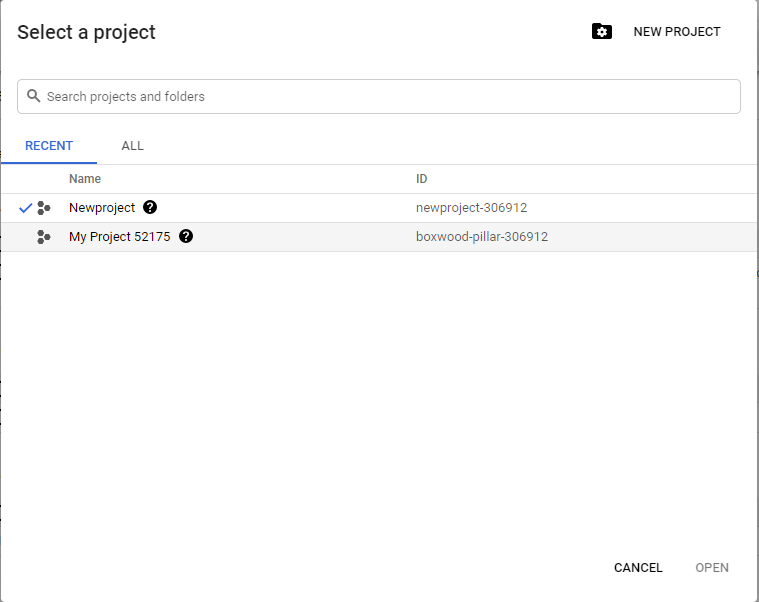


Figure : Creating a Project

1. Click on Create Credentials

Click on create credentials and after that it will prompt a message box. Then click on ‘OAuth client ID’.

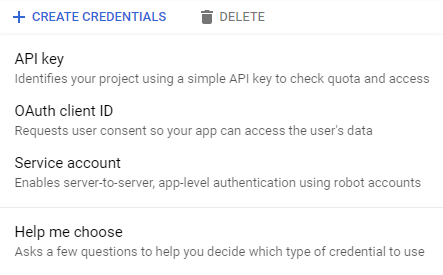


Figure : Creating Credentials - 1

1. Select application type and adding necessary information.

After come in to the ‘create credentials page’, select the type of application that need to create the credentials and provide a name for that OAuth 2.0 client.

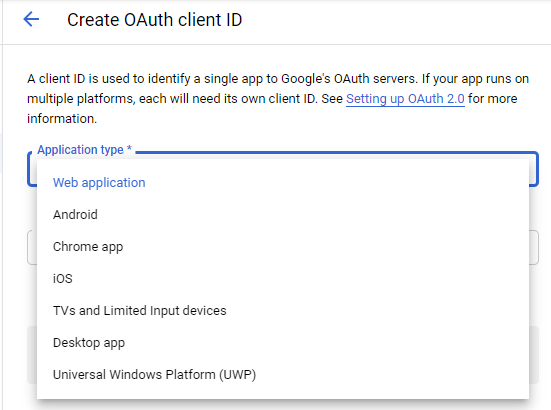


Figure : Creating Credentials - 2

Fill out the redirect URIs or JavaScript origins if any and click on create.

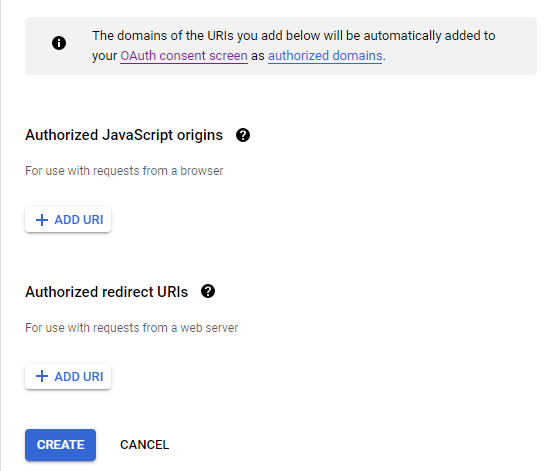


Figure : Creating Credentials - 3

After creating the credentials, those details are appearing in the OAuth 2.0 client IDs section.

