ENV06-J. Production code must not contain debugging entry points

According to J2EE Bad Practices: Leftover Debug Code [Hewlett-Packard 2015]:

> *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 application. When this sort of debug code is accidentally left in the application, the application is open to unintended modes of interaction. 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 application.*
>
> *The most common example of forgotten debug code is a `main()` method appearing in a web application. Although this is an acceptable practice during product development, classes that are part of a production J2EE application should not define a `main()`.*

Noncompliant Code Example

In this noncompliant code example, the `Stuff` class has a `main()` function that tests its methods. Although useful for debugging, if this function is left in production code (for a web application, for example), an attacker can invoke `Stuff.main()` directly, gaining access to `Stuff`'s test methods.

```
class Stuff {
  private static final bool DEBUG = False;
  // Other fields and methods
  public static void main(String args[]) {
    Stuff.DEBUG = True;
    Stuff stuff = new Stuff();
    // Test stuff
  }
}
```

Compliant Solution

A compliant solution simply removes the `main()` method from the `Stuff` class, depriving attackers of this entry point.

Risk Assessment

Leaving extra entry points into production code could allow an attacker to gain special access to the program.

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
ENV06-J	High	Probable	Low	**P18**	**L1**

Automated Detection

This rule is not amenable to automated static analysis.

Tool	Version	Checker	Description
SonarQube	6.7	**S2653**	Detects `main` in `Servlets` and EJBs

Bibliography

[Hewlett-Packard 2015]	J2EE Bad Practices: Leftover Debug Code

← ↑ →