```php
<?php
session_start();

include ("config.php");
include ("db.php");
include ("function.php");
if (isset($_GET['aktie'])) {
    $aktie = $_GET['aktie'];
}
else {
    $aktie = "";
}

// Controleren of gebruiker admin-rechten heeft
// Indien het het wijzigen van het eigen profiel betreft hoeft hij geen admin-rechten te hebben
if (!$aktie == "editprof") {
    check_admin();
}

// Controleren of cookie aanwezig is. Anders login-scherm displayen
check_cookies();

include ("header.php");

?>
<div id="main">
    <h1>Usermanagement</h1>

<?php
//This code runs if the form has been submitted
if (isset($_POST['cancel'])) {
    header("location: edit_users.php?aktie=disp");
}

if (isset($_POST['delete'])) {
    $deluser = $_POST['username'];
    $sql_deluser = mysqli_query($dbconn, "DELETE FROM users WHERE username = '$deluser'");
    writeLogRecord("edit_users","User ".$deluser." is succesvol verwijderd.");
    header("location: edit_users.php?aktie=disp");
}

if (isset($_POST['save'])) {
    form_user_fill('save');
    writeLogRecord("edit_users","Button save is op geklikt voor user: ".$frm_username." form_user_fill is uitgevoerd.");
    writelogrecord("edit_users","formerror:".$formerror." frm_username:".$frm_username." frm_admin:".$frm_admin." frm_indienst:".$frm_indienst);
    writelogrecord("edit_users", "SAVEBUTTON - Wachtwoorden worden gecontroleerd");
    // Checks wanneer password OF verificatiepassword niet leeg zijn
    if (($_POST['pass']) != "" || ($_POST['pass2']) != "") {
        if (!$_POST['pass'] && (!$formerror)) {
            echo '<p class="errmsg"> ERROR: Wachtwoord is een verplicht veld</p>';
            $focus     = 'pass';
            $formerror = 1;
        }
        if (!$_POST['pass2'] && (!$formerror)) {
            echo '<p class="errmsg"> ERROR: Wachtwoord voor verificatie is een verplicht veld</p>';
            $focus     = 'pass2';
            $formerror = 1;
        }
        // Check of de wachtwoorden gelijk zijn
        if (($_POST['pass'] != $_POST['pass2']) && (!$formerror)) {
```

```
61              echo '<p class="errmsg"> ERROR: De wachtwoorden zijn niet gelijk</p>';
62              $focus     = 'pass';
63              $formerror = 1;
64          }
65      }
66      writelogrecord("edit_users", "CHECKFIELDS - Overige velden worden gecontroleerd");
67      if ((!$_POST['voornaam'] || $_POST['voornaam'] == "") && (!$formerror)) {
68          echo '<p class="errmsg"> ERROR: Voornaam is een verplicht veld</p>';
69          $focus     = 'voornaam';
70          $formerror = 1;
71      }
72      if (!$_POST['achternaam'] && (!$formerror)) {
73          echo '<p class="errmsg"> ERROR: Achternaam is een verplicht veld</p>';
74          $focus     = 'achternaam';
75          $formerror = 1;
76      }
77      if (!$_POST['email'] && (!$formerror)) {
78          echo '<p class="errmsg"> ERROR: Email is een verplicht veld</p>';
79          $focus     = 'email';
80          $formerror = 1;
81      }
82      if ($_SESSION['admin'] && (!$formerror)) {
83          if (!isset($_POST['admin'])) {
84              $_POST['admin'] = 0;
85          }
86          else {
87              $_POST['admin'] = 1;
88          }
89          if (!isset($_POST['indienst'])) {
90              $_POST['indienst'] = 0;
91          }
92          else {
93              $_POST['indienst'] = 1;
94          }
95      }
96
97      // here we encrypt the password and add slashes if needed
98      if (!$formerror) {
