

 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

 Code Smell
OS commands should not be vulnerable to argument injection attacks  Vulnerability
"ActiveMQConnectionFactory" should not be vulnerable to malicious code deserialization  Vulnerability
Logging should not be vulnerable to injection attacks  Vulnerability
Exceptions should not be thrown from servlet methods  Vulnerability
Return values should not be ignored when they contain the operation status code  Bug
Repeated patterns in regular expressions should not match the empty string  Bug
AssertJ assertions "allMatch" and "doesNotContains" should also test for emptiness  Bug
Double Brace Initialization should not be used  Bug
Non-primitive fields should not be "volatile"  Bug
"toArray" should be passed an array of the proper type  Bug

Non-serializable objects should not be stored in "HttpSession" objects

Analyze your code

 Bug  Major   cwe

If you have no intention of writing an `HttpSession` object to file, then storing non-serializable objects in it may not seem like a big deal. But whether or not you explicitly serialize the session, it may be written to disk anyway, as the server manages its memory use in a process called "passivation". Further, some servers automatically write their active sessions out to file at shutdown & deserialize any such sessions at startup.

The point is, that even though `HttpSession` does not extend `Serializable`, you must nonetheless assume that it will be serialized, and understand that if you've stored non-serializable objects in the session, errors will result.

Noncompliant Code Example





```
public class Address {  
    //...  
}  
  
//...  
HttpSession session = request.getSession();  
session.setAttribute("address", new Address()); // Noncompliant
```

See

- OWASP Top 10 2021 Category A4 - Insecure Design
- Mitre, CWE-579 - J2EE Bad Practices: Non-serializable Object Stored in Session

Available In:

 |  | 

<div>Neither "Math.abs" nor negation should be used on numbers that could be "MIN_VALUE"</div> <div> Bug</div>
<div>The value returned from a stream read should be checked</div> <div> Bug</div>
<div>"@NonNull" values should not be set to null</div> <div> Bug</div>
<div>"Iterator.next()" methods should throw "NoSuchElementException"</div> <div> Bug</div>