Command Injection in DVWA

Everything done on local host: 127.0.0.1

Security: Low

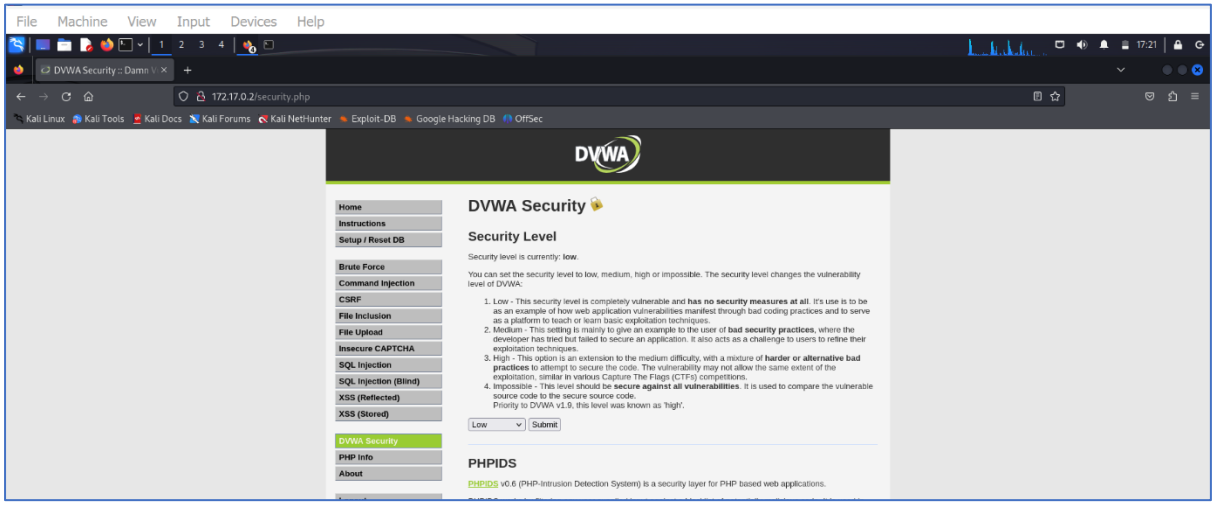
Command Injection:

Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. In this attack, the attacker-supplied operating system commands are usually executed with the privileges of the vulnerable application. Command injection attacks are possible largely due to insufficient input validation.

Command Injection in dvwa process:

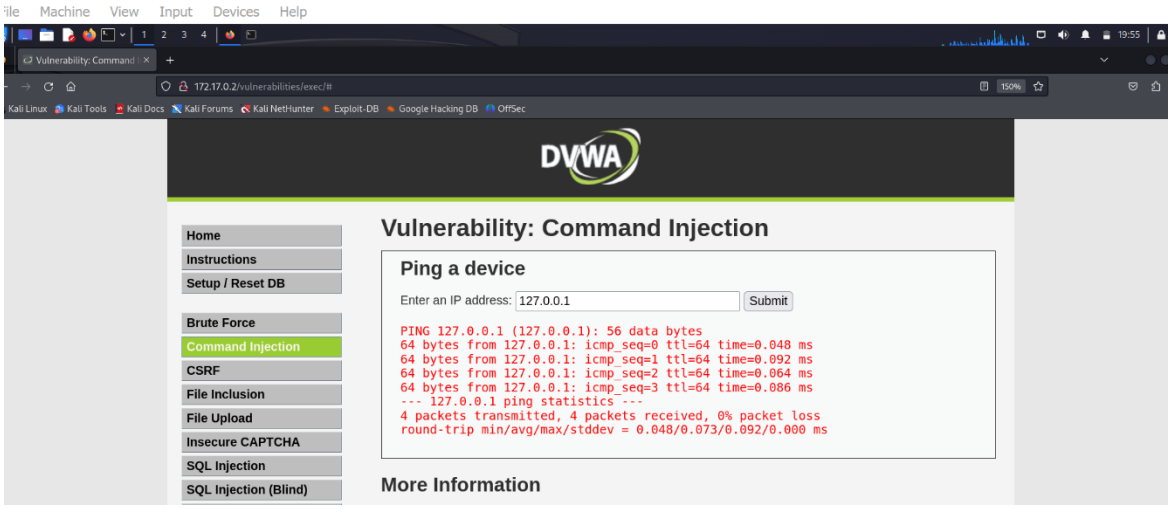
Step 1:

First run the docker command and change the security of dvwa to low after accesing it.



