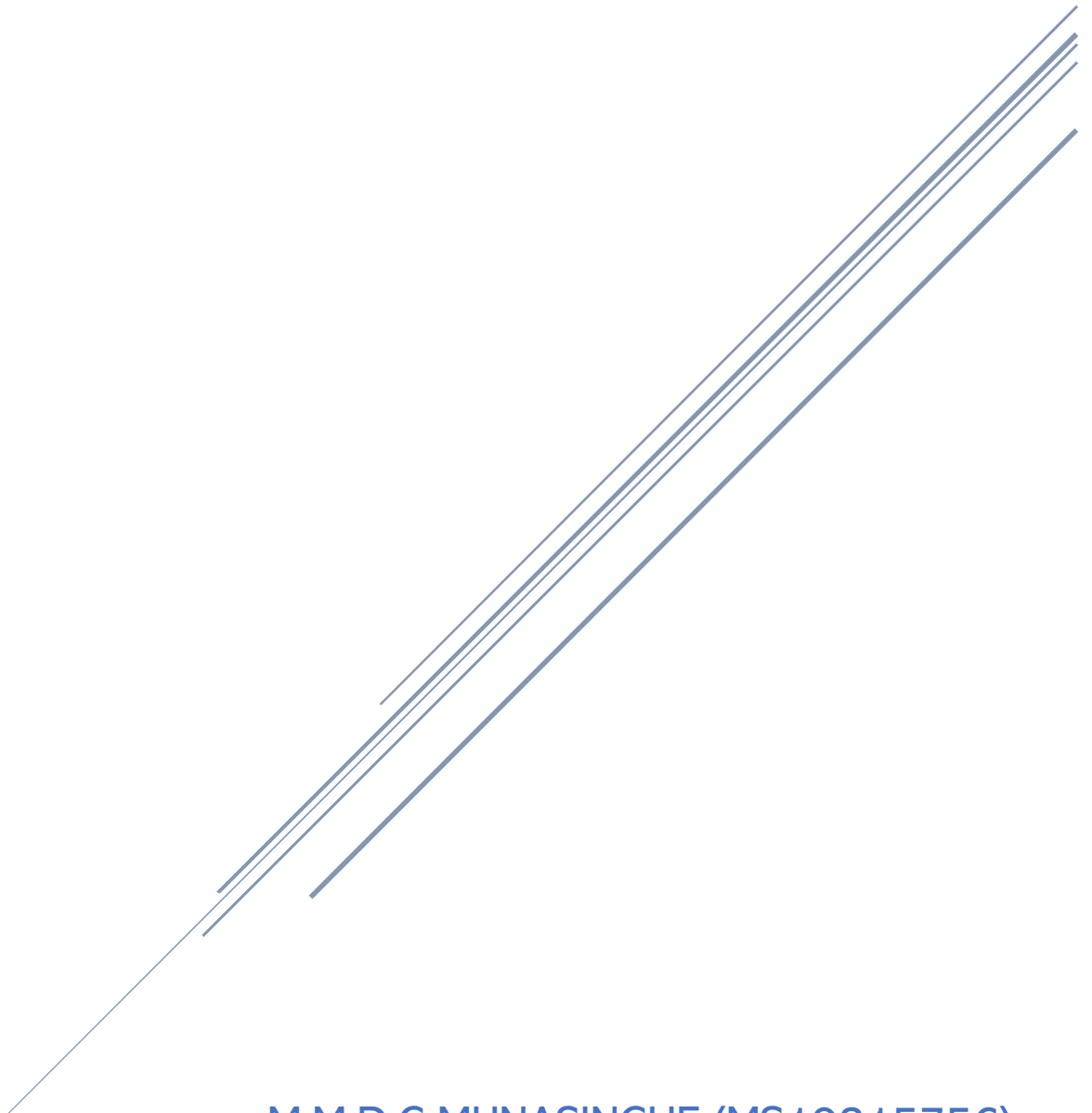


# OAuth AUTHORIZATION APPLICATION TEST

SOFTWARE SECURITY



M.M.D.C MUNASINGHE (MS19815756)  
B.G.M CHANDRASENA (MS19810874)

## Table of Contents

INTRODUCTION.....	2
OAuth Protocol Roles.....	2
Protocol flow .....	2
Process of getting Google API Credentials.....	3
Download Google Client Library for PHP .....	7
WEB APPLICATION DEVELOPMENT .....	8
APPENDIX .....	11
CONFIG.....	11
LOGIN.....	12
LOGOUT.....	16
MAIN .....	17
UPLOAD .....	21

## INTRODUCTION

“OAuth is an open-standard authorization protocol or framework that describes how unrelated servers and services can safely allow authenticated access to their assets without actually sharing the initial, related, single login credential. In authentication parlance, this is known as secure, third-party, user-agent, delegated authorization.” ( Source:- <https://www.csoonline.com/article/3216404/what-is-oauth-how-the-open-authorization-framework-works.html> )

### OAuth Protocol Roles

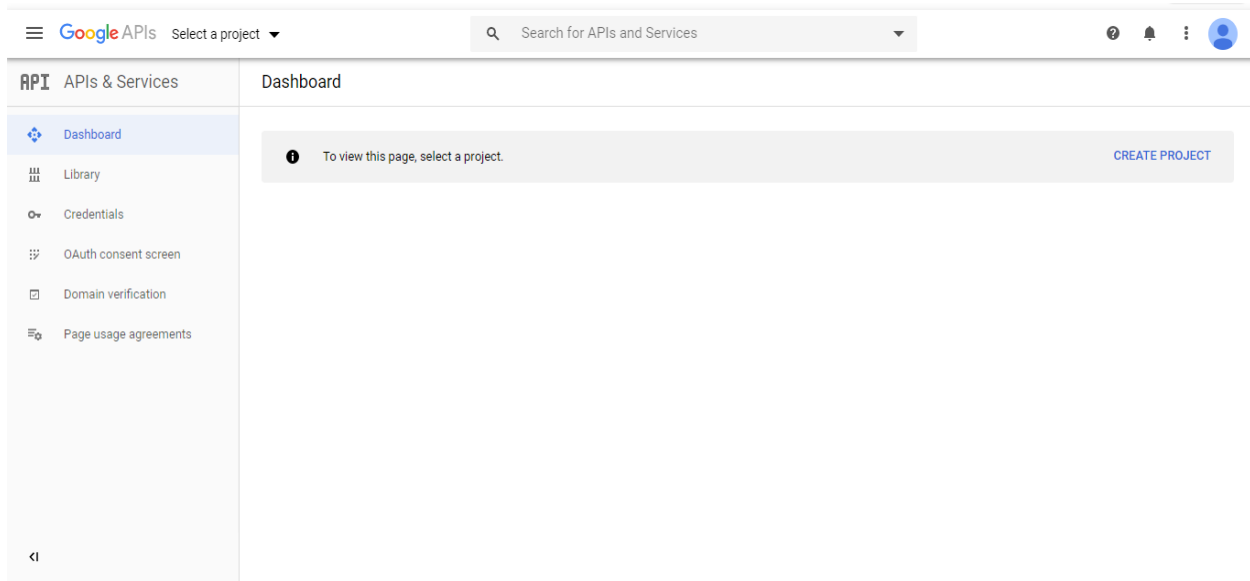
- 1) Resource Owner: Client-side software
- 2) Resource Server:
- 3) Client: Application
- 4) Authorization Server: The server that authenticates the Resource Owner, and issues Access Tokens after getting proper authorization

