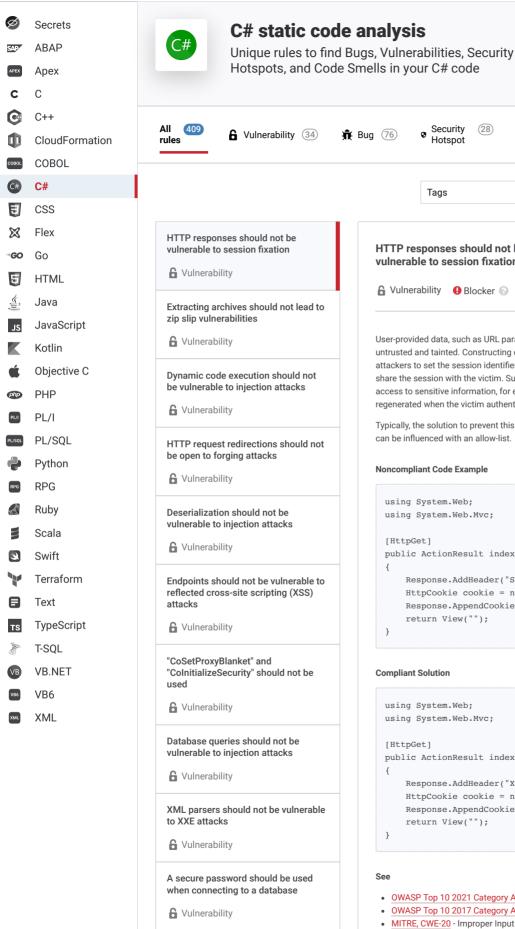
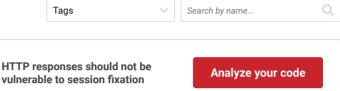
Quick 52 Fix





XPath expressions should not be vulnerable to injection attacks

Vulnerability



injection cwe owasp

⊗ Code Smell

User-provided data, such as URL parameters, should always be considered untrusted and tainted. Constructing cookies directly from tainted data enables attackers to set the session identifier to a known value, allowing the attacker to share the session with the victim. Successful attacks might result in unauthorized access to sensitive information, for example if the session identifier is not regenerated when the victim authenticates.

Typically, the solution to prevent this type of attack is to restrict the cookies that can be influenced with an allow-list.

Noncompliant Code Example

Security

Hotspot

```
using System. Web;
using System.Web.Mvc;
[HttpGet]
public ActionResult index(string val)
    Response.AddHeader("Set-Cookie", val); // Noncompliant
    HttpCookie cookie = new HttpCookie("ASP.NET_SessionId",
    Response.AppendCookie(cookie);
    return View("");
```

Compliant Solution

```
using System.Web;
using System.Web.Mvc;
[HttpGet]
public ActionResult index(string val)
    Response.AddHeader("X-Data", val);
    HttpCookie cookie = new HttpCookie("data", val);
    Response.AppendCookie(cookie);
    return View("");
```

- OWASP Top 10 2021 Category A3 Injection
- OWASP Top 10 2017 Category A1 Injection
- MITRE, CWE-20 Improper Input Validation
- MITRE, CWE-384 Session Fixation

Available In:

Developer sonarcloud 🙆 | sonarqube

I/O function calls should not be vulnerable to path injection attacks Vulnerability
LDAP queries should not be vulnerable to injection attacks Uulnerability
OS commands should not be vulnerable to command injection attacks • Vulnerability
Classes should implement their "ExportAttribute" interfaces

© 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