# CWE Detail – CWE-540

## Description

Source code on a web server or repository often contains sensitive information and should generally not be accessible to users.

## Extended Description

There are situations where it is critical to remove source code from an area or server. For example, obtaining Perl source code on a system allows an attacker to understand the logic of the script and extract extremely useful information such as code bugs or logins and passwords.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2022-25512: Server for Team Awareness Kit (TAK) application includes sensitive tokens in the JavaScript source code.

**•** CVE-2022-24867: The LDAP password might be visible in the html code of a rendered page in an IT Asset Management tool.

**•** CVE-2007-6197: Version numbers and internal hostnames leaked in HTML comments.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes:

## Potential Mitigations

**•** Architecture and Design: Recommendations include removing this script from the web server and moving it to a location not accessible from the Internet. (Effectiveness: N/A)

## Demonstrative Examples

**•** database.inc

**•** N/A