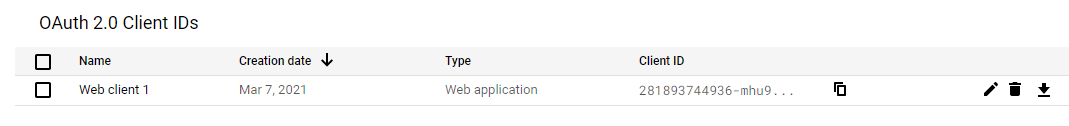


Figure : OAuth Client IDs

1. Download the JSON file and add it to the application folder.

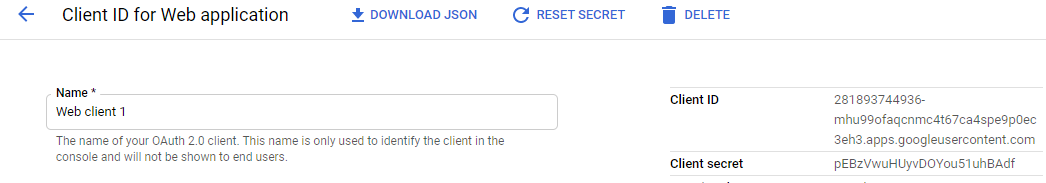


Figure : Download JSON File

1. Get the API files downloaded and add those to the application folder.

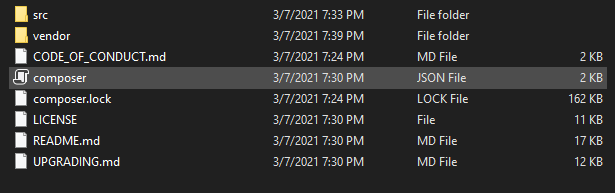


Figure : API Files

1. After do the above steps successfully, then backend of the application need to be developed. So, the codes that used to implement the google sign-in is included in the appendix section.
2. Google OAuth 2.0 Process

Mainly, this authorization process needed some key components such as client id, client secret and access token.

* Client ID – Identifier for the particular application and a unique string which is representing the registration details provided by the client.
* Client Secret – This client password uses to authenticate with the google server.
* Access Token – The token which is issued to the client after the authorization and the life time of this token to limited to a particular time period.

When a user tries to login to the Learning Management System, following are the steps that occurring till the authorization.

1. Create authorization request and set parameters.

In this step authorization request will be created.

1. In order to authenticate, particular user redirect to OAuth 2.0 server.
2. At this step, Google prompts a consent window to the user and it request access.
3. Handle the OAuth 2.0 server response

At this stage, if the user accepts the particular request, authorization code will be received and if not an error message will be received as the response.

1. After receive the authorization code to the web server, it can exchange the authorization code for an access token.

Following diagram depicts the requests send to OAuth and google servers, and responses received to authorize the website to access the relevant data.

