**Login.php**

if (check\_login($\_POST['username'], $\_POST['password'])) {

// login correct

$\_SESSION['username'] = $\_POST['username'];

if (isset($\_POST['remember\_me'])) {

// we hash the password because we \*\*NEVER\*\* store it in plain text anywhere

// so when we would like to check if the cookie value is correct, we will not

// be able to do so if the hash in the cookie was done from the plaintext

// password.

$value = sprintf('%s:%s', $\_POST['username'], md5($\_POST['username'].hash\_password($\_POST['password'])));

setcookie('rememberme', $value);

}

redirect('/your/home/page.php'); // view Post/Redirect/Get design pattern

} else {

// login incorrect, show error message and whatever...

}

if (isset($\_SESSION['username'])) {

// $\_SESSION['username'] is logged in, proceed as you wish

} else if (isset($\_COOKIE['rememberme'])) {

// this user has checked the remember me feature some time ago in a previous login.

// let's check if it is valid.

list($username, $hash) = explode(':', $\_COOKIE['rememberme']);

// we need to get the password hash stored for this user (remember you \*\*NEVER\*\* store passwords in plain text

$pwd\_hash = obtain\_password\_hash\_from\_username($username);

if ($hash == sprintf('%s:%s', $username, md5($username.$pwd\_hash))) {

// yeah, the user remembered is correct. We'll save it to the session to not do this shit again

$\_SESSION['username'] = $username;

} else {

// the cookie value is not correct so maybe an attacker is trying to fool us,

// or the user changed his password. Whatever it is, we remove the cookie

// because it's no longer valid

setcookie('rememberme', '', time() - 3600);

}

} else {

// this user is neither logged in nor "remembered"

}

**friend\_system.php**

**<?php** include\_once("../php\_includes/check\_login\_status.php"); if($user\_ok != true || $log\_username == "") { exit(); } **?>**

**<?php** if (isset($\_POST['type']) && isset($\_POST['user'])){ $user = preg\_replace('#[^a-z0-9]#i', '', $\_POST['user']); $sql = "SELECT COUNT(id) FROM users WHERE username='$user' AND activated='1' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); $exist\_count = mysqli\_fetch\_row($query); if($exist\_count[0] < 1){ mysqli\_close($db\_conx); echo "$user does not exist."; exit(); } if($\_POST['type'] == "friend"){ $sql = "SELECT COUNT(id) FROM friends WHERE user1='$user' AND accepted='1' OR user2='$user' AND accepted='1'"; $query = mysqli\_query($db\_conx, $sql); $friend\_count = mysqli\_fetch\_row($query); $sql = "SELECT COUNT(id) FROM blockedusers WHERE blocker='$user' AND blockee='$log\_username' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); $blockcount1 = mysqli\_fetch\_row($query); $sql = "SELECT COUNT(id) FROM blockedusers WHERE blocker='$log\_username' AND blockee='$user' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); $blockcount2 = mysqli\_fetch\_row($query); $sql = "SELECT COUNT(id) FROM friends WHERE user1='$log\_username' AND user2='$user' AND accepted='1' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); $row\_count1 = mysqli\_fetch\_row($query); $sql = "SELECT COUNT(id) FROM friends WHERE user1='$user' AND user2='$log\_username' AND accepted='1' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); $row\_count2 = mysqli\_fetch\_row($query); $sql = "SELECT COUNT(id) FROM friends WHERE user1='$log\_username' AND user2='$user' AND accepted='0' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); $row\_count3 = mysqli\_fetch\_row($query); $sql = "SELECT COUNT(id) FROM friends WHERE user1='$user' AND user2='$log\_username' AND accepted='0' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); $row\_count4 = mysqli\_fetch\_row($query); if($friend\_count[0] > 99){ mysqli\_close($db\_conx); echo "$user currently has the maximum number of friends, and cannot accept more."; exit(); } else if($blockcount1[0] > 0){ mysqli\_close($db\_conx); echo "$user has you blocked, we cannot proceed."; exit(); } else if($blockcount2[0] > 0){ mysqli\_close($db\_conx); echo "You must first unblock $user in order to friend with them."; exit(); } else if ($row\_count1[0] > 0 || $row\_count2[0] > 0) { mysqli\_close($db\_conx); echo "You are already friends with $user."; exit(); } else if ($row\_count3[0] > 0) { mysqli\_close($db\_conx); echo "You have a pending friend request already sent to $user."; exit(); } else if ($row\_count4[0] > 0) { mysqli\_close($db\_conx); echo "$user has requested to friend with you first. Check your friend requests."; exit(); } else { $sql = "INSERT INTO friends(user1, user2, datemade) VALUES('$log\_username','$user',now())"; $query = mysqli\_query($db\_conx, $sql); mysqli\_close($db\_conx); echo "friend\_request\_sent"; exit(); } } else if($\_POST['type'] == "unfriend"){ $sql = "SELECT COUNT(id) FROM friends WHERE user1='$log\_username' AND user2='$user' AND accepted='1' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); $row\_count1 = mysqli\_fetch\_row($query); $sql = "SELECT COUNT(id) FROM friends WHERE user1='$user' AND user2='$log\_username' AND accepted='1' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); $row\_count2 = mysqli\_fetch\_row($query); if ($row\_count1[0] > 0) { $sql = "DELETE FROM friends WHERE user1='$log\_username' AND user2='$user' AND accepted='1' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); mysqli\_close($db\_conx); echo "unfriend\_ok"; exit(); } else if ($row\_count2[0] > 0) { $sql = "DELETE FROM friends WHERE user1='$user' AND user2='$log\_username' AND accepted='1' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); mysqli\_close($db\_conx); echo "unfriend\_ok"; exit(); } else { mysqli\_close($db\_conx); echo "No friendship could be found between your account and $user, therefore we cannot unfriend you."; exit(); } } } **?><?php** if (isset($\_POST['action']) && isset($\_POST['reqid']) && isset($\_POST['user1'])){ $reqid = preg\_replace('#[^0-9]#', '', $\_POST['reqid']); $user = preg\_replace('#[^a-z0-9]#i', '', $\_POST['user1']); $sql = "SELECT COUNT(id) FROM users WHERE username='$user' AND activated='1' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); $exist\_count = mysqli\_fetch\_row($query); if($exist\_count[0] < 1){ mysqli\_close($db\_conx); echo "$user does not exist."; exit(); } if($\_POST['action'] == "accept"){ $sql = "SELECT COUNT(id) FROM friends WHERE user1='$log\_username' AND user2='$user' AND accepted='1' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); $row\_count1 = mysqli\_fetch\_row($query); $sql = "SELECT COUNT(id) FROM friends WHERE user1='$user' AND user2='$log\_username' AND accepted='1' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); $row\_count2 = mysqli\_fetch\_row($query); if ($row\_count1[0] > 0 || $row\_count2[0] > 0) { mysqli\_close($db\_conx); echo "You are already friends with $user."; exit(); } else { $sql = "UPDATE friends SET accepted='1' WHERE id='$reqid' AND user1='$user' AND user2='$log\_username' LIMIT 1"; $query = mysqli\_query($db\_conx, $sql); mysqli\_close($db\_conx); echo "accept\_ok"; exit(); } } else if($\_POST['action'] == "reject"){ mysqli\_query($db\_conx, "DELETE FROM friends WHERE id='$reqid' AND user1='$user' AND user2='$log\_username' AND accepted='0' LIMIT 1"); mysqli\_close($db\_conx); echo "reject\_ok"; exit(); } } **?>**