### Protocol flow

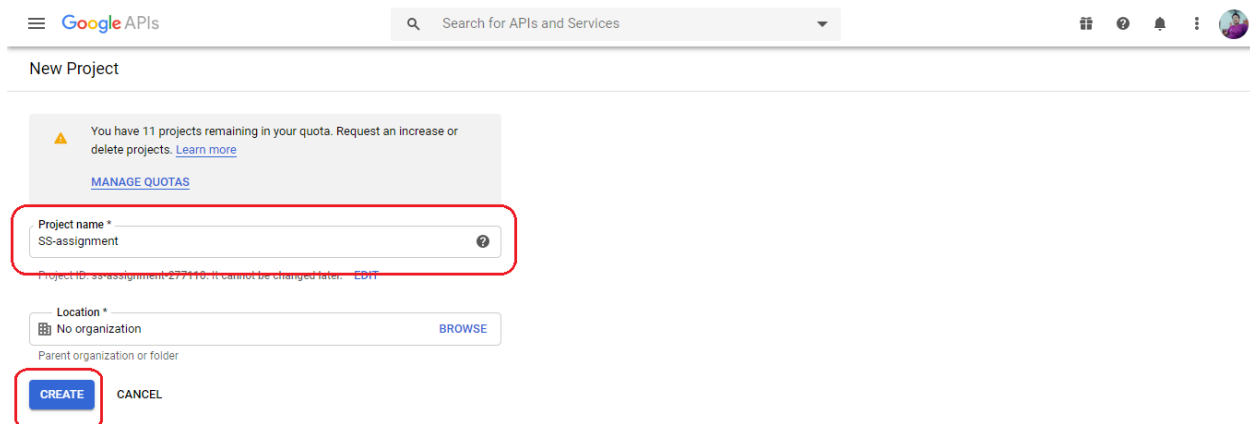


## Process of getting Google API Credentials.

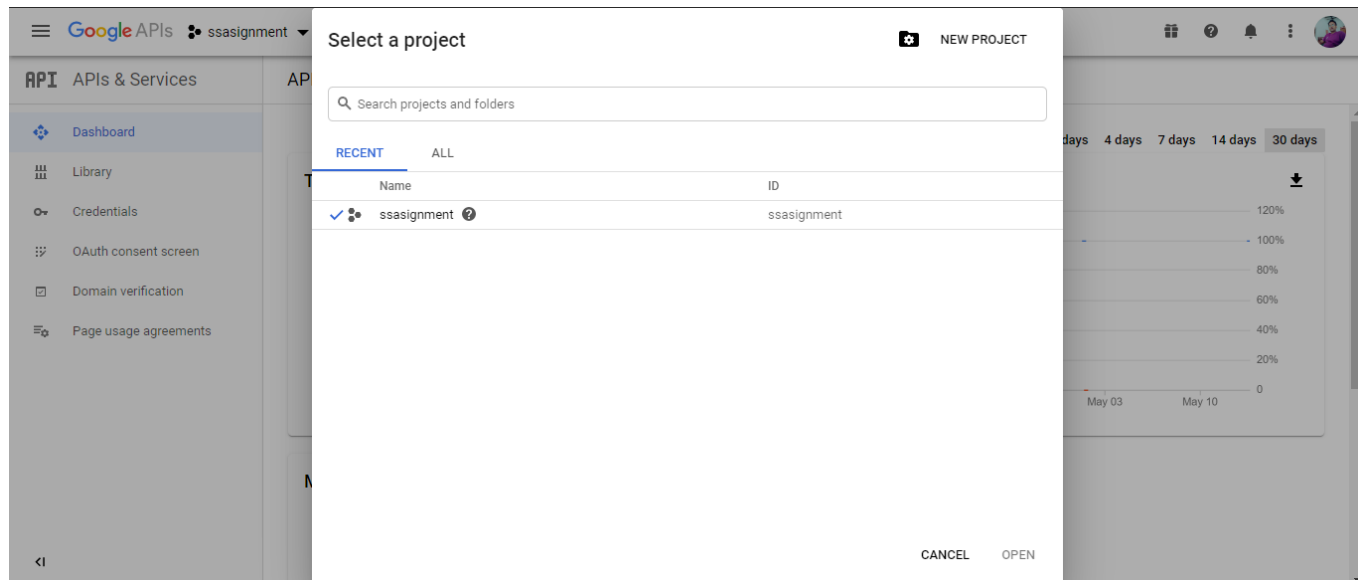
- 1) First, log on to Google API console. To navigate, used this <https://developer.google.com> URL.