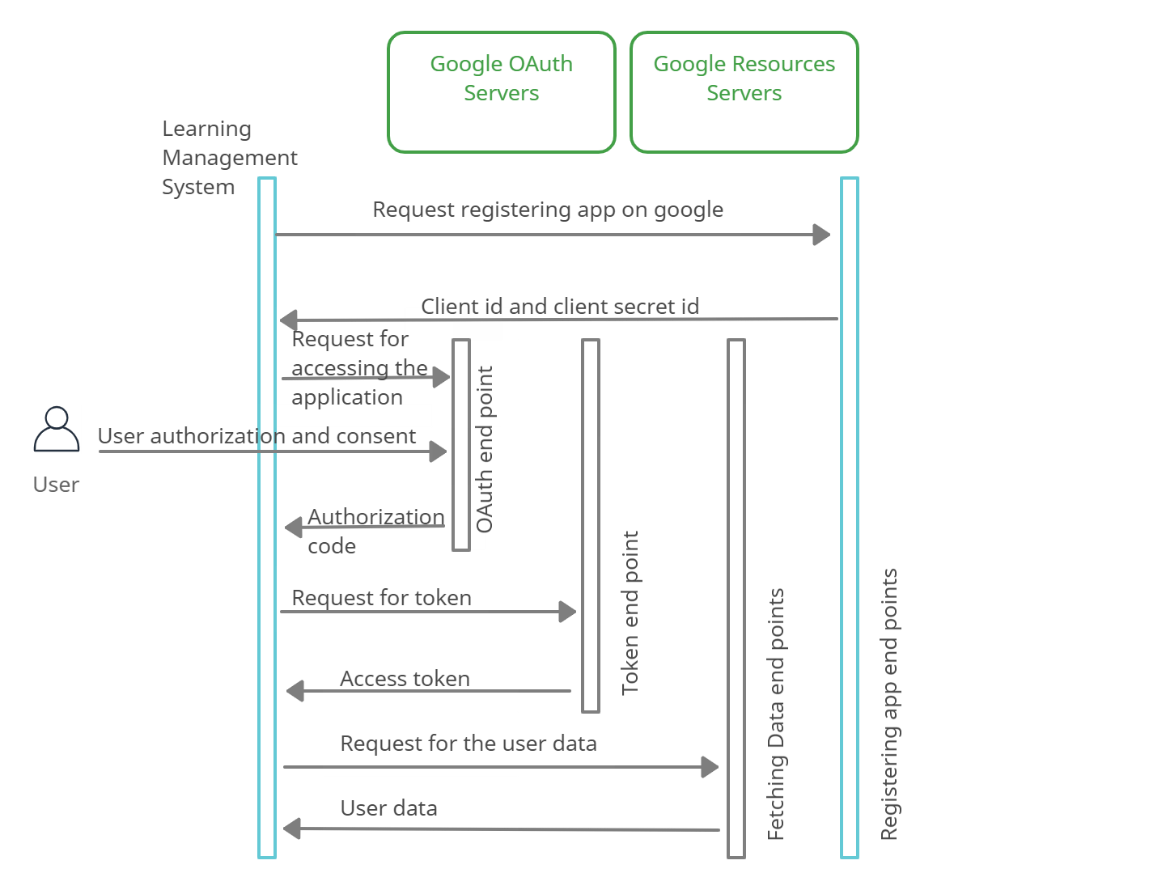


Figure : OAuth and google server Requests

1. Integrating Google Drive API to Upload Files
2. Enable Google Drive API

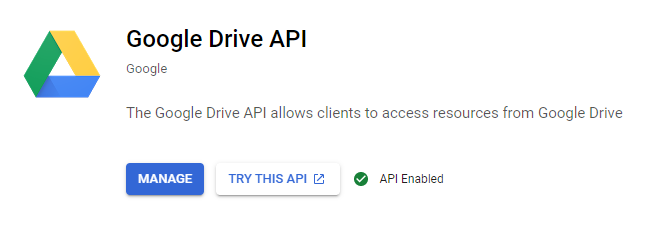


Figure : Enable Google Drive API

1. Configure Google client library in the project

Install the library using following command to the project folder

composer require google/apiclient:^2.0

1. Other Google Resources

* Google map widget was integrated with this web application to indicate the location. That was integrated using a google API key.

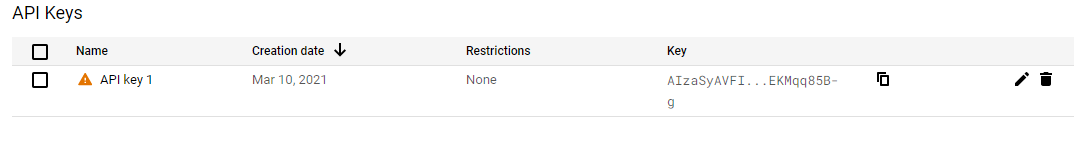


Figure : Google API Keys

Appendix

**Main PHP codes use to perform the functionalities**

<script>

    function myFunction()

    {

       var a = document.getElementById("myDIV");

       if (a.style.display === "none") {

        a.style.display = "block";

            } else {

        a.style.display = "none";

        }

    }

  function reply\_click(clicked\_id)

  {

    if(clicked\_id == '1'){

        document.getElementById("courseid").value = clicked\_id;

        document.getElementById("Price").value = "RS.30000.00";

        document.getElementById("date").value = "Monday - Friday / 3 pm - 5 pm";

    } else if(clicked\_id == '2'){

        document.getElementById("courseid").value = clicked\_id;

        document.getElementById("Price").value = "RS.36000.00";

        document.getElementById("date").value = "Monday - Wednesday / 3 pm - 5 pm";