99          writelogrecord("edit_users", "CREATEQRY1 - Beginnen met het aanmaken van de UPDATE
    query om user ".$_POST['username']."te updaten");
100         $update = "UPDATE users SET ";
101         if (!$_POST['pass'] == "") {
102             $_POST['pass'] = md5($_POST['pass']);
103             writelogrecord("edit_users", "PASS_MD5 - Wachtwoord is middels md5 encrypted");
104             if (!get_magic_quotes_gpc()) {
105                 $_POST['pass'] = addslashes($_POST['pass']);
106                 $_POST['username'] = addslashes($_POST['username']);
107             }
108             $update .= "password='".$_POST['pass']."',";
109         }
110
111         $update .= "admin='".$_POST['admin']."',
112         voornaam='".$_POST['voornaam']."',
113         tussenvoegsel='".$_POST['tussenvoegsel']."',
114         achternaam='".$_POST['achternaam']."',
115         emailadres='".$_POST['email']."',
116         indienst='".$_POST['indienst']."' WHERE username = '".$_POST['username']."'";
117         writeLogRecord("edit_users","UPDQUERY De UPDATE-query wordt nu uitgevoerd op de
    database voor user".$frm_username);
118         $check_upd_user = mysqli_query($dbconn, $update);
119         if ($check_upd_user) {
120             echo '<p class="infmsg">User <b>'.$_POST['username'].'</b> is gewijzigd</p>.';
121             $frm_username      = "";
122             $frm_pass          = "";
```

```
123             $frm_pass2          = "";
124             $frm_voornaam       = "";
125             $frm_tussenvoegsel  = "";
126             $frm_achternaam     = "";
127             $frm_email          = "";
128         }
129         else {
130             echo '<p class="errmsg">Er is een fout opgetreden bij het toevoegen van de
    user. Probeer het nogmaals.<br />
131             Indien het probleem zich blijft voordoen neem dan contact op met de
    webmaster</p>';
132         }
133         header("location: edit_users.php?aktie=disp");
134     }
135 }
136
137 if ($aktie == 'disp') {
138     $sql_allusers = mysqli_query($dbconn, "SELECT * FROM users ORDER BY achternaam");
139     echo "<center><table>";
140     echo
    "<tr><th>ID</th><th>username</th><th>naam</th><th>Emailadres</th><th>Admin</th><th>InDienst
    </th><th colspan=\"3\" align=\"center\">Akties</th></tr>";
141     $rowcolor = 'row-a';
142     while($row_allusers = mysqli_fetch_array($sql_allusers)) {
143         $id             = $row_allusers['ID'];
144         $username       = $row_allusers['username'];
145         $voornaam       = $row_allusers['voornaam'];
146         $tussenvoegsel  = $row_allusers['tussenvoegsel'];
147         $achternaam     = $row_allusers['achternaam'];
148         $emailadres     = $row_allusers['emailadres'];
149         $admin          = $row_allusers['admin'];
150         $indienst       = $row_allusers['indienst'];
151         echo '<tr class="'.$rowcolor.'">
152             <td>'.$id.'</td><td><b>'.$username.'</b></td>
153             <td>'.$achternaam.', '.$voornaam.' '.$tussenvoegsel. '</td>
154             <td>'.$emailadres.'</td>
155             <td align="center">'.$admin.'</td>
156             <td align="center">'.$indienst.'</td>
157             <td><a href="edit_users.php?aktie=edit&edtuser='.$username.'"><img
    src="./img/buttons/user-edit.gif" alt="wijzigen user" title="wijzig user '.$username.'"
    /></a></td>
158             <td><a href="edit_users.php?aktie=delete&edtuser='.$username.'"><img
    src="./img/buttons/user-delete.gif" alt="delete user" title="delete user '.$username.'"
