# CWE Detail – CWE-489

## Description

The product is deployed to unauthorized actors with debugging code still enabled or active, which can create unintended entry points or expose sensitive information.

## Extended Description

A common development practice is to add "back door" code specifically designed for debugging or testing purposes that is not intended to be shipped or deployed with the product. These back door entry points create security risks because they are not considered during design or testing and fall outside of the expected operating conditions of the product.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Related Attack Patterns (CAPEC)

* CAPEC-121
* CAPEC-661

## Modes of Introduction

**•** Implementation: In web-based applications, debug code is used to test and modify web application properties, configuration information, and functions. If a debug application is left on a production server, this oversight during the "software process" allows attackers access to debug functionality.

**•** Build and Compilation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism, Read Application Data, Gain Privileges or Assume Identity, Varies by Context — Notes: The severity of the exposed debug application will depend on the particular instance. At the least, it will give an attacker sensitive information about the settings and mechanics of web applications on the server. At worst, as is often the case, the debug application will allow an attacker complete control over the web application and server, as well as confidential information that either of these access.

## Potential Mitigations

**•** Build and Compilation: Remove debug code before deploying the application. (Effectiveness: N/A)

## Applicable Platforms

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

## Demonstrative Examples

**•** Then a conforming link will look like:

## Notes

**•** Other: In J2EE a main method may be a good indicator that debug code has been left in the application, although there may not be any direct security impact.