Registration and User's Security Pages

Registration.php

- ✓ read: email, password, password_confirmation
- ✓ else if email doesn't contain '@', notify and stop
- ✓ else if password = null, notify and stop
- ✓ else if password_confirmation ≠ password, notify and stop
- ✓ go to RegistrationProcessing.php

RegistrationProcess.php

- ✓ receive from Registration.php: email, password
- ✓ salt ← random integer from 100000 to 999999
  confirmation_code ← random string of 6 characters
- ✓ encrypted_password ← sha1(salt + password)
- ✓ if email is already in Registration, notify and stop (resend code?)
  if email is already in User, notify and stop (forgot password?)
- ✓ insert into Registration: email, encrypted_password, salt, confirmation_code
  send e-mail with confirmation code
  notify (confirmation code sent)
  go to EmailConfirmationForm.php

EmailConfirmationForm.php

- ✓ read: email, entered_confirmation_code
- ✓ if confirmation_code is null, notify
- ✓ else if email doesn't contain '@', notify
- ✓ go to EmailConfirmationProcessing.php
  resend code goes to ResetCode.php

EmailConfirmationProcessing.php

- ✓ receive from EmailConfirmationForm.php: email, entered_confirmation_code
- ✓ reg ← row in Registration that contains email
- ✓ if reg = null, notify and stop (email not registered)
- ✓ if reg.code ≠ entered_confirmation_code, notifiy and stop (wrong code entered)
- ✓ copy username, password, salt from reg to User
  delete reg
  notify (registration successfully done)
  go to Login.php

ResetCode.php

- ✓ receive from EmailConfirmationForm.php: email
  confirmation_code ← random string of 6 characters
- ✓ user ← row in Registration that contains email
- ✓ user.code ← confirmation_code
  send e-mail with code confirmation
  go to EmailConfirmationForm.php

Login.php

  read email, entered_password
- ✓ if email doesn't contain '@', notify and stop
- ✓ else if password = null, notify and stop
  forgot password goes to ForgotPassword.php
  go to LoginProcessing.php

LoginProcessing.php

- ✓ receive from Login.php: email, entered_password
- ✓ user ← row in User that contains email
- ✓ if user = null, notify and stop (email not registered)
- ✓ get password, salt, temp_password from user
- ✓ if sha1(salt + entered_password) = password, go to Main.php
  else if sha1(salt + entered_password) = temp_password, go to ResetPassword.php
  else notify and stop

ForgotPassword.php

  read email
  if email doesn't contain '@', notify and stop
  go to ForgotPassword.php

ForgotPasswordProcessing.php

  receive from ForgotPassword.php: email
  temp_password = random string of length 8
  encrypted_temp_password = sha1(temp_password)
  user ← row in User that contains email
  user.temp_password ← encrypted_temp_password
  send e-mail with code temporary password
  notify (new password sent)
  go to Login.php

ResetPassword.php

  receive from LoginProcessing.php: email
  read password, password_confirmation
  if password = null, notify and stop
  else if password_confirmation ≠ password, notify and stop
  go to ResetPasswordProcessing.php

ResetPasswordProcessing.php

  receive from ResetPassword.php: password, email
  salt ← random integer from 100000 to 999999
  encrypted_password ← sha1(salt + password)
  user ← row in User that contains email
  user.salt ← salt
  user.password ← encrypted_password
  go to Login.php

Main.php

  receive email from LoginProcessing.php
  ...