

New issue

Jump to bottom

There is xss in the front desk which can get hazards such as administrator cookies #33

Closed

Jayway007 opened this issue on May 26, 2020 · 1 comment

Jayway007 commented on May 26, 2020

1、Build an environment to simulate users selecting products at the front desk——add to cart——confirm order-pay:

<http://127.0.0.1:28089/shop-cart/settle>

Insert the payload here at the harvest information:

```
<script> alert (document.cookie) ![image](https://user-images.githubusercontent.com/22486282/82964894-369aa900-9ff9-11ea-982e-c1c9960371b5.png) 2、When the administrator logs in to the background, XSS will be triggered when viewing the "View Recipient Information" of this order in the "Order Management Office" ![1111](https://user-images.githubusercontent.com/22486282/82964966-6c3f9200-9ff9-11ea-97aa-b03066d60513.png)
```



Jayway007 closed this as completed on May 26, 2020



Jayway007 reopened this on May 26, 2020

Jayway007 commented on May 26, 2020

Author

Add a screenshot:

① 127.0.0.1:28089/orders/15905408210417075

新蜂商城 | 后台管理系统 | 课程视频 | 文档 | 问题反馈 | GitHub 地址 | 码云Gitee 地址

newbee 新蜂商城 秒杀 优惠券

个人中心

个人信息

我的订单

退出登录

订单详情 请谨防钓鱼链接或诈骗电话, 了解更多>

订单号: 15905408210417075

取消订单

已支付

newbee商城订单确认中~

下单 付款 配送 出库 交易成功

2020-05-27 08:53:41

华为 HUAWEI P30 Pro 5488元 x 1

收货信息

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

支付方式

支付方式: 微信支付

< > 127.0.0.1:28089/admin/orders##

NEWBEE商城

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

系统管理

Dashboard

127.0.0.1:28089 显示

JIDENTITY=c99d7c5a-d1f6-40e4-8715-2d7a20249c7a



确定

订单管理


修改订单 配置完成 出库 关闭订单

订单号	订单总价	订单状态	支付方式	创建时间	操作
15905408210417075	5488	已支付	微信支付	2020-05-27 08:53:41	查看订单信息 查看收件人信息
15905407528653699	999	已支付	微信支付	2020-05-27 08:52:32	查看订单信息 查看收件人信息
15888311492973409	3999	已支付	微信支付	2020-05-07 13:59:09	查看订单信息 查看收件人信息
15702847670935185	3999	已支付	微信支付	2019-10-05 22:12:47	查看订单信息 查看收件人信息
15702783557537865	6819	待支付	无	2019-10-05 20:20:10	查看订单信息 查看收件人信息
15698039249771093	3199	待支付	无	2019-09-30 08:38:26	查看订单信息 查看收件人信息
15694781962831307	1246	手动关闭	微信支付	2019-09-26 14:09:56	查看订单信息 查看收件人信息
15694781962831307	1246	手动关闭	微信支付	2019-09-26 14:09:56	查看订单信息 查看收件人信息

 **newbee-mall** referenced this issue on May 28, 2020

 **newbee-mall** Fixing xss bug. 

ed8016e

 **newbee-mall** closed this as completed on Oct 20, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

