snyk
API & Web
Dashboard
Discovery
Targets
Findings
Scans
Settings
Help
Wallace
Getting started

Targets > cd bougainvillea > Missing Content Security Policy header

L Missing Content Security Policy header Not fixed

cd bougainvillea | https://cdbougainvillea.netlify.app/

Overview
How To Fix
Evidence
Request And Response
Log

SECURITY INFORMATION

Severity Low

Last found Jul. 24 at 17:53

CVSS score 3.7

CVSS vector CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Compliance PCI-DSS OWASP ISO 27001

Labels

SCAN

Path https://cdbougainvillea.netlify.app/

Method GET

Parameter N/A

STATUS

State Not fixed

Assignee

DESCRIPTION

The Content Security Policy (CSP) is an HTTP header through which site owners define a set of security rules that the browser must follow when rendering their site. The most common usage is to define a list of approved sources of content that the browser can load. This can be used to effectively mitigate Cross-Site Scripting (XSS) and Clickjacking attacks.

CSP is flexible enough for you to define from where the browser can load JavaScript, Stylesheets, images, or fonts, among other options. It can also be used in report mode only, a recommended approach before deploying strict rules in a live environment. However, please note that report mode does not protect you, it just logs policy violations.