# CWE Detail – CWE-530

## Description

A backup file is stored in a directory or archive that is made accessible to unauthorized actors.

## Extended Description

Often, older backup files are renamed with an extension such as .~bk to distinguish them from production files. The source code for old files that have been renamed in this manner and left in the webroot can often be retrieved. This renaming may have been performed automatically by the web server, or manually by the administrator.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Modes of Introduction

**•** Operation: OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.

## Common Consequences

**•** Impact: Read Application Data — Notes: At a minimum, an attacker who retrieves this file would have all the information contained in it, whether that be database calls, the format of parameters accepted by the application, or simply information regarding the architectural structure of your site.

## Potential Mitigations

**•** Policy: Recommendations include implementing a security policy within your organization that prohibits backing up web application source code in the webroot. (Effectiveness: N/A)