User Enumeration in kareadita/kavita

1

Valid Reported on Oct 26th 2022

Description

The migrate-email endpoint is requiring Email, Username, and Password parameter. The Username parameter value will be queried to _userManager.Users and will returning data to user variable, if user variable contain null value, the application will return bad request with "Invalid username" message, which is similar to user doesn't exist message.
This bad request message can be used for user enumeration, with the asumption if an Username parameter value using the valid username, the backend will returing the different message.

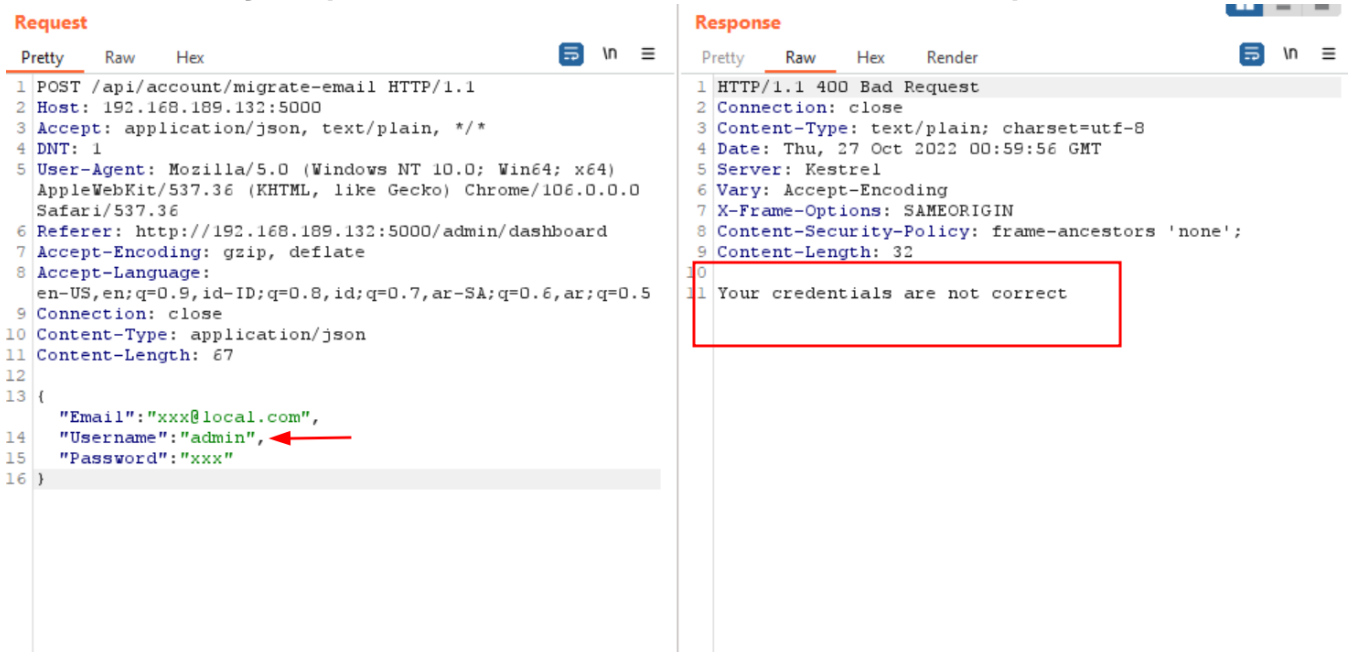
Proof of Concept

1. Send a request with the following parameter :

- Email parameter with any email value
- Username parameter with any value
- Password parameter with any value

2. The backend will response "Invalid username"

3. An then, try to put the valid Username on Username parameter.



4. The backend will response "Your credentials are not correct".

Impact

An attacker could perform an bruteforce attack to either guess or confirm valid users in a system.

Occurrences

C# AccountController.cs L881-L887

References

- What Is User Enumeration?

CVE
CVE-2022-3945
(Published)

Vulnerability Type
CWE-307: Improper Restriction of Excessive Authentication Attempts

Severity
Critical (9.4)

Registry
Other

Affected Version
0.6.0.0

Visibility
Public

Status
Fixed

Found by

zetc0de
@zetc0de
legend

This report was seen 471 times.

We are processing your report and will contact the **kareadita/kavita** team within 24 hours.
a month ago

We have contacted a member of the **kareadita/kavita** team and are waiting to hear back
a month ago

A **kareadita/kavita** maintainer has acknowledged this report a month ago

Joe Milazzo validated this vulnerability 25 days ago

zetc0de has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Joe Milazzo marked this as fixed in **0.6.0.3** with commit **f8db37** 25 days ago

The fix bounty has been dropped ✖

This vulnerability has been assigned a CVE ✔

AccountController.cs#L881-L887 has been validated ✔

zetc0de 25 days ago — Researcher

@admin can disclose this report? Also can to assign cve for this vulnerability?

Joe Milazzo 25 days ago — Maintainer

This is not ready for disclosure. I will publish when it is ready.

Joe Milazzo published this vulnerability 15 days ago

Sign in to join this conversation