

The image features a word cloud in the shape of the map of India. The words are arranged to fit the geographical outline. The most prominent words, shown in larger fonts, include "ATTACK", "DEFENSE", "LABS", "COURSES", "PENTESTER ACADEMY", "TOOL BOX", "PENTESTING", "RED TEAM", "HACKER", "TRAINING", "ACCESS POINT", "WORLD-CLASS TRAINERS", "PATV", "TEAM LABS", "PENETESTER", "ATTACKDEFENSE LABS", "COURSES ACCESS POINT PENTESTER", "ACCESS POINT", "WORLD-CLASS TRAINERS", "TRAINING COURSES SPATV ACCESS", "PENTESTER ACADEMY", "ATTACKDEFENSE LABS", "COURSES PENTESTER ACADEMY", "POINT WORLD-CLASS TRAINERS TRAINING HACKER", "TOOL BOX", "HACKER PENTESTING", "RED TEAM LABS", "ATTACKDEFENSE LABS", "COURSES PENTESTER ACADEMY", "PENTESTER ACADEMY ATTACKDEFENSE LABS", "TOOL BOX WORLD-CI", "TRAINING", "PENTESTER ACADEMY", "TOOL BOX", and "PENTESTING". The words "ATTACK" and "DEFENSE" are the largest and are colored red and dark blue respectively, while the others are in various shades of gray. The phrase "by PentesterAcademy" is written in black at the bottom center of the word cloud.

Name	Directory Traversal
URL	https://www.attackdefense.com/challengedetails?cid=2123
Type	OWASP Top 10 : Broken Access Control

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.

Objective: Directory Traversal attack.

Solution:

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

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
12381: eth0@if12382: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.5/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
12384: eth1@if12385: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:96:15:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.150.21.2/24 brd 192.150.21.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Run Nmap scan on the target IP to find open ports.

Note: The target IP will be 192.150.21.3

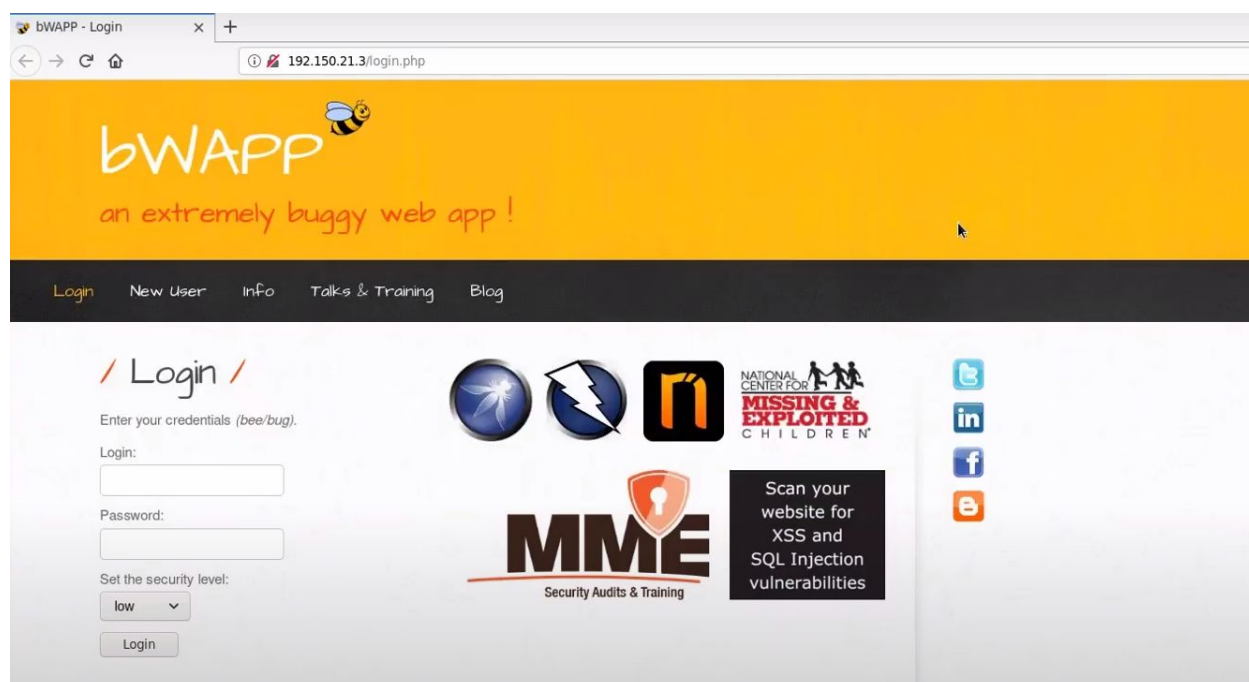
Command: nmap 192.150.21.3

```
root@attackdefense:~# nmap 192.150.21.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-09 11:47 IST
Nmap scan report for target-1 (192.150.21.3)
Host is up (0.000021s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:42:C0:96:15:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
root@attackdefense:~#
```

