Reset Password via Email Project

Primary Mentor	Unknown User (wyclif)
Backup Mentor	Burke Mamlin
Assigned to	Harisu Fanyui

Background

User accounts in the OpenMRS Platform are secured with password hashes and salt; however, because OpenMRS did not historically include the ability to send email, the process for resetting password has been less than ideal. Currently, an administrator sets a temporary password or a user answers their "secret question" (a question and answer set the user previously provided). A medical record system should have a stronger approach to password security and not even an administrator should ever know a user's password (even temporarily). The current approach also puts an undue burden on administrators to reset passwords for users who have forgotten them.

Over the past few years, OpenMRS has been migrating toward use of web services (REST or FHIR), so any new functionality should be designed to work through these RESTful APIs.

Purpose

The goal of this project is to introduce mail capability into the OpenMRS Platform along with the ability for a user to perform a self-service password reset. The primary goal for this project is to introduce the functionality such that it can be managed through the REST API. Only when this is completed and merged into master, will we proceed to build user interfaces for managing the functionality.

Required Skills

- Java
- Basic SQL skills
- Ability to write and refactor a REST API
- Basic Javascript and HTML

Objectives

- Incorporate JSR 919 mail capability into the OpenMRS Platform
- Add the ability for an administrator to configure the mail functionality via the REST API
- Add `users.email` to the `users` table within the Platform along with the ability to set and retrieve a user's email address via the REST API
- Add the ability for a temporary token to be generated for a user that, until it expires, can be used to reset their password. This should be able to be triggered by the user or an admin via the REST API.
- Add support for an email template to be used for password reset messages (should support localization).
- Add support for a REST API method that, given a valid username and reset token along with a new password, will reset the user's password.
- Deprecate the use of user's secret question and secret answer within the Platform.

Design ideas

- User email would be stored in a new `users.email` attribute within core.
- Create an API service for triggering a reset link (default would be current user; an admin may need to trigger it for another user).
    - A new `user_reset_token` table would be used to store user, timestamp, and one-way hashed UUID (max one per user).
    - Using one-way hash of the UUID that was return to the user (via REST response or email) would prevent anyone with database access from simply using the contents of the `user_reset_token` to reset some else's password).

Extra Credit

- Make the
- Demonstrate use of the new password reset REST API endpoints using an OWA (open web app) web application in the OpenMRS Reference Application.
- Add a background process to prune expired reset token.

Resources

- JavaMail
- Password Reset Email Best Practices