




 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



TypeScript static code analysis

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

All rules279

Vulnerability27

Bug51

Security Hotspot43

Code Smell158

Quick Fix50

Tags ▾

Search by name... 🔍

Code Smell

Primitive types should be omitted from initialized or defaulted declarations

Code Smell

Code Smell

Non-null assertions should not be used

Code Smell

Code Smell

"undefined" should not be assigned

Code Smell

Code Smell

Trailing commas should not be used

Code Smell

Code Smell

Array constructors should not be used

Code Smell

Code Smell

Quotes for string literals should be used consistently

Code Smell

Code Smell

Statements should end with semicolons

Code Smell

Code Smell

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

Code Smell

Code Smell

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

Code Smell

Code Smell

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

Code Smell

Code Smell

Lines should not end with trailing whitespaces

Code Smell

Allowing browsers to perform DNS prefetching is security-sensitive

Analyze your code

Security Hotspot

Minor ?

privacy express.js owasp

By default, web browsers perform **DNS prefetching** to reduce latency due to DNS resolutions required when an user clicks links from a website page.

For instance on example.com the hyperlink below contains a cross-origin domain name that must be resolved to an IP address by the web browser:

```
<a href="https://otherexample.com">go on our partner website
```

It can add significant latency during requests, especially if the page contains many links to cross-origin domains. DNS prefetch allows web browsers to perform DNS resolving in the background before the user clicks a link. This feature can cause privacy issues because DNS resolving from the user's computer is performed without his consent if he doesn't intent to go to the linked website.

On a complex private webpage, a combination "of unique links/DNS resolutions" can indicate, to a eavesdropper for instance, that the user is visiting the private page.

Ask Yourself Whether

- Links to cross-origin domains could result in leakage of confidential information about the user's navigation/behavior of the website.

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

Recommended Secure Coding Practices

Implement **X-DNS-Prefetch-Control** header with an *off* value but this could significantly degrade website performances.

Sensitive Code Example

In Express.js application the code is sensitive if the **dns-prefetch-control** middleware is disabled or used without the recommended value:

```
const express = require('express');
const helmet = require('helmet');

let app = express();

app.use(
  helmet.dnsPrefetchControl({
    allow: true // Sensitive: allowing DNS prefetching is se
  })
);
```


Compliant Solution

In Express.js application the **dns-prefetch-control** or **helmet** middleware is the standard way to implement X-DNS-Prefetch-Control header:


https://rules.sonarsource.com/typescript/RSPEC-5743

1/2


Files should contain an empty newline 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

```
const express = require('express');
const helmet = require('helmet');

let app = express();


app.use(
  helmet.dnsPrefetchControl({
    allow: false // Compliant
  })
);
```

See

- [OWASP Top 10 2021 Category A5](#) - Security Misconfiguration
- [OWASP Top 10 2017 Category A3](#) - Sensitive Data Exposure
- [developer.mozilla.org](#) - X-DNS-Prefetch-Control
- [developer.mozilla.org](#) - Using dns-prefetch

Available In:

sonarcloud



sonarqube