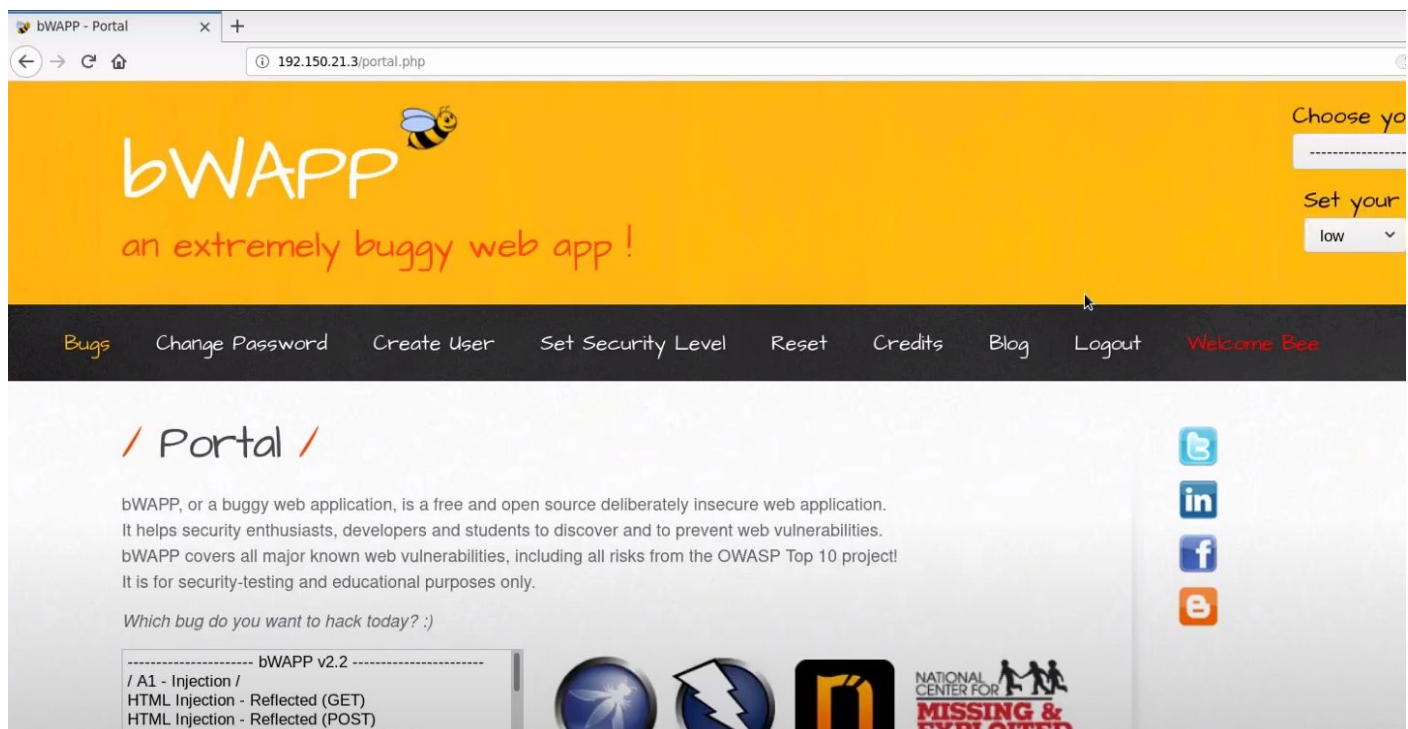
Port 80 and 3306 are open

Step 3: Start firefox and navigate to the target IP.

