##
# Exploit Title: Open-AudIT Professional 2.2.7 - Cross Site Scripting Vulnerability
# Google Dork:NA
##
# Exploit Author: Ranjeet Jaiswal
##
# Vendor Homepage: https://opmantek.com/
# Software Link:https://www.open-audit.org/downloads.php
# Affected Version: 2.2.7
# Category: WebApps
# Tested on: Windows 10
#
#
# 1. Vendor Description:
#
# Network Discovery and Inventory Software | Open-AudIT | Opmantek
Discover what's on your network
Open-AudIT is the world's leading network discovery, inventory and audit program. Used by over 10,000 customers.
#
# 2. Technical Description:
#
# Cross-site scripting (XSS) vulnerability on Orgs Page in Open-AudIT Professional edition in 2.2.7 allows remote attackers to inject arbitrary web script in Orgs name field,as demonstrated in below POC.
#
# 3. Proof Of Concept:

3.1. Proof of Concept for Injecting web script(Cross-site scripting(XSS))

 # #Step to reproduce.
Step1:Login in to Open-AudIT Professional 2.2.7
Step2:Go to Orgs page
Step3:Select any records which are listed
Step4:click on details tab.
Step5:In the Name field put the following payload and click submit.

```
<Script>alert('hack')</script>
```

Step6:Go to export tab and export using HTML Table
Step7:When user open download orgs.html file.Alert Popup will execute.

```
# 4. Solution:
#
# Upgrade to latest release of Open-AudIT version
Please visit below link to get news on latest version of Open-AudIT release.
# https://community.opmantek.com/display/OA/Release+Notes
```