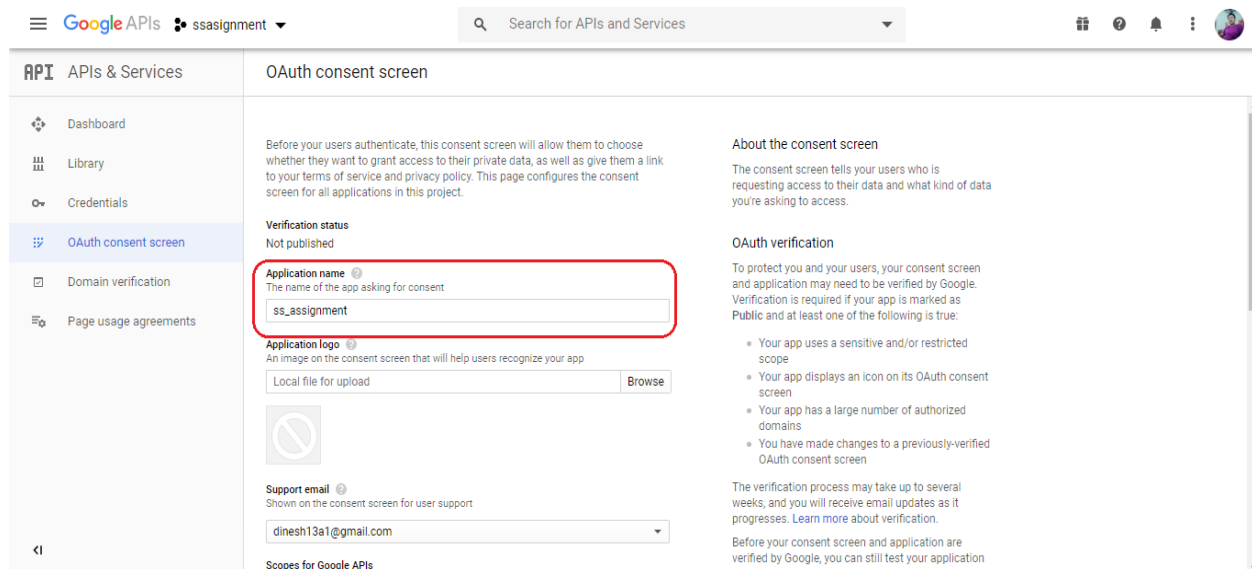
- 2) Then selected create a new project. Added the project name and click on “CREATE” button.



- 3) Then go to the home and select the project from project select box and select the project from that popup window.



- 4) select OAuth consent screen from the left-hand menu and define the application name and other related information and click on “OK”



Google APIs ssassignment Search for APIs and Services

### APIs & Services

- Dashboard
- Library
- Credentials
- OAuth consent screen**
- Domain verification
- Page usage agreements

#### OAuth consent screen

opened

[Add scope](#)

**Authorized domains** ⓘ  
To protect you and your users, Google only allows applications that authenticate using OAuth to use Authorized Domains. Your applications' links must be hosted on Authorized Domains. [Learn more](#)

Type in the domain and press Enter to add it

**Application Homepage link**  
Shown on the consent screen. Must be hosted on an Authorized Domain.

**Application Privacy Policy link**  
Shown on the consent screen. Must be hosted on an Authorized Domain.

**Application Terms of Service link** (Optional)  
Shown on the consent screen. Must be hosted on an Authorized Domain.

[Save](#) [Submit for verification](#) [Cancel](#)

Your current per minute token grant rate limit is 100 grants per minute. The per minute token grant rate resets every minute. Your current per day token grant rate limit is 10,000 grants per day. The per day token grant rate resets every day.

[Raise limit](#)

1h 6h 1d 7d 30d

No data for this time interval

- 5) after saving OAuth consent Screen in formation, click on “credentials” from the left-hand menu. In that window select the “Create Credential” button. on that drop-down menu, we have to select “OAuth Client ID”

Credentials - APIs & Services console.developers.google.com/apis/credentials?project=ssassignment&supportedpurview=project

Google APIs ssassignment Search for APIs and Services

### APIs & Services

- Dashboard
- Library
- Credentials**
- OAuth consent screen
- Domain verification
- Page usage agreements

#### Credentials

[+ CREATE CREDENTIALS](#) [DELETE](#)

Create credentials to access your APIs

**API Keys**

☐ Name  
No API keys to display

**OAuth 2.0 Client IDs**

☐ Name **Creation date** ↓ **Type** **Client ID**

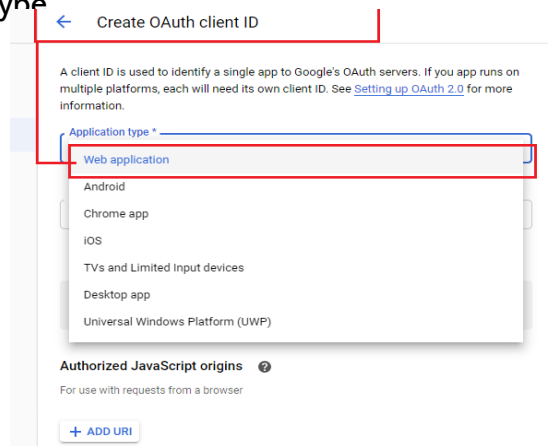
<input type="checkbox"/>	ss_assignment_drive	May 13, 2020	Web application	898854167982-j881...	<a href="#">Copy</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Download</a>
<input type="checkbox"/>	ss assignment	May 1, 2020	Web application	898854167982-tfff...	<a href="#">Copy</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Download</a>

**Service Accounts** [Manage service accounts](#)

☐ Email **Name** ↑ **Usage with all services (last 30 days)** ⓘ

No service accounts to display

- 6) after select on OAuth client ID, it will redirect to another window to select “Application Type”



← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If you app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information.

