# Insecure Password Recovery

<https://www.owasp.org/index.php/Testing_for_weak_password_change_or_reset_functionalities_(OTG-AUTHN-009)>

## Test Objectives

1. Determine the resistance of the application to subversion of the account change process allowing someone to change the password of an account.
2. Determine the resistance of the password reset functionality against guessing or bypassing.

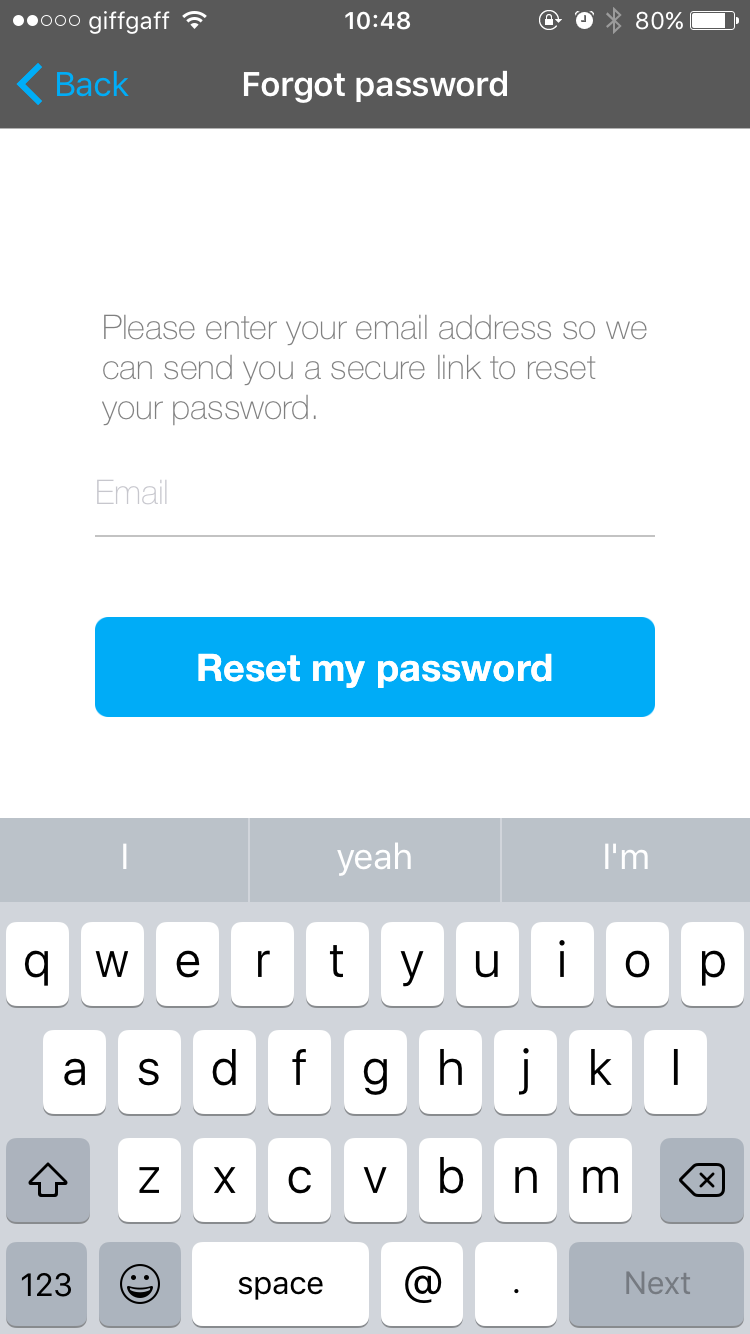
## How To Test

For both password change and password reset it is important to check:

1. If users, other than administrators, can change or reset passwords for accounts other than their own.
2. If users can manipulate or subvert the password change or reset process to change or reset the password of another user or administrator.
3. If the password change or reset process is vulnerable to CSRF.

## Testing Password Reset

### What information is required to reset the password?



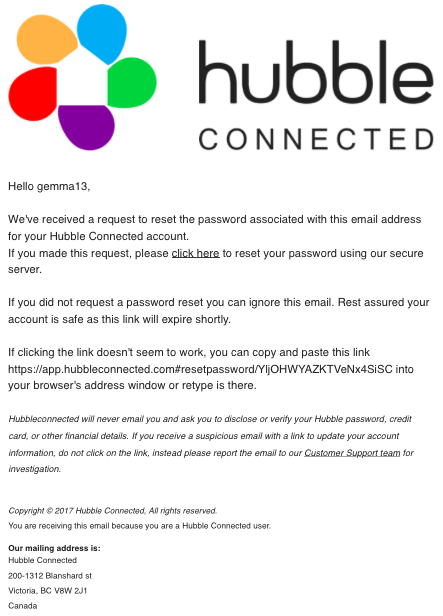
Sending the password (or password reset link) to the user email address without first asking for a secret question means relying 100% on the security of that email address, which is not suitable if the application needs a high level of security.