Step 2:

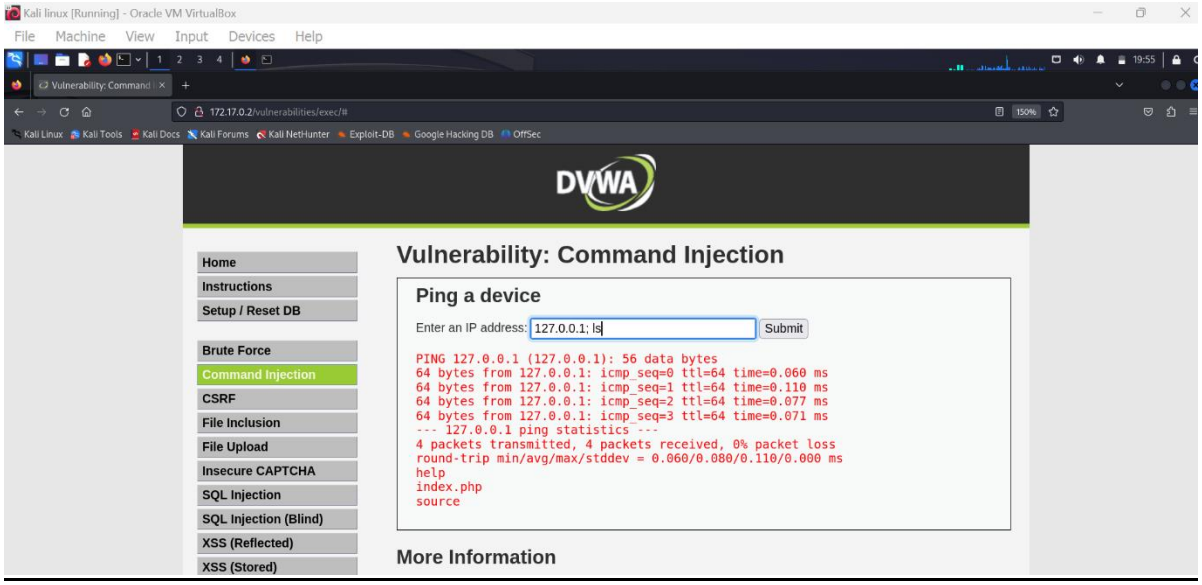
Go to Command Injection and firstly ping the local host: 127.0.0.1



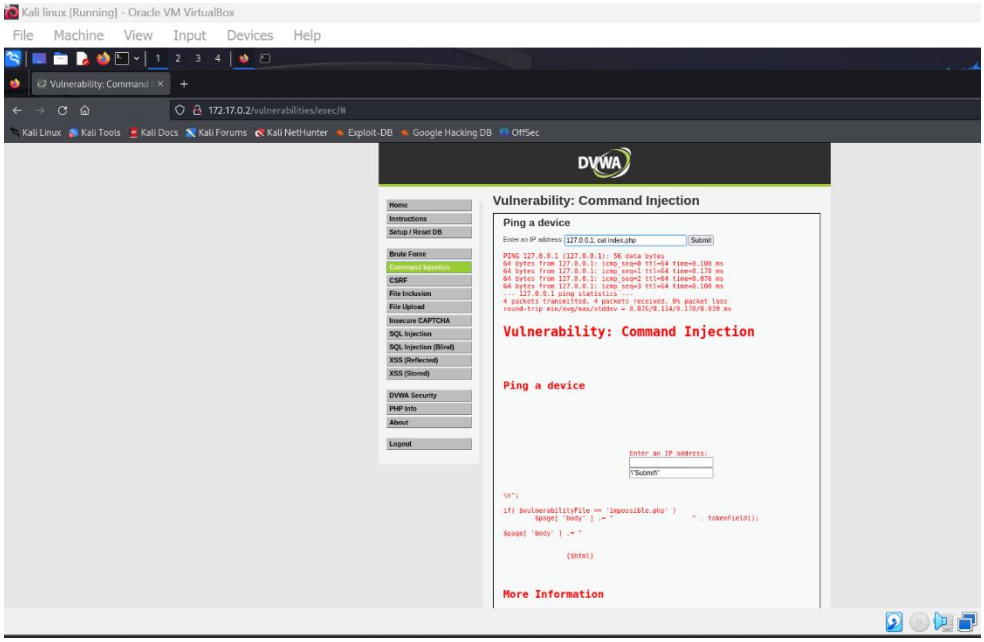
Step 3:

Trying diiferent command injections such as ls, hostname, whoami, cat, etc.

