




 Secrets


 ABAP


 Apex


 C


 C++


 CloudFormation


 COBOL


 C#


 CSS


 Flex


 Go


 HTML


 **Java**


 JavaScript


 Kotlin


 Objective C


 PHP


 PL/I


 PL/SQL


 Python


 RPG


 Ruby


 Scala


 Swift


 Terraform


 Text

 TypeScript

 T-SQL

 VB.NET

 VB6

 XML



Java static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your JAVA code

- All rules 632
- Vulnerability 53
- Bug 154
- Security Hotspot 36
- Code Smell 389
- Quick Fix 42

Bug
"Thread.run()" should not be called directly
Bug
"equals" method overrides should accept "Object" parameters
Bug
The Object.finalize() method should not be called
Bug
Enabling file access for WebViews is security-sensitive
Security Hotspot
Enabling JavaScript support for WebViews is security-sensitive
Security Hotspot
Constructing arguments of system commands from user input is security-sensitive
Security Hotspot
Using unencrypted files in mobile applications is security-sensitive
Security Hotspot
Using biometric authentication without a cryptographic solution is security-sensitive
Security Hotspot
Using unencrypted databases in mobile applications is security-sensitive
Security Hotspot
Authorizing non-authenticated users to use keys in the Android KeyStore is security-sensitive
Security Hotspot
Allowing user enumeration is security-sensitive

Tags ▾

Search by name... 🔍

"switch" statements should have "default" clauses

Analyze your code

- Code Smell
- Critical
- cwe cert

The requirement for a final default clause is defensive programming. The clause should either take appropriate action, or contain a suitable comment as to why no action is taken.

Noncompliant Code Example

```
switch (param) { //missing default clause
  case 0:
    doSomething();
    break;
  case 1:
    doSomethingElse();
    break;
}
```

```
switch (param) {
  default: // default clause should be the last one
    error();
    break;
  case 0:
    doSomething();
    break;
  case 1:
    doSomethingElse();
    break;
}
```





Compliant Solution

```
switch (param) {
  case 0:
    doSomething();
    break;
  case 1:
    doSomethingElse();
    break;
  default:
    error();
    break;
}
```

Exceptions

If the switch parameter is an Enum and if all the constants of this enum are used in the case statements, then no default clause is expected.

Example:

Allowing user enumeration is security-sensitive  Security Hotspot
Allowing requests with excessive content length is security-sensitive  Security Hotspot
Disabling auto-escaping in template engines is security-sensitive  Security Hotspot
Allowing deserialization of LDAP objects is security-sensitive  Security Hotspot
Continuing REXX flow control

```
public enum Day {  
    SUNDAY, MONDAY  
}  
...  
switch(day) {  
    case SUNDAY:  
        doSomething();  
        break;  
    case MONDAY:  
        doSomethingElse();  
        break;  
}
```

See

- [MITRE, CWE-478](#) - Missing Default Case in Switch Statement
- [CERT, MSC01-C](#) - Strive for logical completeness

Available In:

sonarlint

|

sonarcloud

|

sonarqube