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

Tags | Search by name...

Setting JavaBean properties is security-sensitive
Security Hotspot

Disabling CSRF protections is security-sensitive
Security Hotspot

Using non-standard cryptographic algorithms is security-sensitive
Security Hotspot

Using pseudorandom number generators (PRNGs) is security-sensitive
Security Hotspot

Mocking all non-private methods of a class should be avoided
Code Smell

Empty lines should not be tested with regex MULTILINE flag
Code Smell

Methods setUp() and tearDown() should be correctly annotated starting with JUnit4
Code Smell

Class members annotated with "@VisibleForTesting" should not be accessed from production code
Code Smell

"String#replace" should be preferred to "String#replaceAll"
Code Smell

Derived exceptions should not hide their parents' catch blocks
Code Smell

String offset-based methods should be preferred for finding substrings from offsets
Code Smell

"HttpSecurity" URL patterns should be correctly ordered

Analyze your code

Vulnerability | Critical | spring owasp

URL patterns configured on a `HttpSecurity.authorizeRequests()` method are considered in the order they were declared. It's easy to make a mistake and declare a less restrictive configuration before a more restrictive one. Therefore, it's required to review the order of the "antMatchers" declarations. The `/**` one should be the last one if it is declared.

This rule raises an issue when:

- A pattern is preceded by another that ends with `**` and has the same beginning. E.g.: `/page*-admin/db/**` is after `/page*-admin/**`
- A pattern without wildcard characters is preceded by another that matches. E.g.: `/page-index/db` is after `/page*/**`

Noncompliant Code Example

```
protected void configure(HttpSecurity http) throws Excepti
  http.authorizeRequests()
    .antMatchers("/resources/**", "/signup", "/about").per
    .antMatchers("/admin/**").hasRole("ADMIN")
    .antMatchers("/admin/login").permitAll() // Noncomplia
    .antMatchers("/**", "/home").permitAll()
    .antMatchers("/db/**").access("hasRole('ADMIN') and ha
    .and().formLogin().loginPage("/login").permitAll().and
}
```

Compliant Solution

```
protected void configure(HttpSecurity http) throws Excepti
  http.authorizeRequests()
    .antMatchers("/resources/**", "/signup", "/about").per
    .antMatchers("/admin/login").permitAll()
    .antMatchers("/admin/**").hasRole("ADMIN") // Complian
    .antMatchers("/db/**").access("hasRole('ADMIN') and ha
    .antMatchers("/**", "/home").permitAll() // Compliant;
    .and().formLogin().loginPage("/login").permitAll().and
}
```

See

- OWASP Top 10 2021 Category A1 - Broken Access Control
- OWASP Top 10 2017 Category A6 - Security Misconfiguration

Available In:
sonarlint sonarcloud sonarqube

"default" clauses should be last

Code Smell

"equals" method parameters should not be marked "@Nonnull"

Code Smell

A conditionally executed single line should be denoted by indentation

Code Smell

Conditionals should start on new lines

Code Smell