Appendix E

Core Functionality

Login

First, we insert users and data into the users table, the structure of which was designed in the interim report.

+ Options

	id	username	password	email	total
Edit Copy Delete	4	me	f30aa7a662c728b7407c54ae6bfd27d1	me@me.com	32
Edit Copy Delete	5	test	cc03e747a6afbbcbf8be7668acfebee5	test@test.com	0
Edit Copy Delete	6	test1	cc03e747a6afbbcbf8be7668acfebee5	test1@test.com	0
Edit Copy Delete	7	test2	cc03e747a6afbbcbf8be7668acfebee5	test2@test.com	37
Edit Copy Delete	8	test3	cc03e747a6afbbcbf8be7668acfebee5	test3@test.com	0
Edit Copy Delete	9	test4	cc03e747a6afbbcbf8be7668acfebee5	test4@test.com	0
Edit Copy Delete	10	test5	cc03e747a6afbbcbf8be7668acfebee5	test5@test.com	0
Edit Copy Delete	11	test6	cc03e747a6afbbcbf8be7668acfebee5	test6@test.com	0
Edit Copy Delete	12	test7	cc03e747a6afbbcbf8be7668acfebee5	test7@test.com	0
Edit Copy Delete	13	test8	cc03e747a6afbbcbf8be7668acfebee5	test8@test.com	0
Edit Copy Delete	14	test9	cc03e747a6afbbcbf8be7668acfebee5	test9@test.com	0
Edit Copy Delete	15	test10	cc03e747a6afbbcbf8be7668acfebee5	test10@test.com	0
Edit Copy Delete	16	davedave	587a56c91123a44fe2099d7f5f415919	d@d.com	576

For the login box in the header, we first need to be able to check if a user is logged in. A simple way to do this in PHP is to set a session variable. In this case the variable stores the user's username. So we start the session and then check if the session variable has been set.

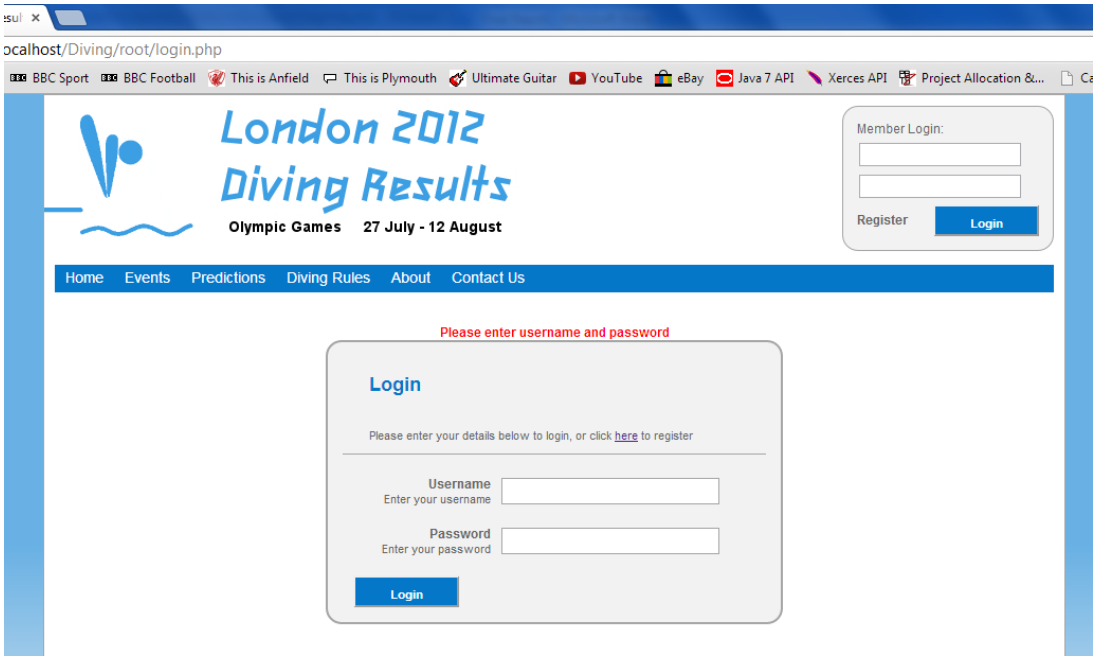
```
session_start();
if ($_SESSION['username']){
      //show user info}
Else{
      //Show login form}
```

To show the user information, we connect to the database and retrieve the information for the username stored in the session variable.

```
SELECT total FROM users WHERE username = '".$_SESSION['username']."'
```

If the form is shown, then the user enters their information and submits it. On submit, we POST and process their credentials using the login.php script.

