Haircut on HackTheBox

Started off with some nmap scans:





Navigating to the website and trying to check robots.txt gives away that the server is running nginx 1.10 

Quick google search shows that this version of nginx is vulnerable to CVE-2021-23017.

A browse + ffuf of the website finds nothing of value other than an image an a forbidden uploads folder.

Decided to use the CVE exploit using <https://github.com/M507/CVE-2021-23017-PoC/blob/main/README.md>, but did not work.

Decided to run dirbuster just as a sanity check, and found some more files: 

Found a little form, so intercepted the request and sent it to burp repeater

Tweaking the values a little got me to this:



The home page could be loaded from an outside IP address rather than the localhost.

So I created a simple html page and hosted it on a python server and uploaded it.

Works!



Page had several php pages running, so decided to test it with php:

Works, but seems to interpret it as html.



Decided to upload an echo ‘test’ to see what would happen:



Wasn’t sure if it was being rendered interpreted or not, so I decided I would put in a time delay to see if it was being executed, and the time delay and inspect-elementing the actual website confirmed that everything was being commented out.

Checked the curl page and found the -o flag might be useful, so decided to write the output to the /uploads folder:

Works AND it slept for 5 seconds!!!! We have execution.



Uploaded a webshell:



Shell!!!!



User flag:



Maria seems to be the only current user on the device after analysing /etc/passwd.

Downloaded linpeas because I can’t find any obvious way to priv esc:



Looks interesting…

A google search finds a priv esc vulnerability in it.

First one didn’t work ☹

Manually compile the C code and uploading it didn’t work ☹



Little nudge from Khalid led me to PwnKit: <https://github.com/ly4k/PwnKit/blob/main/README.md>

WORKED!



ROOOOOOOOOOOOOOOT!!!