




 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... 🔍


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

 Bug


Return values from functions without side effects should not be ignored

 Bug


Special identifiers should not be bound or assigned

 Bug


Values should not be uselessly incremented

 Bug


Related "if/else if" statements should not have the same condition

 Bug


Objects should not be created to be dropped immediately without being used

 Bug


Identical expressions should not be used on both sides of a binary operator

 Bug


All code should be reachable

 Bug


Loops with at most one iteration should be refactored

 Bug


Variables should not be self-assigned

 Bug

Function argument names should be unique


 Bug


Property names should not be duplicated within a class or object


 Bug

Disabling CSRF protections is security-sensitive

Analyze your code

 Security Hotspot

 Critical

 cwe sans-top25 owasp express.js

A cross-site request forgery (CSRF) attack occurs when a trusted user of a web application can be forced, by an attacker, to perform sensitive actions that he didn't intend, such as updating his profile or sending a message, more generally anything that can change the state of the application.

The attacker can trick the user/victim to click on a link, corresponding to the privileged action, or to visit a malicious web site that embeds a hidden web request and as web browsers automatically include cookies, the actions can be authenticated and sensitive.

Ask Yourself Whether

- The web application uses cookies to authenticate users.
- There exist sensitive operations in the web application that can be performed when the user is authenticated.
- The state / resources of the web application can be modified by doing HTTP POST or HTTP DELETE requests for example.

There is a risk if you answered yes to any of those questions.

Recommended Secure Coding Practices

- Protection against CSRF attacks is strongly recommended:
 - to be activated by default for all [unsafe HTTP methods](#).
 - implemented, for example, with an unguessable CSRF token
- Of course all sensitive operations should not be performed with [safe HTTP](#) methods like GET which are designed to be used only for information retrieval.

Sensitive Code Example

[Express.js CSURF middleware](#) protection is not found on an unsafe HTTP method like POST method:

```
let csrf = require('csrf');
let express = require('express');

let csrfProtection = csrf({ cookie: true });

let app = express();





// Sensitive: this operation doesn't look like protected by app.post('/money_transfer', parseForm, function (req, res) {
res.send('Money transferred');
});
```

Protection provided by [Express.js CSURF middleware](#) is globally disabled on unsafe methods:

```
let csrf = require('csrf');
let express = require('express');
```

https://rules.sonarsource.com/javascript/RSPEC-4502

1/2

literal
 Bug
Bitwise operators should not be used in boolean contexts
 Bug
Constructing arguments of system commands from user input is security-sensitive
 Security Hotspot
Allowing requests with excessive content length is security-sensitive
 Security Hotspot

```
app.use(csrf({ cookie: true, ignoreMethods: ["POST", "GET"]
```

Compliant Solution

[Express.js CSRF middleware](#) protection is used on unsafe methods:

```
let csrf = require('csrf');
let express = require('express');

let csrfProtection = csrf({ cookie: true });

let app = express();

app.post('/money_transfer', parseForm, csrfProtection, function (req, res) {
  res.send('Money transferred')
});
```

Protection provided by [Express.js CSRF middleware](#) is enabled on unsafe methods:

```
let csrf = require('csrf');
let express = require('express');

app.use(csrf({ cookie: true, ignoreMethods: ["GET"] })); //
```

See

- [OWASP Top 10 2021 Category A1](#) - Broken Access Control
- [MITRE, CWE-352](#) - Cross-Site Request Forgery (CSRF)
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration
- [OWASP: Cross-Site Request Forgery](#)
- [SANS Top 25](#) - Insecure Interaction Between Components

Available In:

