Devvortex

IP: 10.10.11.242
OS: Ubuntu(Linux)
WEB TECHNOLOGY: Nginx 1.18.0,Joomla
==========
NMAP RESULT:

PORT STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| 256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_ 256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp open http   nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://devvortex.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

==========
ENUMERATION:

Sub-Domain enum → ffuf -u http://devvortex.htb -H "Host: FUZZ.devvortex.htb" -w /usr/share/wordlists/seclists/subdomains-top1million-20000.txt -fs 154
found dev.devvortex.htb

dev.devvortex.htb runs joomla cms
[+] Detecting Joomla Version
[++] Joomla 4.2.6

The Joomla ver is vulnerable to CVE-2023-23752

A ruby exploit exist for the vulnerability and found 2 users and a password

user: logan

user: lewis
"password": "P4ntherg0t1n5r3c0n##"

it was a valid credentials for the administrator page:

then changing the content of index.php(template) to php's reverse shell to get the shell

then accessing the database to get the credentials for “logan”

after cracking the hash the password came up to be : → "tequieromucho"

Priv-Esc:

sudo -l

and found /usr/bin/apport-cli

use it to get root! sudo /usr/bin/apport-cli --file-bug

==========

CREDENTIALS:
Michael
lewis:P4ntherg0t1n5r3c0n##
logan:tequieromucho

==========

USER FLAG: e2cc25f376c1c7bc863d8c27e6d61900
ROOT FLAG:0be88677602678d209ff9c09587e15b0