1. Run the kernel image with “qemu” (https://www.qemu.org/) & forward port 80 (guest) to port 3000 (host). The “nographic” flag is used because the QEMU GUI doesn’t not display the BusyBox terminal.
   Command: *qemu-system-mipsel -kernel BootMe_openwrt-malta-le-vmlinux-initramfs.elf -nographic -net nic,model=pcnet -net user,hostfwd=tcp::3000-:80*

```
┌──(kali㉿kali)-[~/Desktop/bootme]
└─$ qemu-system-mipsel -kernel BootMe_openwrt-malta-le-vmlinux-initramfs.elf -nographic -net nic,
model=pcnet -net user,hostfwd=tcp::3000-:80
```

2. If we try to “curl” the forwarded site, we get a “Connection reset by peer error”. This can be fixed by flushing all **iptables** chains.

```
┌──(kali㉿kali)-[~]
└─$ curl http://127.0.0.1:3000
curl: (56) Recv failure: Connection reset by peer
```

```
root@OpenWrt:/# iptables -F
root@OpenWrt:/#
```

3. Now the website is accessible & the website can be visited on localhost with port 3000, to get the flag.