# Use case: Forgotten Password Reset

**Iteration**: 1

**Primary Actor**: User (Player)

**Goal in context**:

- To allow users to access their account long enough to create a new password.

**Preconditions:**

- The user has access to the OMG platform via a web browser or an application.
- The user has a registered account with an verified username, email and password.

**Trigger**:

- The user wants to access their account but can't give the password they registered with.

**Scenario**:

1. The user navigates to the 'forgot password' screen from the OMG login screen.
2. The screen prompts for:
    a. Email
    b. Username
3. User enters their information.
    a. The system checks both inputs for valid formatting
    b. The system checks the username/email pairing against stored user data.
4. If the input is valid, a temporary password is sent to the provided email address.
    a. The temporary password is deleted from the database 15 minutes after being sent, or right after the user logs in.
5. The system prompts the user to create a new password.
    a. System checks the password's validity.
6. The new password is added to the database.

**<u>Post conditions:</u>**

- The user has a new password that they can log into their account with.

**Exceptions**:

1. Username or email not recognized.
    o User is asked to check that they are entering the correct information.
2. Email not associated with username.
    o User is asked to enter a different email.
3. New password isn't formatted in a valid way.
    o System suggests ways to make a stronger password.

**Priority**: High priority. This feature restores access to the platform in the case that a user forgets their password.

**When available**: First iteration

**Frequency of use**: Intermittent

**Channel to actor**: 'Forgot password' screen, via web browser or application.

**Secondary actors**:

- User data database: database containing usernames, emails and passwords.

**Channel to secondary actors**:

- User data database: application server for returning database information to the client.

**Open issues**:

1. Should there be a limit for password reset requests?
2. Should there be a time-out between reset requests?