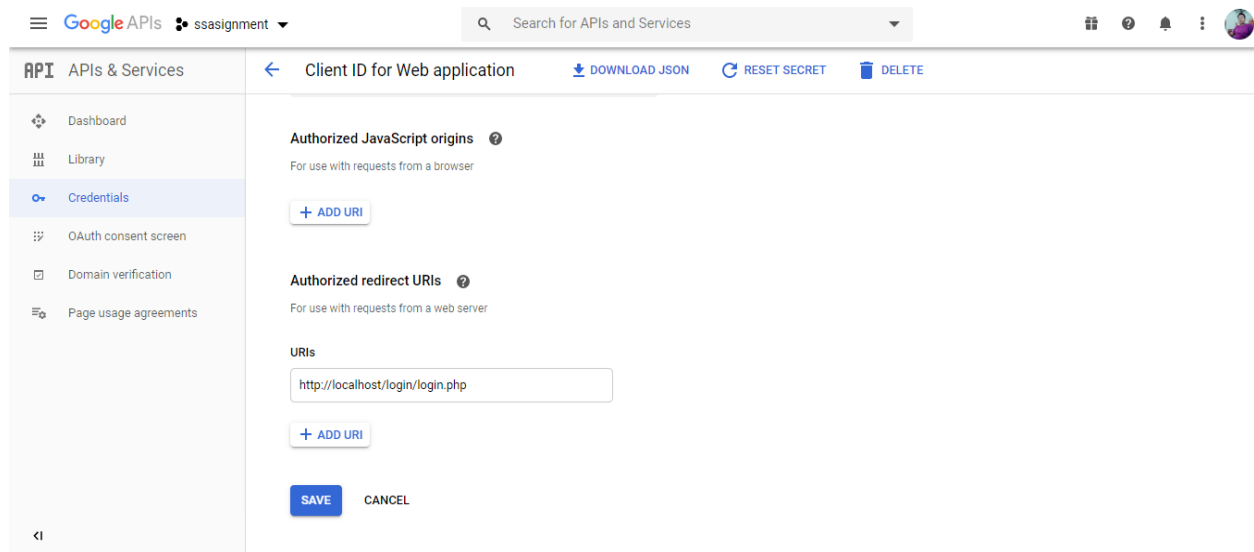
Application type \*

- Web application
- Android
- Chrome app
- iOS
- TVs and Limited Input devices
- Desktop app
- Universal Windows Platform (UWP)

Authorized JavaScript origins ⓘ  
For use with requests from a browser

+ ADD URI

- 7) Select the application type as a web application and add the URL of the web application. In our case it is <http://localhost/login/login.php>



Google APIs ssassignment

Search for APIs and Services

APIs & Services

← Client ID for Web application

DOWNLOAD JSON RESET SECRET DELETE

Authorized JavaScript origins ⓘ  
For use with requests from a browser

+ ADD URI

Authorized redirect URIs ⓘ  
For use with requests from a web server

URIs

http://localhost/login/login.php

+ ADD URI

SAVE CANCEL

Finally, click on the Save button. Once click on the save button it will provide the Client ID and the client secret key. There need to copy both keys for implementation.

## Download Google Client Library for PHP

After receiving google API credentials, We need to download the **Google Client library for PHP**. To do that we have to go command prompt type below composer command.

```
composer require google/apiclient:"^2.0"
```

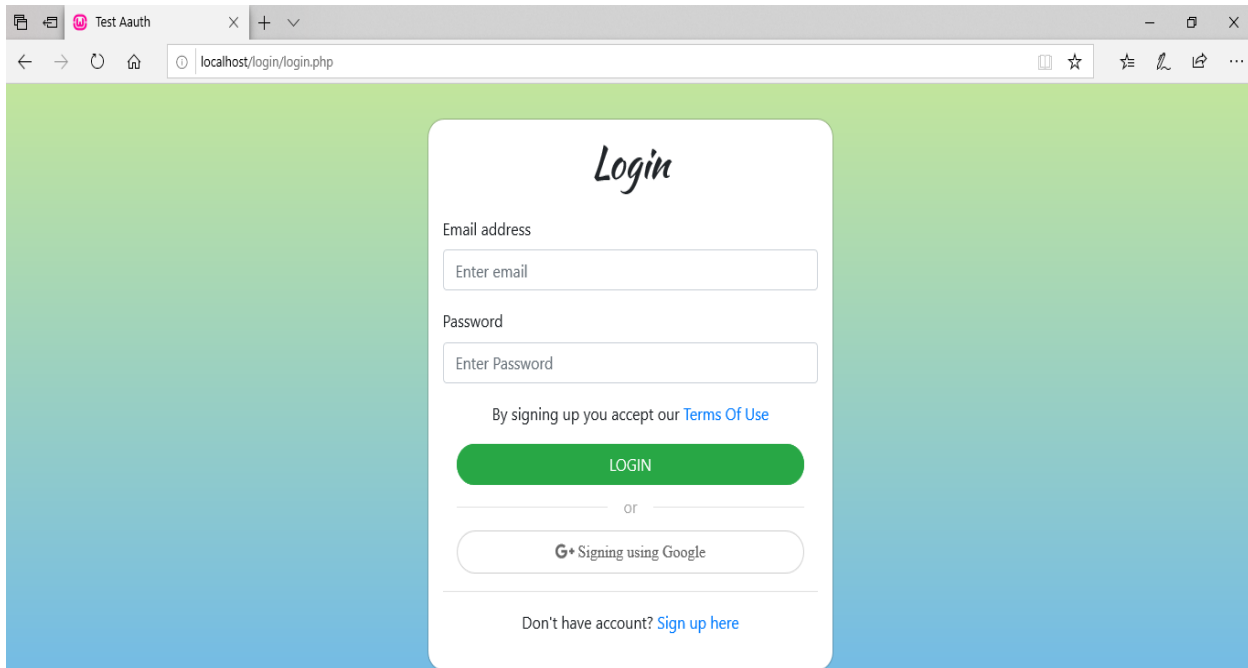
the above command will download the **Google Client Library for PHP** to our defined directory.



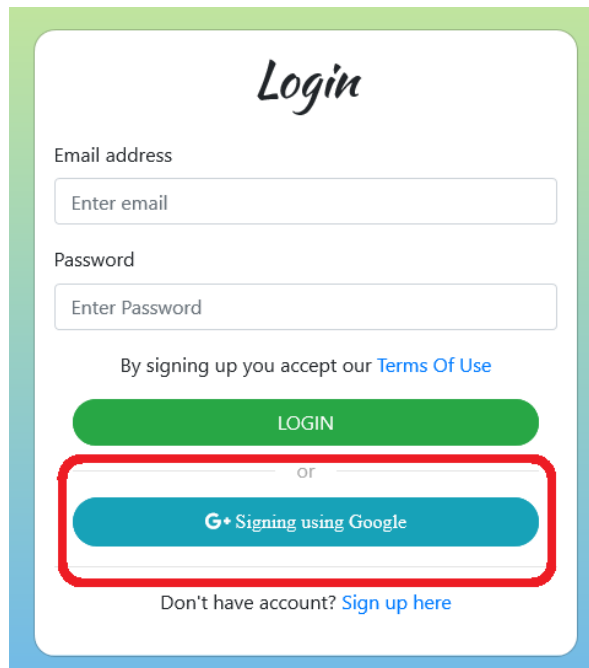
## WEB APPLICATION DEVELOPMENT

We developed the web application using PHP to test the OAuth authentication and apply the knowledge of how to use Google API Client Library for login using Google account with PHP.

