Code Smell (144)



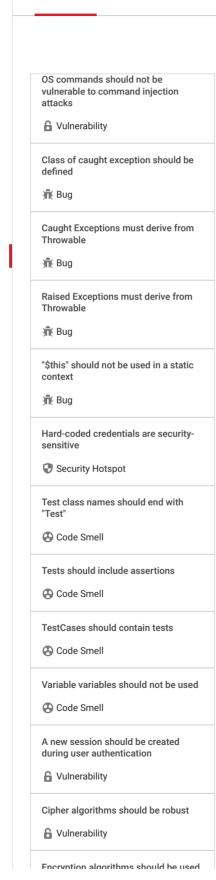
php

All rules (268)



VB₆

XML



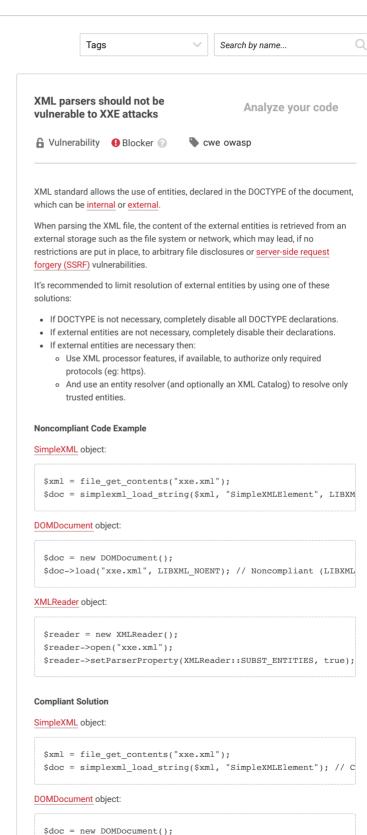
PHP static code analysis

6 Vulnerability 40

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

∰ Bug (51)

Security Hotspot 33



\$doc->load("xxe.xml"); // Compliant (external entities subst

with secure mode and padding scheme

Vulnerability

Server hostnames should be verified during SSL/TLS connections

Vulnerability

Server certificates should be verified during SSL/TLS connections

Vulnerability

LDAP connections should be authenticated

Vulnerability

XMLReader object:

```
$reader = new XMLReader();
$reader->open("xxe.xml");
$reader->setParserProperty(XMLReader::SUBST_ENTITIES, false)
```

See

- OWASP Top 10 2021 Category A5 Security Misconfiguration
- OWASP Top 10 2017 Category A4 XML External Entities (XXE)
- OWASP XXE Prevention Cheat Sheet
- MITRE, CWE-611 Information Exposure Through XML External Entity Reference
- MITRE, CWE-827 Improper Control of Document Type Definition

Available In:

sonarlint ⊖ | sonarcloud 👌 | sonarqube

© 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