DisguisedRoot / Exploit Public

main

Exploit / Persistent XSS / PoC

DisguisedRoot Update PoC

History

1 contributor

39 lines (27 sloc) | 1 KB

```
# Exploit Title: Purchase Order Management System - Multiple Persistent XSS
# Exploit Author: Kshitij Rewandkar
# Vendor Name: oretnom23
# Vendor Homepage: https://www.sourcecodester.com/php/14935/purchase-order-management-system-using
# Software Link: https://www.sourcecodester.com/php/14935/purchase-order-management-system-using-p
# Version: v1.0
# Tested on: Windows 11, Apache
# CVE: (CVE-2022-3503)


Description:
A Persistent XSS issue in Purchase Order Management System v1.0 allows to inject Arbitrary JavaScr



Parameters Vulnerable:
A) Supplier Name
B) Address
C) Contact person
D) Contact


Payload:
<script>confirm(1)</script>


Steps:

1) Login into your account
2) Now go to "Supplier List" and create a new file.
```

```
3) Now put the payload in the below parameter:

A) Supplier Name
B) Address
C) Contact person
D) Contact

Payload: <script>confirm(1)</script>

4) Now save the details and our payload has been executed
```