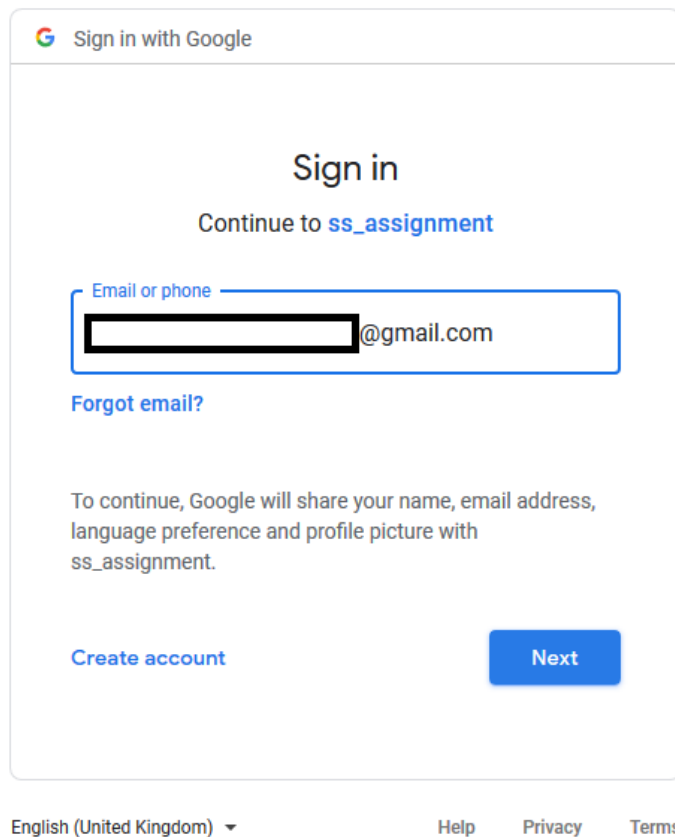
Below is the screenshot of the login page of the client-side application. We



There is an option to “Signing using Google”. That is the OAuth Authentication which we have implemented using google API.

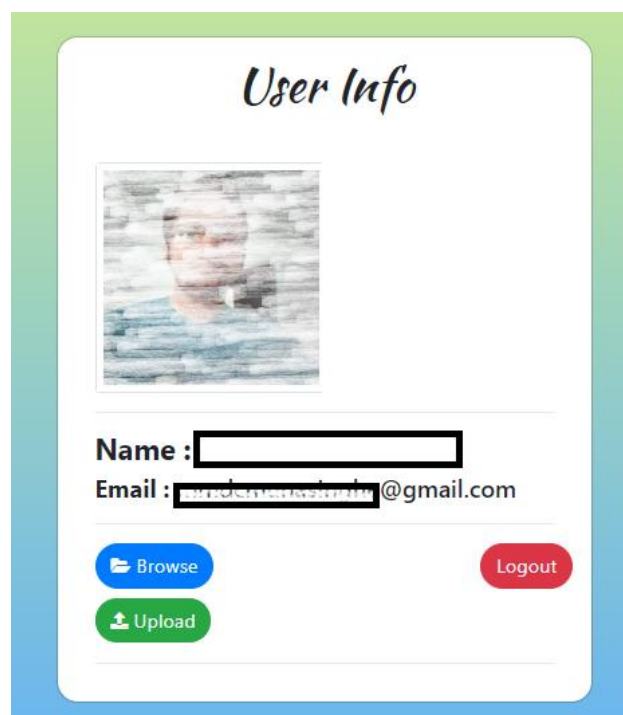


When providing google credentials it will automatically redirect to google and obtain the authentication from google.

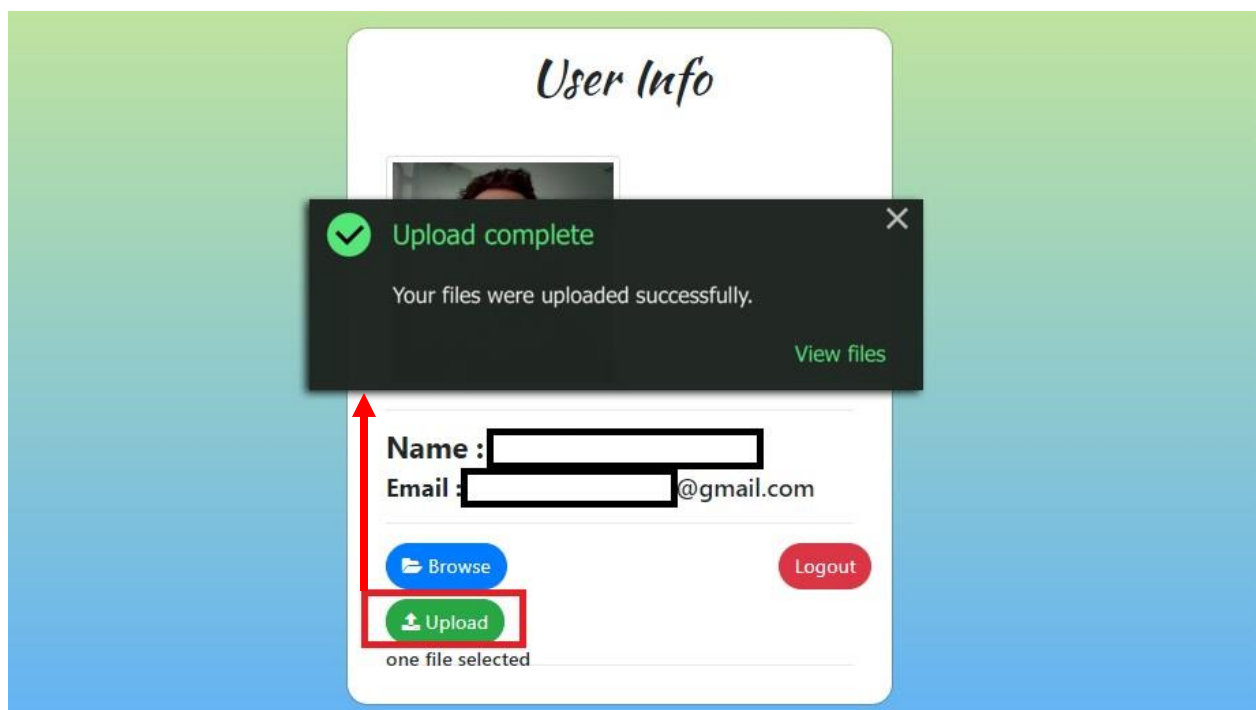
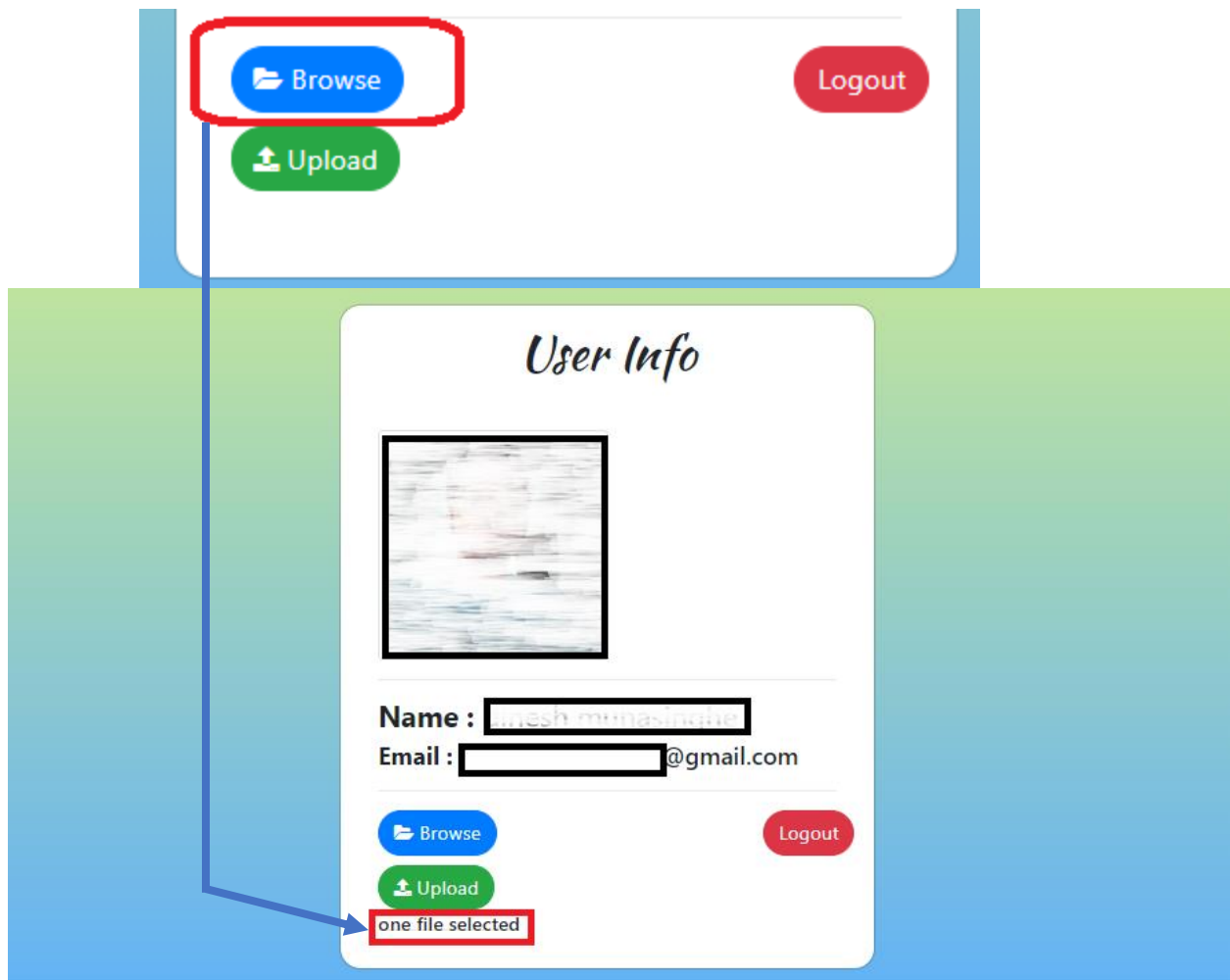


The image shows a Google Sign in interface. At the top, it says "Sign in with Google". Below that, the heading "Sign in" is centered, followed by "Continue to ss\_assignment". There is a text input field for "Email or phone" with a blue border, containing a redacted email address followed by "@gmail.com". Below the input field is a link "Forgot email?". A paragraph of text states: "To continue, Google will share your name, email address, language preference and profile picture with ss\_assignment." At the bottom left is a link "Create account", and at the bottom right is a blue button labeled "Next". The footer contains "English (United Kingdom)" with a dropdown arrow, and links for "Help", "Privacy", and "Terms".

After the authentication, this web application allows uploading files to the google drive



The image shows a "User Info" interface with a green and blue gradient border. At the top, the heading "User Info" is in a cursive font. Below it is a profile picture of a man. Under the picture, there are two labels: "Name :" followed by a redacted name in a black box, and "Email :" followed by a redacted email address in a black box, ending with "@gmail.com". At the bottom, there are three buttons: a blue "Browse" button with a folder icon, a green "Upload" button with an upload icon, and a red "Logout" button.



## APPENDIX

### CONFIG

```
<?php
//Import vnder autoloard.php file

require_once 'vendor/autoload.php';

//define new client class and assign to variable

$google_client = new Google_Client();

//set client ID to client variable using below method

$google_client->setClientId('898854167902-
tfffjoje4p6mtrsarpa14mmiaro2tsei.apps.googleusercontent.com');

// set client secret key to client variable using below method

$google_client->setClientSecret('nhztlT2hG6hEDpz6e9hu51OM');

//redirect to home page using below method

$google_client->setRedirectUri('http://localhost/login/login.php');

//define scope for access google API

$google_client->addScope('email');

$google_client->addScope('profile');

//start session

session_start();

?>
```