    /></a></td>
159             <td><a href="add_user.php"><img src="./img/buttons/user-plus.gif"
    alt="toevoegen nieuwe user" title="toevoegen nieuwe user" /></a></td>
160             </tr>';
161         // <td><a href="edit_users.php?aktie=delete&deluser='.$username.'"><img
    src="./img/buttons/user-delete.gif" alt="delete user" title="delete user '.$username.'"
    onClick="return confirmDelete()" /></a></td>
162         if ($rowcolor == 'row-a') $rowcolor = 'row-b';
163         else $rowcolor = 'row-a';
164     }
165     echo "</table></center>";
166 }
167
168 if ($aktie == 'edit' || $aktie == 'delete' || $aktie == 'editprof') {
169     $edtuser = $_GET['edtuser'];
170     $focus = "pass";
171     $sql_dspuser = mysqli_query($dbconn, "SELECT * FROM users WHERE username =
    '$edtuser'");
172     while($row_dspuser = mysqli_fetch_array($sql_dspuser)) {
173         $frm_username = $row_dspuser['username'];
174         $frm_voornaam = $row_dspuser['voornaam'];
```

```
175         $frm_tussenvoegsel = $row_dspuser['tussenvoegsel'];
176         $frm_achternaam = $row_dspuser['achternaam'];
177         $frm_email = $row_dspuser['emailadres'];
178         if ($row_dspuser['admin'] == 1) $frm_admin = "checked";
179         else $frm_admin = "";
180         if ($row_dspuser['indienst'] == 1) $frm_indienst = "checked";
181         else $frm_indienst = "";
182     }
183
184 ?>
185
186 <form name="AddUser" action="<?php echo $_SERVER['PHP_SELF']; ?>" method="post">
187     <p>
188     <table>
189         <tr>
190             <td><b>Username</b></td>
191             <td><input <?php if ($aktie == "edit" || $aktie == "editprof") { echo
    "readonly"; } ?> type="text" name="username" maxlength="40" value="<?php if
    (isset($frm_username)) { echo $frm_username; } ?>"></td>
192         </tr>
193         <tr>
194             <td>Wachtwoord</td>
195             <td><input type="password" name="pass" maxlength="10" value="<?php if
    (isset($frm_pass)) { echo $frm_pass; } ?>"></td>
196             <td>Confirm</td>
197             <td><input type="password" name="pass2" maxlength="10" value="<?php if
    (isset($frm_pass2)) { echo $frm_pass2; } ?>"></td>
198         </tr>
199         <tr>
200             <td>Admin</td>
201             <td><input type="checkbox" <?php if (!$_SESSION['admin']) { echo "checked
    disabled "; } ?>name="admin" <?php { echo $frm_admin; } ?>></td>
202         </tr>
203         <tr>
204             <td>Voornaam</td>
205             <td><input type="text" name="voornaam" maxlength="24" value="<?php if
    (isset($frm_voornaam)) { echo $frm_voornaam; } ?>"></td>
206         </tr>
207         <tr>
208             <td>Tussenv.</td>
209             <td><input type="text" name="tussenvoegsel" maxlength="10" value="<?php if
    (isset($frm_tussenvoegsel)) { echo $frm_tussenvoegsel; } ?>"></td>
210             <td>Achternaam</td>
211             <td><input type="text" name="achternaam" maxlength="40" value="<?php if
    (isset($frm_achternaam)) { echo $frm_achternaam; } ?>"></td>
212         </tr>
213         <tr>
214             <td>Email</td>
215             <td colspan="2"><input type="text" name="email" size="40" maxlength="60"
    value="<?php if (isset($frm_email)) { echo $frm_email; } ?>"></td>
216         </tr>
217         <tr>
218             <td>In dienst</td>
219             <td><input type="checkbox" <?php if (!$_SESSION['admin']) { echo "checked
    disabled "; } ?>name="indienst" <?php { echo $frm_indienst; } ?>></td>
220         </tr>
221     </table>
222     <br />
223     <?php if ($aktie == 'edit' || $aktie == 'editprof') echo '<input class="button"
    type="submit" name="save" value="save">'; ?>
224     <?php if ($aktie == 'delete') echo '<input class="button" type="submit" name="delete"
    value="delete" onClick="return confirmDelUser()">'; ?>
225     <input class="button" type="submit" name="cancel" value="cancel">
226     </p>
```

```
</form>
<br />
<?php
if (!isset($focus)) {
    $focus='username';
}
setfocus('AddUser', $focus);

// Einde van if aktie=edit
}

include ("footer.php");
?>


```