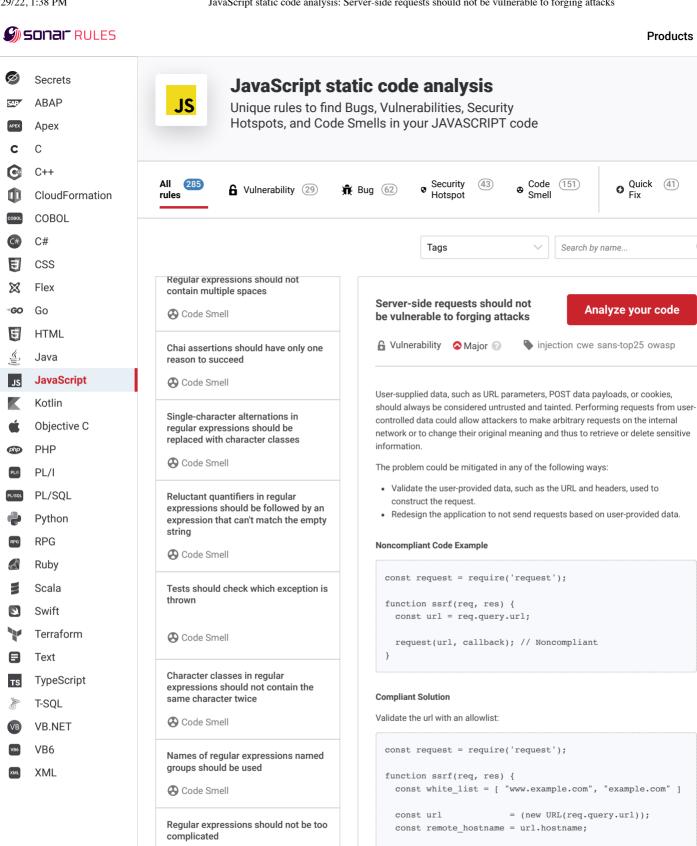
Products >



```
const white_list = [ "www.example.com", "example.com" ]
                       = (new URL(reg.query.url));
 if (white_list.includes(remote_hostname)) {
    request(url, callback);
}
```

See

- OWASP Top 10 2021 Category A10 Server-Side Request Forgery (SSRF)
- OWASP Attack Category Server Side Request Forgery
- OWASP Top 10 2017 Category A5 Broken Access Control
- MITRE, CWE-20 Improper Input Validation
- MITRE, CWE-641 Improper Restriction of Names for Files and Other Resources
- MITRE, CWE-918 Server-Side Request Forgery (SSRF)
- SANS Top 25 Risky Resource Management

Code Smell

Code Smell

Code Smell

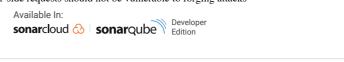
Code Smell

Shorthand promises should be used

Template literals should not be nested

"in" should not be used on arrays

JavaScript static code analysis Assignments should not be redundant
Code Smell
Functions should not have identical implementations
☼ Code Smell
Sparse arrays should not be declared
♦ Code Smell
Array-mutating methods should not be used misleadingly
☼ Code Smell
Collection and array contents should be used



© 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