



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information

 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPOIT MANUAL SUBMISSIONS

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:**   / **Cookiebot**
by Usercentrics**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```
# 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
```

Cookiebot
by Usercentrics**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

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

©

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