Joomla

Challenges

writeup: https://www.hackingarticles.in/hack-kevgir-vm-ctf-challenge/

Notes

look for "joomla.xml" file in "/administrator/manifests/files" directory
readable without authenticating to the application.

Get version commands :

curl -s http://fooblog.site/administrator/manifests/files/joomla.xml \ |grep "<version>" | grep -Po "(\d+\.)+\d+"

for i in $(cat **sites.txt**); \
do curl -s **$i**/administrator/manifests/files/joomla.xml \ |grep "<version>" | grep -Po "(\d+\.)+\d+"; done

curl -sSL -D - http://fooblog.site -o /dev/null
curl -sSL -D - http://fooblog.site -o /dev/null |**grep "X-Powered-By"**

Tools:

Joomscan : https://github.com/rezasp/joomscan
joomscan -u http://joomla.site

Jommlascan:
python joomlascan.py -u http://joomla.site/joomla

JoomBrute : https://github.com/0rbz/JoomBrute
python JoomBrute.py --url http://joomla.site/joomla/administrator --username admin --wordlist /usr/share/wordlists/rockyou.txt

Dirsearch :
./dirsearch.py -u http://joomla.site/joomla -e php -x403