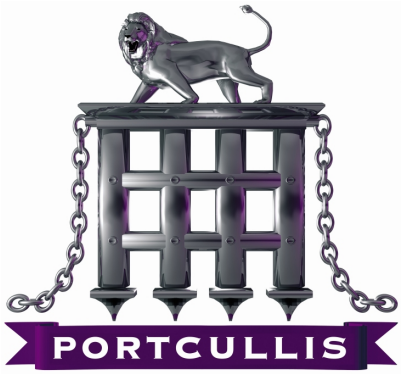


# Password Reset Good Practice Guide

**Written By** Kieran Combes

Portcullis Computer Security LTD
The Grange Barn
Pike's End
Pinner
Middlesex
HA5 2EX

Tel: 020 8868 0098
Fax: 020 8868 0017
ktc@portcullis-security.com

**Document Reference** Whitepapers/Password Reset White Paper/wp_Password Reset White Paper_1.0
**Version** 1.0

**Date** 24 March 2012

# 1 Document History

| Revision | Author | Role | Date | Comments |
|---|---|---|---|---|
| 0.1 | KTC | Researcher | 20/03/2012 | 1st Draft Whitepaper |
| 0.2 | DUB | Peer Reviewer | 24/03/2012 | 2nd Draft Whitepaper |
| 1.0 | KTC | Researcher | 24/03/2012 | Publication |

Table 1: Document Revision History

# Contents

# 3 Introduction

The purpose of this document is to discuss the password reset functionality which allows a user, who has forgotten their password, to authenticate against the system and negotiate a new password. There are a number of common methods that can be employed to achieve this. One of which is to only ask the user to answer a predefined security question. Two of the most commonly used questions are given below:

- What is your mother's maiden name?
- What was the name of your first school?

However, the problem with this approach is that it creates a weakness in the authentication process. In this situation it may be possible for someone to change a users password with a piece of information that can be easily gathered through the use of search engines or social networking sites such as Facebook and Linkedin.

For example, United States Vice President Candidate 2008, Sarah Palin's email account was compromised[1] using the password reset functionality with easily obtainable personal information

# 4 Good Practice

Whilst there are numerous methods to implement a secure password reset process they are all based around the following three ideas:

1. Reset Initiation Attack Protection - Minimise the likely success of automated attacks against the reset initiation function.
2. Continued Use - Allow a legitimate user who is being targeted to continue using the application.
3. Out-of-band (OOB) Communication - Use an OOB communication mechanism as an integral part of the reset process, e.g. SMS or Email.

## 4.1 Reset Initiation Attack Protection

The password reset functionality should be implemented in a manner that cannot be easily used to enumerate current registered users. This can be achieved by forcing users to supply both their userid or email address as well as a second piece of "Secret" information when the reset process is initiated. A second protection that can be used, although it may only slow down automated attacks, is to implement a CAPTCHA system.

This step is important but not as much as the Out-of-band Communication step. If stage 3 is well implemented a brute-force attack alone is not likely to be successful to compromise an account, even if the correct user details are guessed.

It is always important to check for brute-force attempts against these types of functions as well as the login ones. This can be achieved by applying account lock out protection in an intelligent manner. Many sites use metrics to measure the likelihood that any anomaly is an automated attack. Information such as a previously correct logon IP address can be used to rate numerous incorrect login attempts. In addition, implementing a CAPTCHA system in a way that has a minimal effect on a legitimate user, such as only enabling it once a small number of incorrect logins have occurred, is also a good trade off between security and usability.

It is also recommended that the user is informed about these failed reset attempts, this can be done as a message to the user when they successfully login or by using the OOB communication mechanism.

## 4.2 Continued Use

If an automated attack manages to correctly guess the data required to initiate the password reset, this should not result in a Denial of Service condition for the legitimate user. The current credentials should continue to work until the process of the password reset has been completed successfully. If this is not done, an attacker could prevent a user from being able to login by continually bombarding the system with password reset requests, which will have the effect of locking out the real user.

## 4.3 Out-of-band Communication

An OOB communication mechanism should be used to supply the user with a randomly generated piece of information, which is required to reset their password. This should be implemented in a manner which means that if this communication is intercepted then the interceptor cannot reset the account password with this information alone. This can be achieved by sending an email to the users registered address

with a one time, time limited, link. Once the user follows the link they are then requested to supply a Secret" piece of information. An alternative solution is to use a second OOB communication channel. This could be a text message containing the Secret" information. In this way the attacker would need to have compromised two OOB transport mediums.

The randomly generated data should also be of sufficient quality that it cannot be guessed by an attacker. This can be helped by having a time limited window for which the random data is usable. For instance if the random data is only a four digit PIN and an automated attack can generate arbitrary numbers of these reset PIN's then it would be possible in a reasonable amount of time to gain access to the account without intercepting the OOB communication. In addition, if the link is not one time but based on the account userid/email address this could be calculated by an attacker.

# 5 Secret Information

Secret information can take two forms:

1. Information supplied when an account is created;
2. Information based around current account conditions.

A list of questions that can be used to enable users to supply extra information are contained below. These are designed to not be easily searchable or findable by way of data mining techniques.

The second method is to use general account information such as digits from registered credit cards, direct debit information or other information that would be easily found by the legitimate user, but not by an attacker.

## 5.1 Sample Questions

A small sample of questions that could be used has been supplied below:

- What was your childhood nickname?
- In what city did you meet your partner?
- What is the name of your favourite childhood friend?
- What street did you live on when you attended primary school?
- What is your oldest sibling's birthday month and year? (for example, January 1900).
- What is the middle name of your youngest child?
- What is your oldest sibling's middle name?
- What secondary school did you attend?
- What was your childhood phone number including area code? (for example, 00000,0000000)
- What is your oldest cousin's first and last name?
- What was the name of your first stuffed animal?
- In what city or town did your mother and father meet?
- Where were you when you had your first kiss?
- What is the first name of the boy or girl that you first kissed?
- What was the last name of your favourite teacher?
- In what city does your nearest sibling live?
- What is your youngest brother's birthday month and year? (for example., January 1900)
- What is your maternal grandmother's maiden name?
- In what city or town was your first job?
- What is the name of the place your wedding reception was held?
- What is the name of a university you applied for but did not attend?

- Where were you when you first heard about 9/11?

# 6 Example Implementations

**Method 1**

1. A user enters either a username or email address in the forgotten password page.
2. An email with a link that expires in 24 hours is then sent to the email account for that username
3. The user then has to click on the link prompting the system to send a text with a code is sent to the user's mobile phone.
4. The user then has to enter the code that was sent to them and only at that stage, be allowed to enter a new password for that account.

This method offers a good level of security as it does not rely on the system trusting that the person trying to reset their password is the account owner. If a malicious person tried to hijack a user's account they would need to have access to both the user's email account and their mobile phone. The original password would not be changed until both steps had been completed thereby removing the possibility of a Denial of Service attack against the user. The only concern would be flooding a user's mobile with account reset requests.

**Method 2**

A second method to improve the effectiveness of a password reset would be to authenticate a genuine password reset by asking a user for two pieces of information after they have supplied their username/email address. The information required should include difficult to obtain information such as three digits from their registered credit card and a standard question such as "What secondary school did you attend". A link could then be sent to the user allowing them to reset their password.
In order to increase the security of this method after the link has been accessed a further security question could be asked of the user before allowing them to reset their password.

When generating a link to send to a user, enabling them to reset their password, it should be random so that it is not possible for an attacker or malicious user, who has knowledge of the username and the security questions for an account holder, to pre-determine the link.