# CWE Detail – CWE-620

## Description

When setting a new password for a user, the product does not require knowledge of the original password, or using another form of authentication.

## Extended Description

This could be used by an attacker to change passwords for another user, thus gaining the privileges associated with that user.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2007-0681: Web app allows remote attackers to change the passwords of arbitrary users without providing the original password, and possibly perform other unauthorized actions.

**•** CVE-2000-0944: Web application password change utility doesn't check the original password.

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Gain Privileges or Assume Identity — Notes:

## Potential Mitigations

**•** Architecture and Design: When prompting for a password change, force the user to provide the original password in addition to the new password. (Effectiveness: N/A)

**•** Architecture and Design: Do not use "forgotten password" functionality. But if you must, ensure that you are only providing information to the actual user, e.g. by using an email address or challenge question that the legitimate user already provided in the past; do not allow the current user to change this identity information until the correct password has been provided. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** While the code confirms that the requesting user typed the same new password twice, it does not confirm that the user requesting the password change is the same user whose password will be changed. An attacker can request a change of another user's password and gain control of the victim's account.