    } else if(clicked\_id == '3'){

        document.getElementById("courseid").value = clicked\_id;

        document.getElementById("Price").value = "RS.40000.00";

        document.getElementById("date").value = " Saturday - Sunday / 3 pm - 5 pm";

    }

  }

</script>

<?php

error\_reporting(E\_ALL);

ini\_set('display\_errors', 1);

$google\_redirect\_url = 'http://localhost:10080/auth/redirect.php';

session\_start();

// google api files

include\_once 'lib/vendor/autoload.php';

// New google client

$gClient = new Google\_Client();

$gClient->setApplicationName('ApplicationName');

$gClient->setAuthConfigFile('client\_secret\_281893744936-mhu99ofaqcnmc4t67ca4spe9p0ec3eh3.apps.googleusercontent.com.json');

$gClient->addScope(Google\_Service\_Oauth2::USERINFO\_PROFILE);

$gClient->addScope(Google\_Service\_Oauth2::USERINFO\_EMAIL);

// New Google Service

$google\_oauthV2 = new Google\_Service\_Oauth2($gClient);

// LOGOUT?

if (isset($\_REQUEST['logout']))

{

    unset($\_SESSION["auto"]);

    unset($\_SESSION['token']);

    $gClient->revokeToken();

    header('Location: ' . filter\_var($google\_redirect\_url, FILTER\_SANITIZE\_URL));

}

// GOOGLE CALLBACK?

if (isset($\_GET['code']))

{

    $gClient->authenticate($\_GET['code']);

    $\_SESSION['token'] = $gClient->getAccessToken();

    header('Location: ' . filter\_var($google\_redirect\_url, FILTER\_SANITIZE\_URL));

    return;

}

// PAGE RELOAD?

if (isset($\_SESSION['token']))

{

    $gClient->setAccessToken($\_SESSION['token']);

}

// Autologin?

if(isset($\_GET["auto"]))

{

    $\_SESSION['auto'] = $\_GET["auto"];

}

// LOGGED IN?

if ($gClient->getAccessToken())

{

    try {

        $user = $google\_oauthV2->userinfo->get();

        $\_SESSION['token']    = $gClient->getAccessToken();

        $arr = json\_decode(json\_encode($\_SESSION['token']));

        $to = $arr->access\_token;

        file\_put\_contents('token.json',  '{"access\_token": "'.$to.'", "expires\_in": 3599,"refresh\_token":"1\/\/0gjBBJrwz540vCgYIARAAGBASNwF-L9Ir6NhuzuAKDcvGNK28IuaSpHkLzgHXnb8lwunZMatfUZBxtNaIfXDvfC7z4WkgjD\_3QaU","scope":"https:\/\/www.googleapis.com\/auth\/drive","token\_type":"Bearer","created":1618817979}' );

        //(View course details / Course registration / Assignment Submission)

        echo ' <section id="home" class="video-section js-height-full">

        <br /><br /><br /><br /><br /><a  style = "position:absolute; left:30px; top:200px;" href="?logout=1" class="btn btn-primary wow slideInLeft">Log Out</a><br />

        <div style = "position:absolute; left:30px; top:280px;border-style: dotted;background-color: black;">

        <a href="'.$profile\_url.'" style = ""  target="\_blank"><img src="'.$profile\_image\_url.'?sz=40" /></a><br /><br />

        <input type="text" value="Name - '.$user\_name.'" disabled style= "width:270px; color: black; " /><br />

        <input type="text" value="Email - '.$email.'" disabled  style= "width:270px; color: black; "/>

        </div>

        <div style = "position:absolute; left:780px; top:540px;">

              <form action="submit.php" method="post" enctype="multipart/form-data" >

                   <label for="" style = "background-color: Black;">Upload Your Assignments</label>

                   <input type="file" name="file" >

                   <br>

                   <input style = "background-color: DodgerBlue;color: Black;" type="submit" name="submit" value="submit" >

              </form>

        </div>

        <div style = "position:absolute; left:780px; top:280px;">

              <button onclick="myFunction()" class="btn"  style = "background-color: DodgerBlue;"><i class="fa fa-bars"></i> Courses</button>

