Thirumurugan A
18BCE2060

```php
<?php

$message = array();
$message_css = "";

function changePassword($user,$oldPassword,$newPassword,$newPasswordCnf){
  global $message;
  global $message_css;

    $server = "localhost";
    $dn = "ou=People,dc=example";

    error_reporting(0);
    ldap_connect($server);
    $con = ldap_connect($server);
    ldap_set_option($con, LDAP_OPT_PROTOCOL_VERSION, 3);

    // bind anon and find user by uid
    $user_search = ldap_search($con,$dn,"(|(uid=$user)(mail=$user))");
    $user_get = ldap_get_entries($con, $user_search);
    $user_entry = ldap_first_entry($con, $user_search);
    $user_dn = ldap_get_dn($con, $user_entry);
    $user_id = $user_get[0]["uid"][0];
    $user_givenName = $user_get[0]["givenName"][0];
    $user_search_arry = array( "*", "ou", "uid", "mail", "passwordRetryCount", "passwordhistory" );
    $user_search_filter = "(|(uid=$user_id)(mail=$user))";
    $user_search_opt = ldap_search($con,$user_dn,$user_search_filter,$user_search_arry);
    $user_get_opt = ldap_get_entries($con, $user_search_opt);
    $passwordRetryCount = $user_get_opt[0]["passwordRetryCount"][0];
    $passwordhistory = $user_get_opt[0]["passwordhistory"][0];

    //$message[] = "Username: " . $user_id;
    //$message[] = "DN: " . $user_dn;
    //$message[] = "Current Pass: " . $oldPassword;
    //$message[] = "New Pass: " . $newPassword;

    /* Start the testing */
    if ( $passwordRetryCount == 3 ) {
      $message[] = "Your Account is Locked Out!!!";
      return false;
    }
    if (ldap_bind($con, $user_dn, $oldPassword) === false) {
      $message[] = "Current Username or Password is wrong.";
      return false;
    }
    if ($newPassword != $newPasswordCnf ) {
      $message[] = "Your New passwords do not match!";
      return false;
    }
    $encoded_newPassword = "{SHA}" . base64_encode( pack( "H*", sha1( $newPassword ) ) );
    $history_arr = ldap_get_values($con,$user_dn,"passwordhistory");
    if ( $history_arr ) {
```

```
53.       $message[] = "Your new password matches one of the last 10
   passwords that you used.";
54.       return false;
55.     }
56.     if (strlen($newPassword) < 8 ) {
57.       $message[] = " Your new password is too short, 8 characters
   long.";
58.       return false;
59.     }
60.     if (!preg_match("/[0-9]/",$newPassword)) {
61.       $message[] = "Your new password must contain at least one
   number.";
62.       return false;
63.     }
64.     if (!preg_match("/[a-zA-Z]/",$newPassword)) {
65.       $message[] = " Your new password must contain at least one
   letter.";
66.       return false;
67.     }
68.     if (!preg_match("/[A-Z]/",$newPassword)) {
69.       $message[] = " Your new password must contain at least one
   uppercase letter.";
70.       return false;
71.     }
72.     if (!preg_match("/[a-z]/",$newPassword)) {
73.       $message[] = " Your new password must contain at least one
   lowercase letter.";
74.       return false;
75.     }
76.     if (!$user_get) {
77.       $message[] = " Unable to connect to server, you may not change
   your password at this time, sorry.";
78.       return false;
79.     }
80.
81.     $auth_entry = ldap_first_entry($con, $user_search);
82.     $mail_addresses = ldap_get_values($con, $auth_entry, "mail");
83.     $given_names = ldap_get_values($con, $auth_entry, "givenName");
84.     $password_history = ldap_get_values($con, $auth_entry,
   "passwordhistory");
85.     $mail_address = $mail_addresses[0];
86.     $first_name = $given_names[0];
87.
88.     /* And Finally, Change the password */
89.     $entry = array();
90.     $entry["userPassword"] = "$encoded_newPassword";
91.
92.     if (ldap_modify($con,$user_dn,$entry) === false){
93.       $error = ldap_error($con);
94.       $errno = ldap_errno($con);
95.       $message[] = " Your password cannot be change, please contact the
   administrator.";
96.       $message[] = "$errno - $error";
97.     } else {
98.       $message_css = "yes";
99.       mail($mail_address,"Password change notice","Dear $first_name,
```

```
100. Your password on http://support.example.com for account $user_id was
   just changed. If you did not make this change, please contact
   support@example.com.
101. If you were the one who changed your password, you may disregard this
   message.
102.
103. Thanks
104. -Matt");
105.     $message[] = "The password for $user_id has been changed.<br/>An
   informational email as been sent to $mail_address.<br/>Your new
   password is now fully Active.";
106.   }
107. }
108.
109. ?>
110. <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
111. <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
112. <head>
113. <title>Password Change Page</title>
114. <style type="text/css">
115. body { font-family: Verdana,Arial,Courier New; font-size: 0.7em; }
116. th { text-align: right; padding: 0.8em; }
117. #container { text-align: center; width: 500px; margin: 5% auto; }
118. .msg_yes { margin: 0 auto; text-align: center; color: green;
   background: #D4EAD4; border: 1px solid green; border-radius: 10px;
   margin: 2px; }
119. .msg_no { margin: 0 auto; text-align: center; color: red; background:
   #FFF0F0; border: 1px solid red; border-radius: 10px; margin: 2px; }
120. </style>
121. <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
122. </head>
123. <body>
124. <div id="container">
125. <h2>Password Change Page</h2>
126. <p>Your new password must be 8 characters long or longer and have at
   least:<br/>
127. one capital letter, one lowercase letter, & one number.<br/>
128. You must use a new password, your current password<br/>can not be the
   same as your new password.</p>
129. <?php
130.       if (isset($_POST["submitted"])) {
131.
   changePassword($_POST['username'],$_POST['oldPassword'],$_POST['newPass
   word1'],$_POST['newPassword2']);
132.         global $message_css;
133.         if ($message_css == "yes") {
134.           ?><div class="msg_yes"><?php
135.          } else {
136.           ?><div class="msg_no"><?php
137.           $message[] = "Your password was not changed.";
138.         }
139.         foreach ( $message as $one ) { echo "<p>$one</p>"; }
140.       ?></div><?php
141.       } ?>
142. <form action="<?php print $_SERVER['PHP_SELF']; ?>"
   name="passwordChange" method="post">
```

```
143. <table style="width: 400px; margin: 0 auto;">
144. <tr><th>Username or Email Address:</th><td><input name="username"
   type="text" size="20px" autocomplete="off" /></td></tr>
145. <tr><th>Current password:</th><td><input name="oldPassword"
   size="20px" type="password" /></td></tr>
146. <tr><th>New password:</th><td><input name="newPassword1" size="20px"
   type="password" /></td></tr>
147. <tr><th>New password (again):</th><td><input name="newPassword2"
   size="20px" type="password" /></td></tr>
148. <tr><td colspan="2" style="text-align: center;" >
149. <input name="submitted" type="submit" value="Change Password"/>
150. <button
   onclick="$('frm').action='changepassword.php';$('frm').submit();">Cance
   l</button>
151. </td></tr>
152. </table>
153. </form>
154. </div>
155. </body>
```