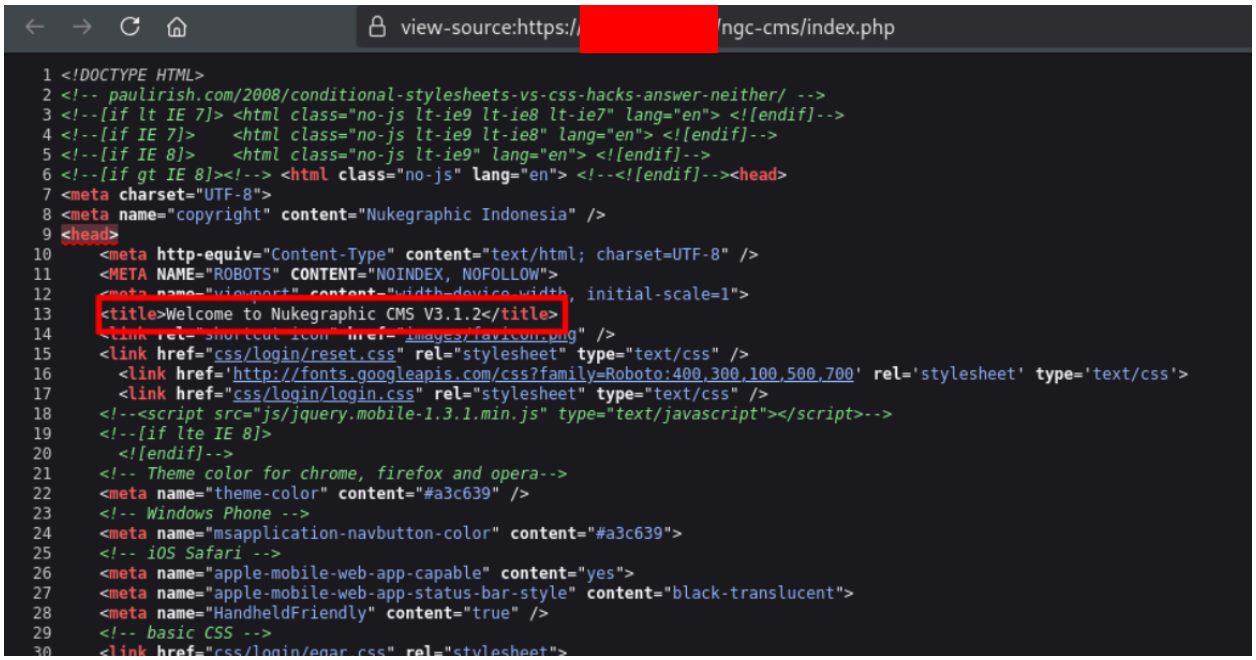
Application Name: Nukegraphic CMS V3.1.2



Vulnerability found by: Carlos Budiman & Nicholas Abraham

Vulnerability 1: Stored Cross Site Scripting at NGC-CMS

Score: 8.1, CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Vulnerability Location: https://target.com/ngc-cms/user-edit-profile.php

Affected URLs: https://target.com/ngc-cms/* (Script loads site-wide)

Description

During testing, the team intercepted the HTTP request generated when a user edits their profile. By modifying this request and inserting a proof-of-concept (PoC) payload into the *name* field, the malicious script was successfully stored in the backend database.

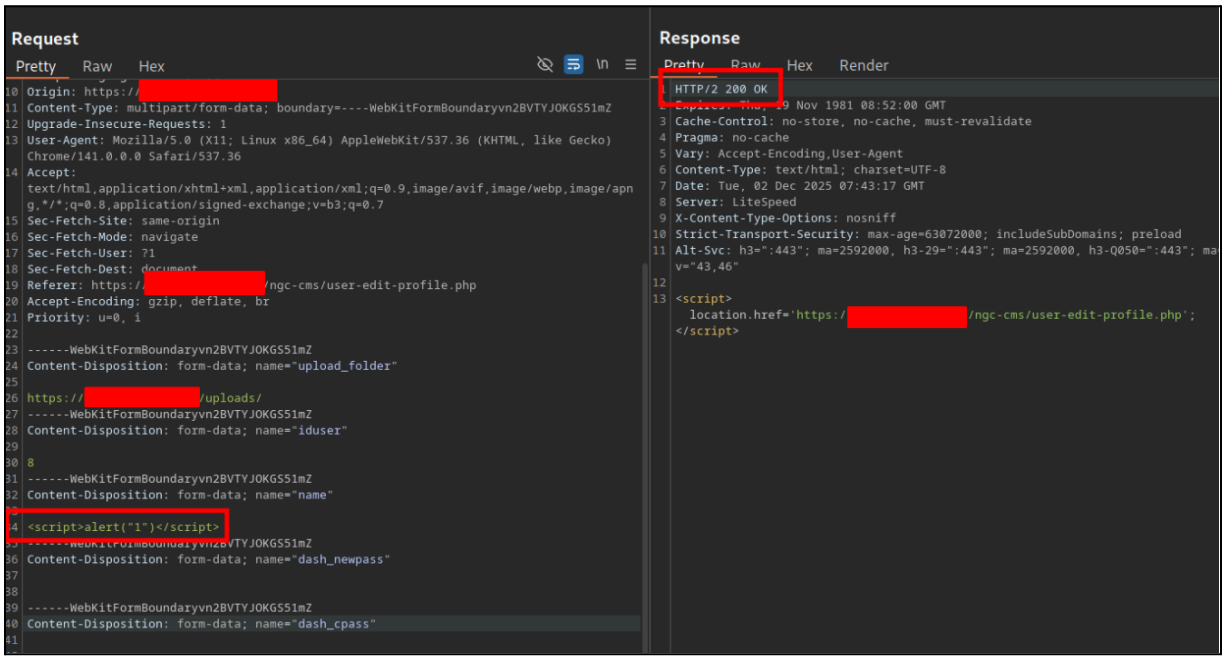
When the CMS later rendered the name value on various pages, the stored JavaScript executed automatically.

This means the XSS payload appeared:

- On the response page after updating the profile.
- On CMS pages where the name is displayed.
- On any other page that renders the affected field.

Proof of Concept

1. Navigate to Edit Profile & capture a valid edit profile request, add the PoC Script and send the PoC POST Request



2. Javascript is executed CMS-wide.