




 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





JavaScript static code analysis


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


All rules 285

 Vulnerability 29

 Bug 62


 Security Hotspot 43

 Code Smell 151


 Quick Fix 41


Tags ▾

Search by name... 🔍


 Bug


Function parameters, caught exceptions and foreach variables' initial values should not be ignored







Forwarding client IP address is security-sensitive







Allowing confidential information to be logged is security-sensitive







Allowing browsers to perform DNS prefetching is security-sensitive






Disabling Certificate Transparency monitoring is security-sensitive





Disabling Strict-Transport-Security policy is security-sensitive



Disabling strict HTTP no-referrer policy is security-sensitive

Allowing browsers to sniff MIME types is security-sensitive



Disabling content security policy frame-ancestors directive is security-sensitive

Allowing mixed-content is security-sensitive

Disabling content security policy fetch directives is security-sensitive

A "for" loop update clause should move the counter in the right direction

Analyze your code

 Bug  Major ?

A `for` loop with a stop condition that can never be reached, such as one with a counter that moves in the wrong direction, will run infinitely. While there are occasions when an infinite loop is intended, the convention is to construct such loops as `while` loops. More typically, an infinite `for` loop is a bug.




Noncompliant Code Example

```
for (var i = 0; i < strings.length; i--) { // Noncompliant;
  //...
}
```

Compliant Solution

```
for (var i = 0; i < strings.length; i++) {
  //...
}
```




Available In:

 |  | 

© 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](#)

https://rules.sonarsource.com/javascript/RSPEC-2251

1/2

<div>Disabling resource integrity features is security-sensitive</div> <div> Security Hotspot</div>
<div>Disclosing fingerprints from web application technologies is security-sensitive</div> <div> Security Hotspot</div>
<div>Having a permissive Cross-Origin Resource Sharing policy is security-sensitive</div> <div> Security Hotspot</div>
<div>Delivering code in production with debug features activated is security-</div>