I used gobuster to find links with potential data leaks. While gobuster was running, I also realized that all of the php extensions required that I be logged into pfsense, so I modified the command of gobuster to ‘gobuster dir -u http://10.10.10.60:80 -w /usr/share/.../2.3-common.txt -x .txt,.html -k (the -k is to skip ssl certifications). I found an extension called system-users.txt which contained login credentials with username:rohit and password: company defaults. Company defaults is not the password; the default pfsense password (pfsense) is the password. I saw that the pfsense version was 2.1.3, and found an exploit that worked on versions < 2.1.4 on exploitdb. The exploit worked and I was in with root permissions.