




 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... 🔍

Object literal shorthand syntax should be used

Code Smell

Strings and non-strings should not be added

Code Smell

Object literal syntax should be used

Code Smell

"undefined" should not be assigned

Code Smell

Trailing commas should not be used

Code Smell

Array constructors should not be used

Code Smell

Quotes for string literals should be used consistently

Code Smell

Statements should end with semicolons

Code Smell

Comments should not be located at the end of lines of code

Code Smell

Loops should not contain more than a single "break" or "continue" statement

Code Smell

Variable, property and parameter names should comply with a naming convention

Code Smell

Lines should not end with trailing whitespaces

Code Smell

Forwarding client IP address is security-sensitive

Analyze your code

Security Hotspot

Minor ?

privacy express.js owasp

Users often connect to web servers through HTTP proxies.

Proxy can be configured to forward the client IP address via the x-Forwarded-For or Forwarded HTTP headers.

IP address is a personal information which can identify a single user and thus impact his privacy.

Ask Yourself Whether

- The web application uses reverse proxies or similar but doesn't need to know the IP address of the user.

There is a risk if you answered yes to this question.

Recommended Secure Coding Practices

User IP address should not be forwarded unless the application needs it, as part of an authentication, authorization scheme or log management for examples.

Sensitive Code Example

```
node-http-proxy

var httpProxy = require('http-proxy');

httpProxy.createProxyServer({target: 'http://localhost:9000',
    .listen(8000);

http-proxy-middleware

var express = require('express');

const { createProxyMiddleware } = require('http-proxy-middle

const app = express();

app.use('/proxy', createProxyMiddleware({ target: 'http://lo
app.listen(3000);

Compliant Solution





node-http-proxy

var httpProxy = require('http-proxy');

// By default xfdw option is false
httpProxy.createProxyServer({target: 'http://localhost:9000'}
    .listen(8000);
```

https://rules.sonarsource.com/javascript/RSPEC-5759

1/2

Files should contain an empty newlne at the end
 Code Smell
An open curly brace should be located at the end of a line
 Code Smell
Tabulation characters should not be used
 Code Smell
Function and method names should comply with a naming convention
 Code Smell

[http-proxy-middleware](#)

```
var express = require('express');

const { createProxyMiddleware } = require('http-proxy-middle

const app = express();

// By default xfwd option is false
app.use('/proxy', createProxyMiddleware({ target: 'http://lo
app.listen(3000);
```

See

- [OWASP Top 10 2021 Category A5](#) - Security Misconfiguration
- [OWASP Top 10 2017 Category A3](#) - Sensitive Data Exposure
- [developer.mozilla.org](#) - X-Forwarded-For

Available In:

