

# Simulating a DoS attack on the Web Server

## Step 1:

Launching a large number of requests to the webserver by running the following from a machine where you can access your host machine (please replace “192.168.56.104” with the IP address of your host machine)

```
ab -n 100000 -c 1000  
'http://192.168.56.104:8000/WebGoat/start.mvc#lesson/SqlInjectionAdvanced.lesson/4'
```

To run the above command, you will need to have “apache2-utils” installed.

## Step 2 (has to run concurrently with Step 1):

While you are launching the DoS attack, you may monitor the network activities in the VM by running the following command (this command will log the requests sent to the webserver on the VM):

```
sudo tcpdump -i any port 8000 -w web.pcap -vn
```

You can stop the monitoring anytime and check the captured contents using the following command:

```
tcpdump -qns 0 -A -r web.pcap
```