huntr

Insertion of Sensitive Information Into Debugging Code in microweber/microweber

0

✓ Valid Reported on Feb 20th 2022

Description

Laravel debug mode exposes sensitive data, eg: internal source codes, stack traces, sql queries, databases names, tables names, user's cookies, email, phone number, username, laravel version, php version, etc

Proof of Concept

Login into http://demo.microweber.org
Navigate to this endpoint(including single quote at the end):
http://demo.microweber.org/demo/admin/category/create'
you will see all the exposed information.

Impact

Server running in debug mode, exposing sensitive information about server and user.

CVE
CVE-2022-0721
(Published)

Vulnerability Type
CWE-215: Insertion of Sensitive Information Into Debugging Code

Severity
High (8.8)

Visibility
Public

Status
Fixed

Chat with us

Found by

Damanpreet

@daman-preet-singh

unranked

Fixed by

Bozhidar Slaveykov

@bobimicroweber

maintainer

This report was seen 445 times.

We are processing your report and will contact the **microweber** team within 24 hours.
9 months ago

We have contacted a member of the **microweber** team and are waiting to hear back
9 months ago

Bozhidar Slaveykov validated this vulnerability 9 months ago

Damanpreet has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bozhidar Slaveykov marked this as fixed in **1.3** with commit **b12e1a** 9 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us