Improper Access Control in microweber/microweber

0

Valid Reported on Jan 2nd 2022

Description

Access Controls are used in an application to restrict a user to access only intended functions. If the user is able to access any feature/function which is not allowed by the application and user gets successful in this attempt, then it will be considered as broken access control vulnerability. In this vulnerability, the normal user (i.e. not admin) is able to steal sensitive information of other users like `laraval_session` auth cookie, cart orders, order payment details, user email, user address and much more.

Proof of Concept

1 Create an account as a normal user and visit

```
https://demo.microweber.org/demo/api/users/export_my_data?user_id=1
```

NOTE: In above url, keep replacing the `user_id` to other numbers like 2, 3 and so on.. to get other users information.

Impact

Attacker can steal sensitive information of other users like `laraval_session` auth cookie, cart orders, order payment details, user email, user address and much more.

Occurrences

api.php L12-L46

CVE
CVE-2022-0277
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

Rohan Sharma
@r0hansh
unranked

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 374 times.

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

Rohan Sharma submitted a patch a year ago

Rohan Sharma submitted a patch a year ago

Rohan Sharma a year ago Researcher

Submitted the updated patch.
Earlier, I was accessing logged-in user's user_id via `mw()->user_manager->id()` , but now accessing it via `user_id()` function

We have contacted a member of the **microweber** team and are waiting to

We have sent a follow up to the **microweber** team. We will try again in 7 days. a year ago

We have sent a follow up to the **microweber** team. We will try again in 7 days. a year ago

We have sent a second follow up to the **microweber** team. We will try again in 10 days. 10 months ago

Bozhidar 10 months ago Maintainer

its fixed

Peter Ivanov validated this vulnerability 10 months ago

Rohan Sharma has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Peter Ivanov marked this as fixed in **1.2.11** with commit **e680e1** 10 months ago

Peter Ivanov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

api.php#L12-L46 has been validated ✔

Bozhidar 10 months ago Maintainer

https://github.com/microweber/microweber/commit/e17f3e94289b2dac7187e8039e1a3429779e273c

Sign in to join this conversation