Attack path:
For blocky, I conducted an nmap scan and saw that port 21, 22, and 80 were open. I used dirsearch to enumerate the website and saw that there was a web extension /plugins. I downloaded the blockycore class file and using the strings command, saw that there was password. It did not work for user root, but after using wpscans to enumerate the users on the wordpress account, I saw that notch was another potential user. Using the password and username “notch,” I was able to ssh into the machine. I then ran the command sudo -l to check notch’s permissions, and saw that he had root access with command sudo su.