nsparker1337 Add files via upload History

1 contributor

25 lines (18 sloc) | 1.24 KB

Exploit Title: Online Market Place Site v1.0 - Insecure Direct Object Reference(IDOR)

Exploit Author: NS Kumar (n1_x)

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/defa

ult/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 IDOR - Broken Access Control Vulnerability allowing attackers to modify the product that owned by other sellers(vertical privilege escalation).

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

Step 1: Register and login as a seller.

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

Step 3: The id parameter is the vulnerable to insecure direct object reference(idor).

step 4: change the product id that not listed in your product page.

step 5: Now You can edit the product of other sellers.