

Vulnerability

₩ Bug

"@SpringBootApplication" and

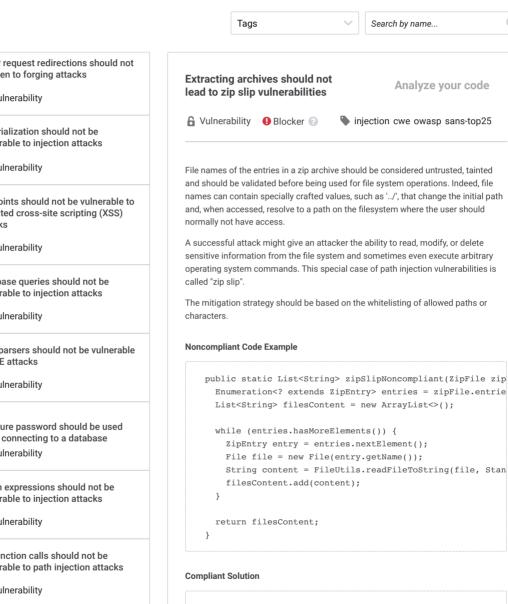
used in the default package

"@ComponentScan" should not be

Java static code analysis

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

Security Hotspot	36	Code Smell	389)	0	Quick Fix	42)
------------------	----	---------------	------	---	--------------	-------------



```
public static List<String> zipSlipCompliant(ZipFile zipFil
 Enumeration<? extends ZipEntry> entries = zipFile.entrie
 List<String> filesContent = new ArrayList<>();
 while (entries.hasMoreElements()) {
   ZipEntry entry = entries.nextElement();
    File file = new File(entry.getName());
    String canonicalDestinationPath = file.getCanonicalPat
    if (!canonicalDestinationPath.startsWith(targetDirecto
      throw new IOException("Entry is outside of the targe
    String content = FileUtils.readFileToString(file, Stan
    filesContent.add(content);
```

"@Controller" classes that use
"@SessionAttributes" must call
"setComplete" on their
"SessionStatus" objects



"wait" should not be called when multiple locks are held



"PreparedStatement" and "ResultSet" methods should be called with valid indices



Files opened in append mode should not be used with ObjectOutputStream

return filesContent;
}

See

- OWASP Top 10 2021 Category A1 Broken Access Control
- OWASP Top 10 2021 Category A3 Injection
- OWASP Top 10 2017 Category A1 Injection
- snyk Zip Slip Vulnerability
- MITRE, CWE-20 Improper Input Validation
- MITRE, CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- MITRE, CWE-99 Improper Control of Resource Identifiers ('Resource Injection')
- MITRE, CWE-641 Improper Restriction of Names for Files and Other Resources
- SANS Top 25 Risky Resource Management

Available In:

sonarcloud 🚷 | sonarqube | Developer Edition

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved.

Privacy Policy