## LOGIN

```
<?php

//index.php

//Include Configuration File
include('config.php');

$login_button = "";

//This $_GET["code"] variable value received after user has login into their Google Account
redirect to PHP script then this variable value has been received
if(isset($_GET["code"]))
{
    //It will Attempt to exchange a code for an valid authentication token.
    $token = $google_auth_client->fetchAccessTokenWithAuthCode($_GET["code"]);

    //This condition will check there is any error occur during geting authentication token.
    If there is no any error occur then it will execute if block of code/
    if(!isset($token['error']))
    {
        //Set the access token used for requests
        $google_auth_client->setAccessToken($token['access_token']);

        //Store "access_token" value in $_SESSION variable for future use.
        $_SESSION['access_token'] = $token['access_token'];

        //Create Object of Google Service OAuth 2 class
        $google_service = new Google_Service_Oauth2($google_auth_client);

        //Get user profile data from google
        $data = $google_service->userinfo->get();

        //Below you can find Get profile data and store into $_SESSION variable
        if(!empty($data['given_name']))
        {
            $_SESSION['user_first_name'] = $data['given_name'];
        }

        if(!empty($data['family_name']))
        {
            $_SESSION['user_last_name'] = $data['family_name'];
        }
    }
}
```

```

    }

    if(!empty($data['email']))
    {
        $_SESSION['user_email_address'] = $data['email'];
    }

    if(!empty($data['gender']))
    {
        $_SESSION['user_gender'] = $data['gender'];
    }

    if(!empty($data['picture']))
    {
        $_SESSION['user_image'] = $data['picture'];
    }
}
}

```

//This is for check user has login into system by using Google account, if User not login into system then it will execute if block of code and make code for display Login link for Login using Google account.

```

if(!isset($_SESSION['access_token']))
{
    //Create a URL to obtain user authorization
    $login_button = '<a href="'. $google_auth_client->createAuthUrl()."></a>';
}

```

?>

<!DOCTYPE html>

<html>

<head>

<title> Login Page</title>

<link href="//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css"

rel="stylesheet" id="bootstrap-css">

<script src="//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js"></script>

<script src="//cdn.jsdelivr.net/npm/jquery/3.2.1/jquery.min.js"></script>

<!-- Include the above in your HEAD tag -->

<script

src="https://cdn.jsdelivr.net/jquery.validation/1.15.1/jquery.validate.min.js"></script>

<link href="https://fonts.googleapis.com/css?family=Kaushan+Script" rel="stylesheet">

```

<link href="https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-
awesome.min.css" rel="stylesheet" integrity="sha384-
wvfXpqpZZVQGK6TAh5PVIGOfQNHSoD2xbE+QkPxCAFINEevoEH3Sl0sibVcOQVnN"
crossorigin="anonymous">
<link rel="stylesheet" type="text/css" href="css/styles.css">

</head>

<body>
  <div class="container">
    <div class="row">
      <div class="col-md-5 mx-auto">
        <div id="first">
          <div class="myform form " >
            <div class="logo mb-3">
              <div class="col-md-12 text-center">
                <h1>Login</h1>
              </div>
            </div>
            <form action="" method="post">
              <div class="form-group">
                <label for="exampleInputEmail1">Email address</label>
                <input type="email" name="email" class="form-control" id="email"
aria-describedby="emailHelp" placeholder="Enter email">
              </div>
              <div class="form-group">
                <label for="exampleInputEmail1">Password</label>
                <input type="password" name="password" id="password"
class="form-control" aria-describedby="emailHelp" placeholder="Enter Password">
              </div>
              <div class="form-group">
                <p class="text-center">By signing up you accept our <a
href="#">Terms Of Use</a></p>
              </div>
              <div class="col-md-12 text-center ">
                <button type="submit" class=" btn btn-block mybtn btn-success tx-
tfm">Login</button>
              </div>
              <div class="col-md-12 ">
                <div class="login-or">
                  <hr class="hr-or">
                  <span class="span-or">or</span>
                </div>
              </div>
            </form>
          </div>
        </div>
      </div>
    </div>
  </div>

```

```

<div class="col-md-12 mb-3">
    <p class="text-center">
        <?php

            echo ' <a href="'. $google_auth_client->createAuthUrl().'" class="
google btn mybtn btn-outline-info "><i class="fa fa-google-plus" > Signing using Google
</i></a> ';

            // $login_button = ' <a href="'. $google_auth_client-
>createAuthUrl().'"></a>';

        ?>
        <?php

            if ($login_button == "")
            {

                header('Location: main.php');

            }
            else
            {
                echo ' <div align="center">'. $login_button . ' </div>';
            }

        ?>
    </p>
</div>

<hr>

<div class="form-group">
    <p class="text-center">Don't have account? <a href="#"
id="signup">Sign up here</a></p>
</div>
</form>

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

</html>

```



## LOGOUT

```
<?php
```

```
//logout.php
```

```
include('config.php');
```

```
//Reset OAuth access token  
$google_client->revokeToken();
```

```
//Destroy entire session data.  
session_destroy();
```

```
//redirect page to index.php  
header('location:login.php');
```

```
?>
```

## MAIN

```
<?php

//index.php

//Include Configuration File
include('config.php');

$login_button = "";

//This $_GET["code"] variable value received after user has login into their Google Account
redirect to PHP script then this variable value has been received
if(isset($_GET["code"]))
{
    //It will Attempt to exchange a code for an valid authentication token.
    $token = $google_auth_client->fetchAccessTokenWithAuthCode($_GET["code"]);

    //This condition will check there is any error occur during geting authentication token. If
    there is no any error occur then it will execute if block of code/
    if(!isset($token['error']))
    {
        //Set the access token used for requests
        $google_auth_client->setAccessToken($token['access_token']);

        //Store "access_token" value in $_SESSION variable for future use.
        $_SESSION['access_token'] = $token['access_token'];

        //Create Object of Google Service OAuth 2 class
        $google_service = new Google_Service_Oauth2($google_auth_client);

        //Get user profile data from google
        $data = $google_service->userinfo->get();

        //Below you can find Get profile data and store into $_SESSION variable
        if(!empty($data['given_name']))
        {
            $_SESSION['user_first_name'] = $data['given_name'];
        }

        if(!empty($data['family_name']))
        {
            $_SESSION['user_last_name'] = $data['family_name'];
        }
    }
}
```

```

}

if(!empty($data['email']))
{
    $_SESSION['user_email_address'] = $data['email'];
}

if(!empty($data['gender']))
{
    $_SESSION['user_gender'] = $data['gender'];
}

if(!empty($data['picture']))
{
    $_SESSION['user_image'] = $data['picture'];
}
}
}

//This is for check user has login into system by using Google account, if User not login
into system then it will execute if block of code and make code for display Login link for
Login using Google account.
if(!isset($_SESSION['access_token']))
{
    //Create a URL to obtain user authorization
    $login_button = '<a href="'. $google_auth_client->createAuthUrl()."></a>';
}

?>

<!DOCTYPE html>
<html>
<head>
    <title> User Information</title>

    <link href="//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css"
    rel="stylesheet" id="bootstrap-css">
    <script src="//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js"></script>
    <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
    <!-- Include the above in your HEAD tag -->

    <script
    src="https://cdn.jsdelivr.net/jquery.validation/1.15.1/jquery.validate.min.js"></script>
    <link href="https://fonts.googleapis.com/css?family=Kaushan+Script" rel="stylesheet">

