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

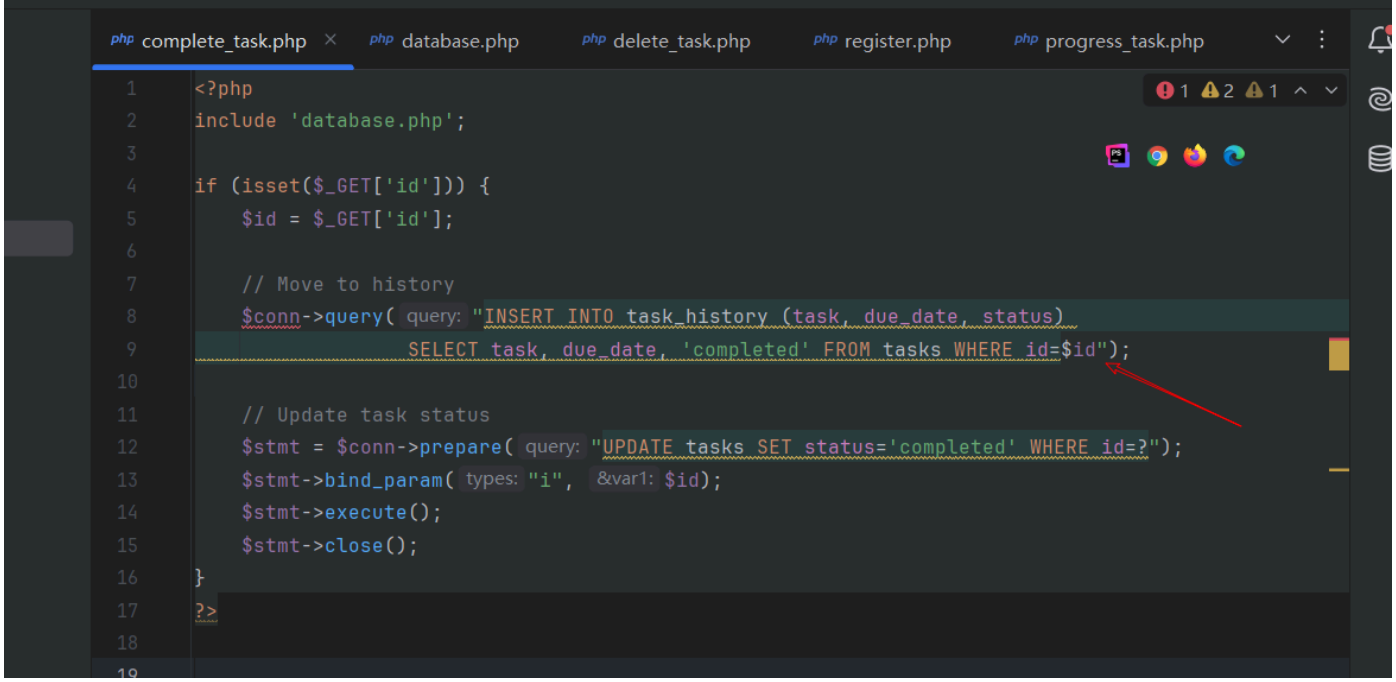
PROBLEM TYPE

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.



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

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