**Code Correctness: Erroneous String Compare Development Mitigation**

**SOP**

Code correctness vulnerabilities occur when an Object API is not used properly or as intended. Code correctness vulnerabilities can occur from erroneous string comparisons when the comparison is done with == or !=, instead of the equals() method.

1. Main difference between .equals() method and == operator is that one is method and other is operator.
2. We can use == operators for reference comparison (**address comparison**) and .equals() method for **content comparison**. In simple words, == checks if both objects point to the same memory location whereas .equals() evaluates to the comparison of values in the objects.
3. If a class does not override the equals method, then by default it uses equals(Object o) method of the closest parent class that has overridden this method.

**Defense Against Code Correctness: Erroneous String Compare**

The use of == or != to compare two strings for equality only compares the objects for equality, not their values. The equals()method should be used to compare both equality and value.

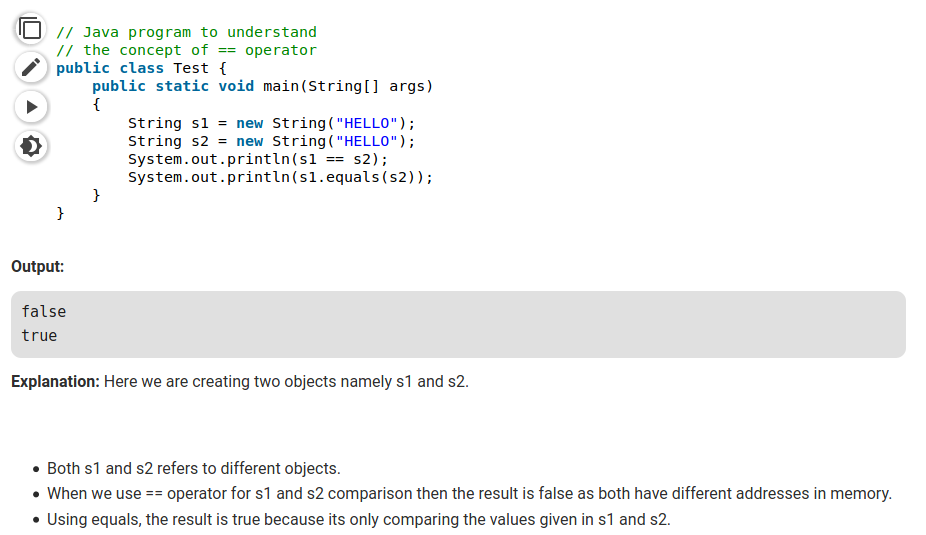
**Examples**

**General Example**

if(args[0] == STRING\_CONSTANT) {

logger.info(“miracle”);

}



**Explanation**

In the code above, since the objects being compared are not of the same type, this will always return false.

**Recommendation**

The code below demonstrates how using the equals() method can correctly compare the two objects for both equality and value:

if(STRING\_CONSTANT.equals(args[0])) {

logger.info(“could happen”);

}

**Example**

if(event.getType() == “activated”) {

…

}

**Explanation**

Strings should be compared with the equals() method.

**Resources**

1. [HP Enterprise Security – Code Correctness: Erroneous String Compare](https://vulncat.fortify.com/en/detail?id=desc.structural.java.code_correctness_erroneous_string_compare#Java%2fJSP)
2. <https://www.geeksforgeeks.org/difference-equals-method-java/>
3. <https://www.java67.com/2012/11/difference-between-operator-and-equals-method-in.html>