```

```

<link href="https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-
awesome.min.css" rel="stylesheet" integrity="sha384-
wvXpqpZZVQGK6TAh5PVIGOfQNHSoD2xbE+QkPxCAFINEevoEH3Sl0sibVcOQVnN"
crossorigin="anonymous">
<link rel="stylesheet" type="text/css" href="css/styles.css">

</head>

<body>
  <div class="container">
    <div class="row">
      <div class="col-md-5 mx-auto">
        <div id="first">
          <div class="myform form " id="login_form">
            <div class="logo mb-3">
              <div class="col-md-12 text-center">
                <h1>User Info</h1>
              </div>
            </div>
            <form action="" method="post" name="login">

              <div class="col-md-12 mb-3">
                <p class="text-center">

                  <?php
                    if ($login_button == ")
                    {
                      echo '<div class= " tooltip">User Informations</div><div
class="panel-body">';
                      echo '';
                      echo '<hr>';
                      echo '<h4><b>Name :</b> '.$_SESSION['user_first_name'].'
'.$_SESSION['user_last_name'].'</h4>';
                      echo '<h5><b>Email :</b>
'.$_SESSION['user_email_address'].'</h5>';
                      echo '<hr>';
                      echo' <div>
                        <form method="post" enctype="multipart/form-data">
                        <div class="row" >
                          <div class="col-md-6">
                            <div class="form-group" style="height:0px;padding:
0;margin: 0">

                              <div class="image-upload pull-left">

```

```

        <label for="image_file">
            <span class="btn btn-primary mybtn" ><i class="fa
fa-folder-open"></i>&nbsp; Browse</span>

        </label>
        <input type="file" name="file" id="image_file"
style="display: none;" />
        <button type="submit" name="upload_button"
id="upload_button" class="btn btn-success mybtn"><i class="fa fa-upload"></i>&nbsp;
Upload</button>

    </div>
</div>
</form>
</div>' ;

        echo '<h5><button class="btn btn-danger mybtn"><a
href="logout.php" class="text-light">Logout </a></h5></div>';

    }
    else
    {
        echo '<div align="center" >'. $login_button . '</div>';
    }
?>
<hr>
<!-- <button class="btn btn-danger mybtn"><a
href="upload.php" class="text-light">next </a> -->
</p>
</div>
</form>
</div>
</div>
</div>
</body>
</html>

```

## UPLOAD

```
<!DOCTYPE html>
<html>
<head>
  <title>Upload Files</title>

  <link href="//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css"
rel="stylesheet" id="bootstrap-css">
  <script src="//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js"></script>
  <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
  <!-- Include the above in your HEAD tag ----->

  <script
src="https://cdn.jsdelivr.net/jquery.validation/1.15.1/jquery.validate.min.js"></script>
  <link href="https://fonts.googleapis.com/css?family=Kaushan+Script" rel="stylesheet">
  <link href="https://stackpath.bootstrapcdn.com/font-awesome/4.7.0/css/font-
awesome.min.css" rel="stylesheet" integrity="sha384-
wvfXpqpZZVQGK6TAh5PVIGfQNHSoD2xbE+QkPxCafINEevoEH3Sl0sibVcOQVnN"
crossorigin="anonymous">
  <link rel="stylesheet" type="text/css" href="css/styles.css">

</head>

<body>
  <div class="container">
    <div class="row">
      <div class="col-md-5 mx-auto">
        <div id="first">
          <div class="myform form " id="login_form">
            <div class="logo mb-3">
              <div class="col-md-12 text-center">
                <h1>File Upload</h1>
              </div>
            </div>
          </div>
          <div>
            <form method="post" enctype="multipart/form-data">
              <div class="row" >
                <div class="col-md-6">
                  <div class="form-group" style="height:Opx;padding: 0;margin: 0">
                    <div class="image-upload pull-left">
                      <label for="image_file">
                        <span class="btn btn-primary mybtn" ><i class="fa fa-folder-
open"></i>&nbsp; Browse</span>
```

```

        </label>
        <input type="file" name="file" id="image_file" style="display:
none;" />
        <button type="submit" name="upload_button"
id="upload_button" class="btn btn-success mybtn"><i class="fa fa-upload"></i>&nbsp;
Upload</button>
    </div>
</div>
</form>
</div>
<br>
<hr>
<div class="container ">
    <form action="#" method="post" enctype="multipart/form-data">
        Type Folder Name:<input type="text" name="foldername" /><br/><br/>
        Select Folder to Upload: <input type="file" name="files[]" id="files"
multiple directory="" moxdirectory="" /><br/><br/>
        <input type="Submit" value="Upload" name="upload" />
    </form>
</div>

</div>
</div>
</div>
</div>
</body>
</html>
<?php
if(isset($_POST['upload']))
{
    if($_POST['foldername'] != "")
    {
        $foldername=$_POST['foldername'];
        if(!is_dir($foldername))
            mkdir($foldername);
        foreach($_FILES['files']['name'] as $i => $name)
        {
            if(!is_dir($name))
            {
                mkdir($foldername."/".$name);
                if(strlen($_FILES['files']['name'][$i]) > 1)
                {
                    move_uploaded_file($_FILES['files']['tmp_name'][$i],$foldername."/".$name);
                }
            }
        }
    }
}

```

```
}
else
{
    if(strlen($_FILES['files']['name'][$i]) > 1)
    {
        move_uploaded_file($_FILES['files']['tmp_name'][$i], $foldername."/".$name);
    }
}
}
echo "Folder is successfully uploaded";
}
else
    echo "Upload folder name is empty";
}
?>
```