

JT-Bug-Id	Description
Sec 1	<u>DP: Classloaders should only be created inside doPrivileged block</u>
Sec 2	<u>DP: Method invoked that should be only be invoked inside a doPrivileged block</u>
Sec 3	<u>EI: May expose internal representation by returning reference to mutable object</u>
Sec 4	<u>EI2: May expose internal representation by incorporating reference to mutable object</u>
Sec 5	<u>FI: Finalizer should be protected, not public</u>
Sec 6	<u>MS: May expose internal static state by storing a mutable object into a static field</u>
Sec 7	<u>MS: Field isn't final and can't be protected from malicious code</u>
Sec 8	<u>MS: Public static method may expose internal representation by returning array</u>
Sec 9	<u>MS: Field should be both final and package protected</u>
Sec 10	<u>MS: Field is a mutable array</u>
Sec 11	<u>MS: Field is a mutable Hashtable</u>
Sec 12	<u>MS: Field should be moved out of an interface and made package protected</u>
Sec 13	<u>MS: Field should be package protected</u>
Sec 14	<u>MS: Field isn't final but should be</u>
Sec 15	<u>MS: Field isn't final but should be refactored to be so</u>
Sec 16	<u>Dm: Hardcoded constant database password</u>
Sec 17	<u>Dm: Empty database password</u>
Sec 18	<u>HRS: HTTP cookie formed from untrusted input</u>
Sec 19	<u>HRS: HTTP Response splitting vulnerability</u>
Sec 20	<u>PT: Absolute path traversal in servlet</u>
Sec 21	<u>PT: Relative path traversal in servlet</u>
Sec 22	<u>SQL: Nonconstant string passed to execute method on an SQL statement</u>
Sec 23	<u>SQL: A prepared statement is generated from a nonconstant String</u>
Sec 24	<u>XSS: JSP reflected cross site scripting vulnerability</u>
Sec 25	<u>XSS: Servlet reflected cross site scripting vulnerability in error page</u>
Sec 26	<u>XSS: Servlet reflected cross site scripting vulnerability</u>