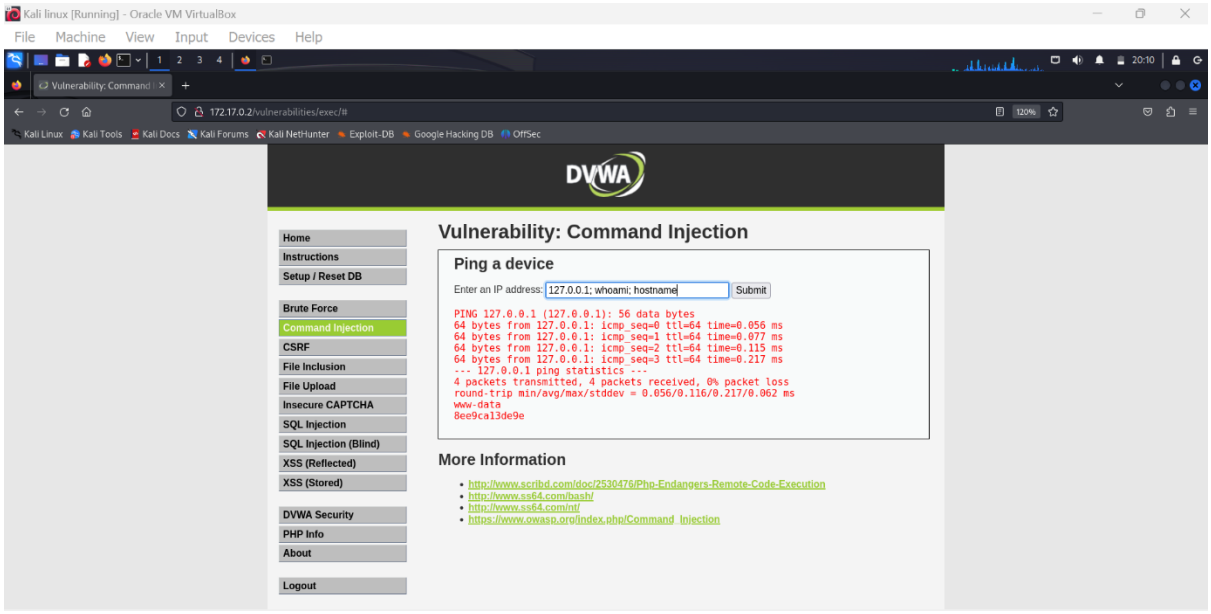
Ls command:



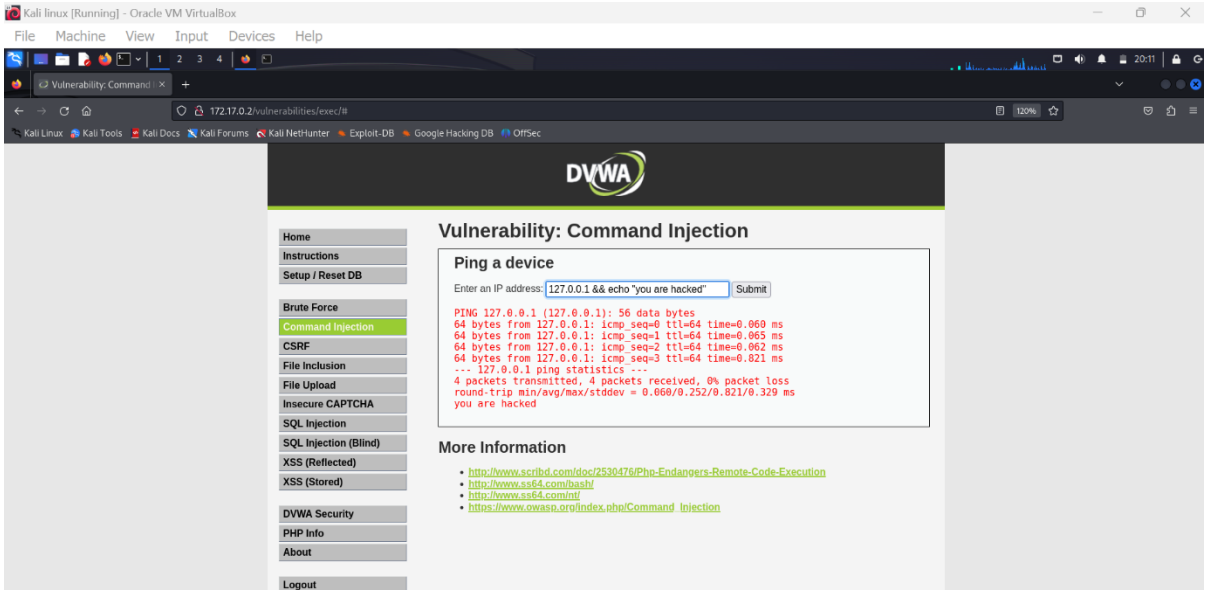
Cat command:



Hostname and whoami command:



Echo command:



RESULT:

Thus completed Command Injection in dvwa at low security.