When using a PHP script for a POST form, the form will navigate to that PHP file in the browser. This is where any errors will be reported and users will have a second chance to log in. Thus, this page needs to be a full page with the same template to fit in with the rest of the website. Because the login form is contained in the header of the website, we need to display a second, larger login form on this page where errors are reported and a second chance to login is displayed. So, instead of simply processing the information, we need to implement this new page that was not originally scoped for. This form is implemented similarly to the register and contact forms.




```
If session
      Print already logged in
End If
Else
      username = POST data
      password = POST data
      If ($username && $password){
            connect to database
            SELECT * FROM users WHERE username= POST username
            If number of rows != 0
                  Get DB username
                  Get DB password
                  If (username== DB username&& md5(password)==DB password)
                        session_start();
                        $_SESSION['username'] = username;
                        If (http_referer = login or register)
                              Redirect index
                        End If
                        Else
                              Redirect previous page
                        End Else
                  End If
                  Else
                        Print incorrect password
                  End Else
            End If
            Else
                  Print user does not exist
            End Else
      End If
      Else
            Print no username and password entered
      End Else
End Else
```

First, we need to check the user is not logged in already. Although this page cannot be navigated to on the site, it could be typed into a browser by an already logged in user. The login script gets the username and password from the POST data, we strip any tags for security purposes and convert the username to lower case. The username will be stored in lower case as this will help to avoid any possible issues with differing cases when matching records in the database. If the username and password are blank, we know they were not entered so report the error. Else we connect to the database and select the user that was entered. If the query returns zero rows, we know that the user doesn't exist and report the error. Otherwise we compare the password entered to the password in the database. For security purposes, we store the MD5 value of the password rather than the actual string, so we need to use an MD5 function on the entered password. If this is unsuccessful we know the password is incorrect and report the error, otherwise we now begin the session with the username as the session variable.

Because the login page is displayed regardless of whether the process was successful or not, if the login is successful we need to instead redirect the user back to the page they came from. So for example, if a user clicks the events page, then logs in from the header, they are then logged in but instantly returned back to the events page. There are two exceptions to this, if the user came from the login page (i.e. they had some error then logged in again) or the register page then we don't want to return them to these pages as they are now irrelevant to a logged in user. So in this case the user is returned back to the index page.

Logout

When a user clicks to logout (the link in the login box in the header) we simply destroy the session and return the user to the page they were on previously.

```
session_destroy();
header("Location: ".$_SERVER['HTTP_REFERER']);
```

