




 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 rules285

Vulnerability29

Bug62

Security Hotspot43


Code Smell151

Quick Fix41


Tags ▾

Search by name... 🔍


Repeated patterns in regular expressions should not match the empty string

 Bug


Empty collections should not be accessed or iterated

 Bug


"delete" should be used only with object properties

 Bug


"with" statements should not be used

 Bug


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

 Bug


Forwarding client IP address is security-sensitive

 Security Hotspot


Allowing confidential information to be logged is security-sensitive

 Security Hotspot


Allowing browsers to perform DNS prefetching is security-sensitive

 Security Hotspot


Disabling Certificate Transparency monitoring is security-sensitive

 Security Hotspot

Disabling Strict-Transport-Security policy is security-sensitive




 Security Hotspot

Disabling strict HTTP no-referrer policy is security-sensitive

 Security Hotspot

Properties of variables with "null" or "undefined" values should not be accessed

Analyze your code

 Bug  Major  cwe

When a variable is assigned an undefined or null value, it has no properties. Trying to access properties of such a variable anyway results in a `TypeError`, causing abrupt termination of the script if the error is not caught in a catch block. But instead of catch-ing this condition, it is best to avoid it altogether.




Noncompliant Code Example

```
if (x === undefined) {
  console.log(x.bar); // Noncompliant; TypeError will be thrown
}
```

See

- [MITRE, CWE-476](#) - NULL Pointer Dereference





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-2259

1/2

<div>Allowing browsers to sniff MIME types is security-sensitive</div> <div> Security Hotspot</div>
<div>Disabling content security policy frame-ancestors directive is security-sensitive</div> <div> Security Hotspot</div>
<div>Allowing mixed-content is security-sensitive</div> <div> Security Hotspot</div>
<div>Disabling content security policy fetch directives is security-sensitive</div> <div> Security Hotspot</div>