              <p> </p>

              <div id="myDIV" style="display:none">

                  <table class="data" cellpadding="8" border="1">

                         <thead>

                            <tr>

                                <th class="first" style="width:120px;color: Black;"> Course Name </th>

                                <th class="" style = "color: Black;"> Description </th>

                                <th class="" style = "color: Black;">Action </th>

                            </tr>

                        </thead>

                        <tbody>';

        //Check whether user is registered or not

        $db = mysqli\_connect('localhost', 'root', '', 'test');

        $sql = "SELECT \* FROM registrations WHERE email = '$email'";

        $result = mysqli\_query($db, $sql);

        $rows = mysqli\_num\_rows($result);

        if ($rows > 0) {

         } else {

         }

       echo '

           <div class="modal fade" id="myModal" role="dialog">

               <div class="modal-dialog">

                       <div class="modal-content">

                            <div class="modal-header">

                            </div>

                                <form method="post" id="coursematerials\_data" name="coursematerials\_data" >

                                        <div class="row">

                                            <div class="col-sm-12">

                                                <div class="panel panel-default">

                                                    <div class="panel-body">

                                                <div class="row">

                                                        <div class="col-sm-12">

                                                            <div class="form-group">

                                                                <label for="">Email <span class="required">\*</span></label>

                                                                <input required="true"

                                                                    type="text" name="email" id="email"

                                                                    class="form-control" value="'.$email.'" readonly>

                                                                <div class="help-block with-errors"></div>

                                                            </div>

                                                    </div>

                                                </div>

                                                <div class="row">

                                                        <div class="col-sm-12">

                                                            <div class="form-group">

                                                                <label for="">Name <span class="required">\*</span></label>

                                                                <input required="true"

                                                                    type="text" name="name" id="name"

                                                                    class="form-control">

                                                                <div class="help-block with-errors"></div>

                                                            </div>

                                                    </div>

                                                </div>

                                                <div class="row">

                                                    <div class="col-sm-12">

                                                        <div class="form-group pull-right">

                                                            <button type="submit" class="btn btn-success" name="save" id="save">

                                                                <span class="glyphicon glyphicon-send"></span>&nbsp;&nbsp; Submit

                                                            </button> &nbsp;

                                                                <button type="button" class="btn btn-default" data-dismiss="modal">Close</button>

                                                            </a>

                                                        </div>

                                                    </div>

                                                </div>

                                    </div>

                                </div>

                            </div>

                        </div>

                    </form>

                 </div>

              </div>

        </div>

    ';

            //Save user details in the database

                $name = "";

                $email = "";

                $id = 0;

                $update = false;

                if (isset($\_POST['save'])) {

                    $name = $\_POST['name'];

                    $email = $\_POST['email'];

                    mysqli\_query($db, "INSERT INTO registrations (email, name) VALUES ('$email', '$name')");

                    header('location: redirect.php');

                }

                } catch (Exception $e) {

                    // The user revoke the permission for this App. Therefore reset session token

                    unset($\_SESSION["auto"]);

                    unset($\_SESSION['token']);

                    header('Location: ' . filter\_var($google\_redirect\_url, FILTER\_SANITIZE\_URL));

                }

            }

            else // Sign up

            {

                $authUrl = $gClient->createAuthUrl();

                // Fast access or manual login button?

                if(isset($\_GET["auto"]))

                {

                }

                else

                {

                    echo ' <section id="home" class="video-section js-height-full">

                    <!-- <div class="overlay"></div> -->

                    <div class="home-text-wrapper relative container">

                        <div class="home-message">

                        <a class="login" href="'.$authUrl.'"><img src="google3.jpg"  width="220" height="60"/></a>

                            <p>Learning Management System</p>

                            <small>Edulogy is the ideal choice for your organization, your business and your online education system. Create your online course now with unlimited page templates, color options, and menu features.</small>

                            <div class="btn-wrapper">

                                <div class="text-center">

                                </div>

                            </div><!-- end row -->

                        </div>

                    </div>

                    <div class="slider-bottom">

                        <span>Explore <i class="fa fa-angle-down"></i></span>

                    </div>

                    </section>';

                            }

                    }

?>