- Secrets
- ABAP
- Apex
- C
- C++
- CloudFormation
- COBOL
- C#
- CSS
- Flex
- Go
- HTML
- Java
- JavaScript
- Kotlin
- Kubernetes
- Objective C
- PHP
- PL/I
- PL/SQL
- Python
- RPG
- Ruby
- Scala
- Swift
- Terraform
- Text
- TypeScript
- T-SQL
- VB.NET
- VB6
- XML

<XML/>

XML static code analysis

Unique rules to find Bugs and Code Smells in your XML code

All rules 36 | Vulnerability 6 | Bug 5 | Security Hotspot 9 | Code Smell 16

Tags | Search by name...

- Defined filters should be used
  Vulnerability
- Basic authentication should not be used
  Vulnerability
- Hibernate should not update database schemas
  Bug
- Dependencies should not have "system" scope
  Bug
- XML files containing a prolog header should start with "<?xml" characters
  Bug
- Using clear-text protocols is security-sensitive
  Security Hotspot
- Receiving intents is security-sensitive
  Security Hotspot
- Restrict access to exported components with appropriate permissions
  Vulnerability
- "DefaultMessageListenerContainer" instances should not drop messages during restarts
  Bug
- "SingleConnectionFactory" instances should be set to "reconnectOnException"
  Bug
- Defining a single permission for read and write access of Content Providers is security-sensitive
  Security Hotspot
- Allowing application backup is security-sensitive
  Security Hotspot
- Requesting dangerous Android permissions is security-

Defined filters should be used

Analyze your code

Vulnerability | Critical | owasp

Every filter defined in `web.xml` file should be used in a `<filter-mapping>` element. Otherwise such filters are not invoked.

Noncompliant Code Example

```
<filter>
   <filter-name>DefinedNotUsed</filter-name>
   <filter-class>com.myco.servlet.ValidationFilter</filter-class>
</filter>
```

Compliant Solution

```
<filter>
   <filter-name>ValidationFilter</filter-name>
   <filter-class>com.myco.servlet.ValidationFilter</filter-class>
</filter>

<filter-mapping>
   <filter-name>ValidationFilter</filter-name>
   <url-pattern>/*</url-pattern>
</filter-mapping>
```

See

- OWASP Top 10 2021 Category A5 - Security Misconfiguration
- OWASP Top 10 2017 Category A6 - Security Misconfiguration

Available In:

sonarlint | sonarcloud | sonarqube