Register

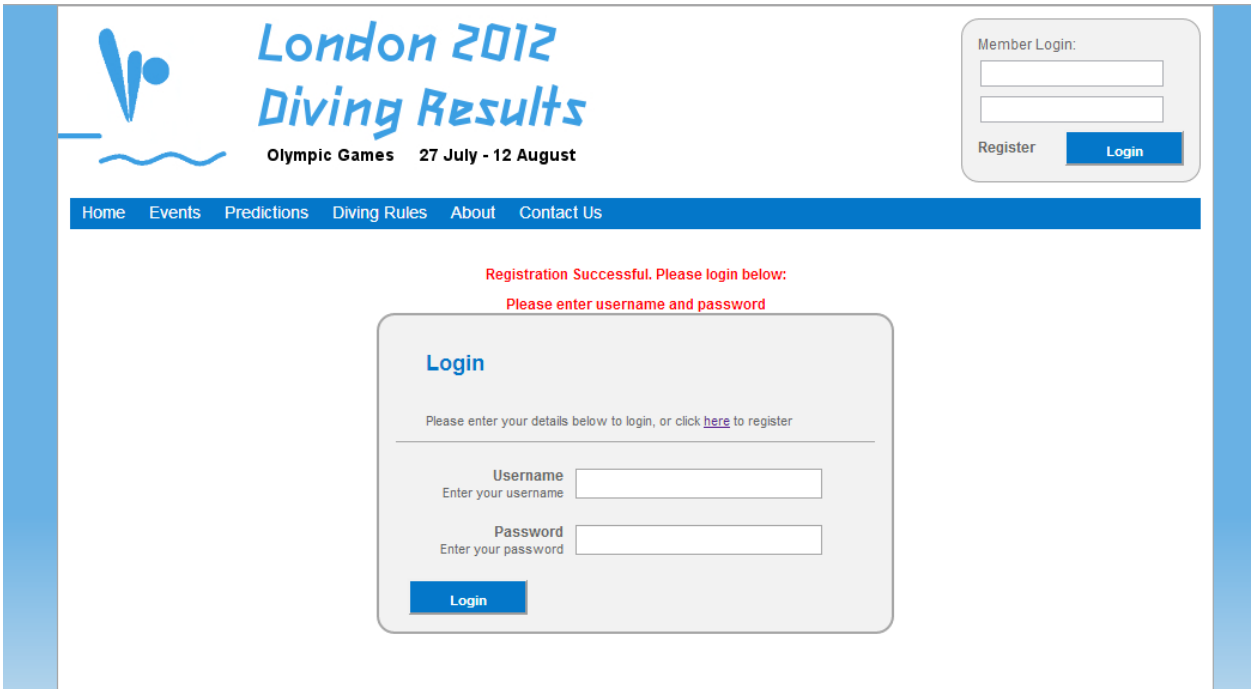
```
If Session
	cant register when logged in
End If
Else
	submit = POST submit
	username = lower(POST username)
	email = POST email
	confirmemail = POST confirmemail
	password = POST password
	confirmpassword = POST confirmpassword

	If(submit)
		If(password==confirmpassword)
			If(email==confirmemail)
				If(email format)
					If(username>25)
						username too long
					End If
					Else
						If(password>25 || password<6)
							password length wrong
						End If
						Else
							connect to DB
					SELECT username FROM users WHERE username = username
```

```
                                        If(count >0)
                                                username in use
                                        End If
                                        Else
                                SELECT username FROM users WHERE email ='$email'");
                                        If(count >0)
                                                email in use
                                        End If
                                        Else
                                                md5($password)
                                INSERT INTO users (id, username, password, email) VALUES
                                (DEFAULT,'username','password','email')
                                                Redirect loginreg
                                        End Else
                                End Else
                                End If
                                Else
                                        not valid email format
                                End Else
                        End If
                        Else
                                emails dont match
                        End Else
                End If
                Else
                        passwords dont match
                End Else
        End If
End Else
```

The register page is a self processing form, i.e. the register script is contained within the page itself. So to process the contents of the form, we first check if the submit button has been pressed. We then need to go through several error checking processes, and if an error is found output the error to the user.

- Check the password and the password confirmation match
- Check the email and email confirmation match
- Check the email address is a valid email format
- Check the username does not exceed 25 characters (so that excessively long usernames do not have to be handled by the database)
- Check the password is between 6 and 25 characters
- Check the desired username does not already exist in the database
- Check the entered email address is not already registered to a user

If all of these error checks are passed then the form information is inserted into the database to create the new user. We use an MD5 function on the password so that we only store an MD5 value rather than the actual string for security purposes. After this the user needs to be informed of their successful registration and redirected to the login form. However, the problem here is that if the user is directed to login.php then we will instantly be returned with errors as the user will not have entered anything into this form, and there is no way to print out a success message. So to get past this problem a new page was implemented, which displays the same login form but shows the registration success message and uses the login.php script to log the user in.



Contact

Like the register form, the contact form is also a self processing form. It gets the post data and strips it of tags. If submit is pressed, and the fields are not blank then the PHP mail function is called to send the email, else the user is asked to fill out all fields of the form. It is worth nothing that this implementation currently doesn't work because the server being used has not been configured as mail server. However, as soon as this server configuration is changed then the mail function will work.

```
$submit = $_POST['submit'];
$email = (strip_tags($_POST['email']));
$subject = strip_tags($_POST['subject']);
$message = strip_tags($_POST['message']);
$fullname = strip_tags($_POST['fullname']);

if ($submit && $email!="" && $subject!="" && $message!="" && $fullname!=""
){
      mail("me@gmail.com", $subject,
      $message, "From: " .$fullname." ".$email);
      echo "<h4 id=\"error\">Your message was sent. Thank you for using our
mail form</h4>";
}
else{
      echo "<h4 id=\"error\">Please complete all fields to send your
message.</h4>";
}
```