### Are reset passwords generated randomly?

The most insecure scenario here is if the application sends or visualizes the old password in clear text because this means that passwords are not stored in a hashed form, which is a security issue in itself. The best security is achieved if passwords are randomly generated with a secure algorithm that cannot be derived.

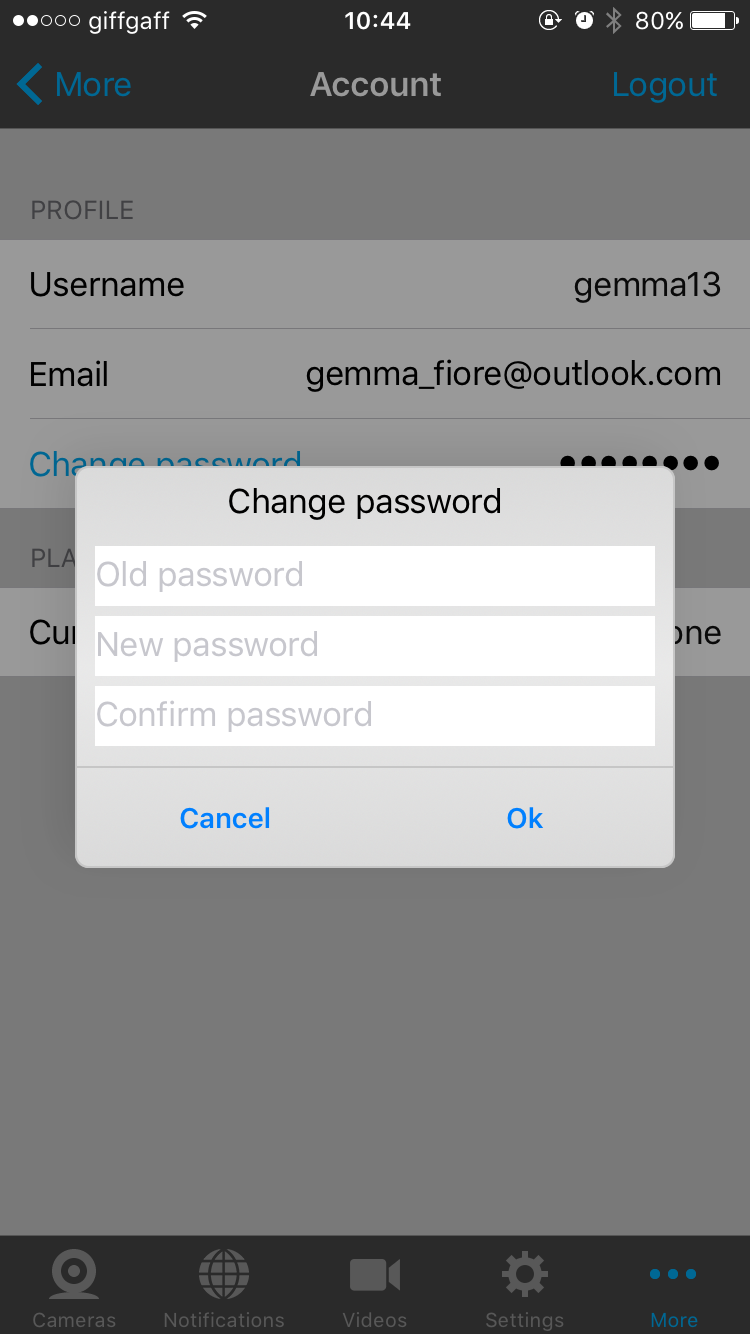
### Is the reset password functionality requesting confirmation before changing the password?

To limit denial-of-service attacks the application should email a link to the user with a random token, and only if the user visits the link then the reset procedure is completed. This ensures that the current password will still be valid until the reset has been confirmed.



## Testing Password Change

The old password is requested to complete the change:



The most insecure scenario would be if the application permits the change of the password without requesting the current password, as if the attacker were able to take control of a valid session they could change the victim’s password.