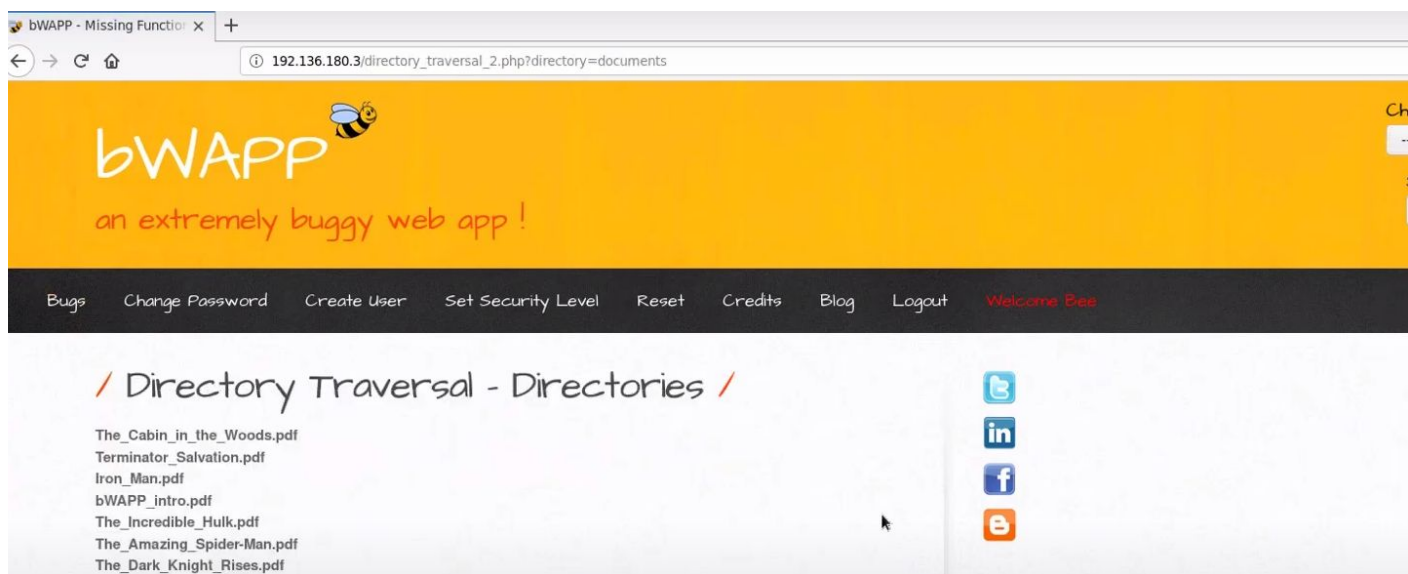


An instance of bWAPP is running at port 80 of the target.

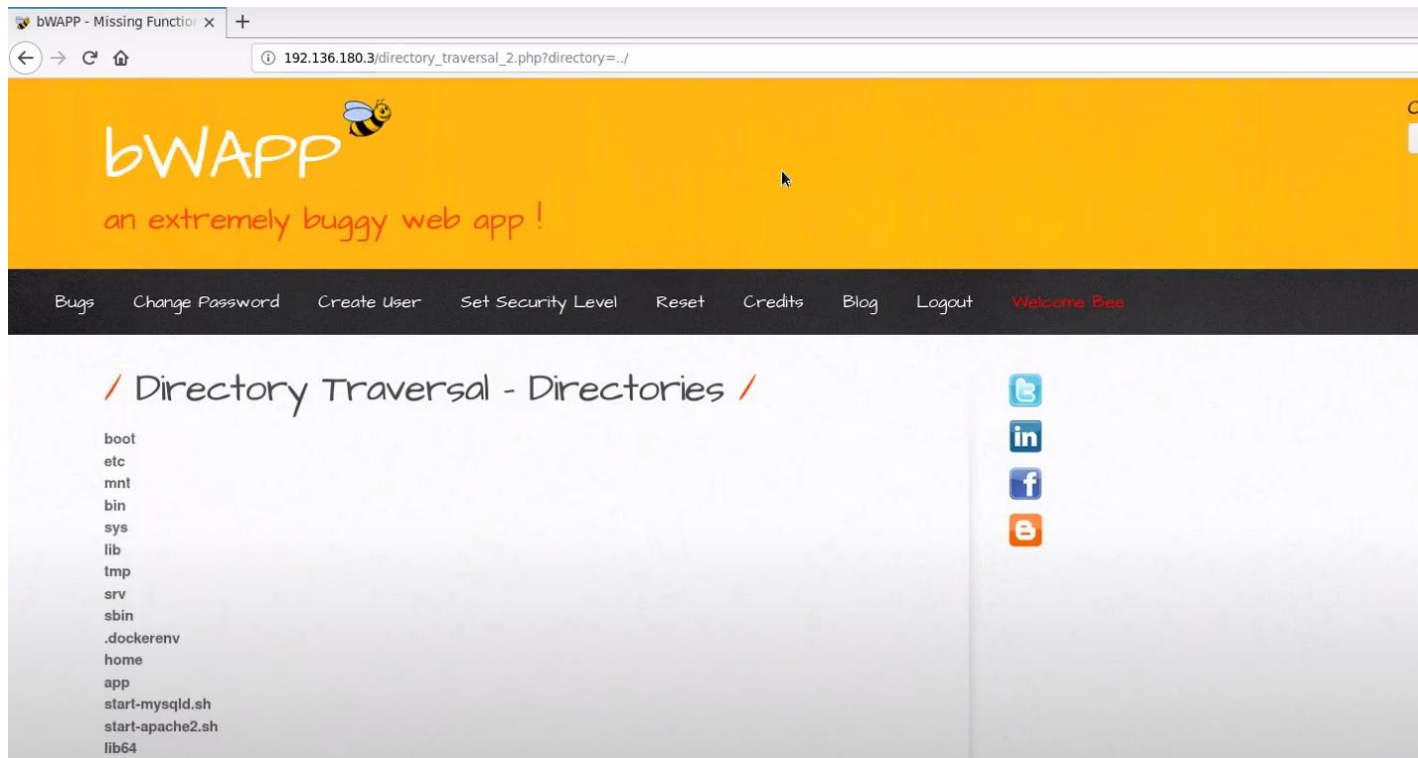
Step 4: Log in to the application using **bee:bug** credentials.



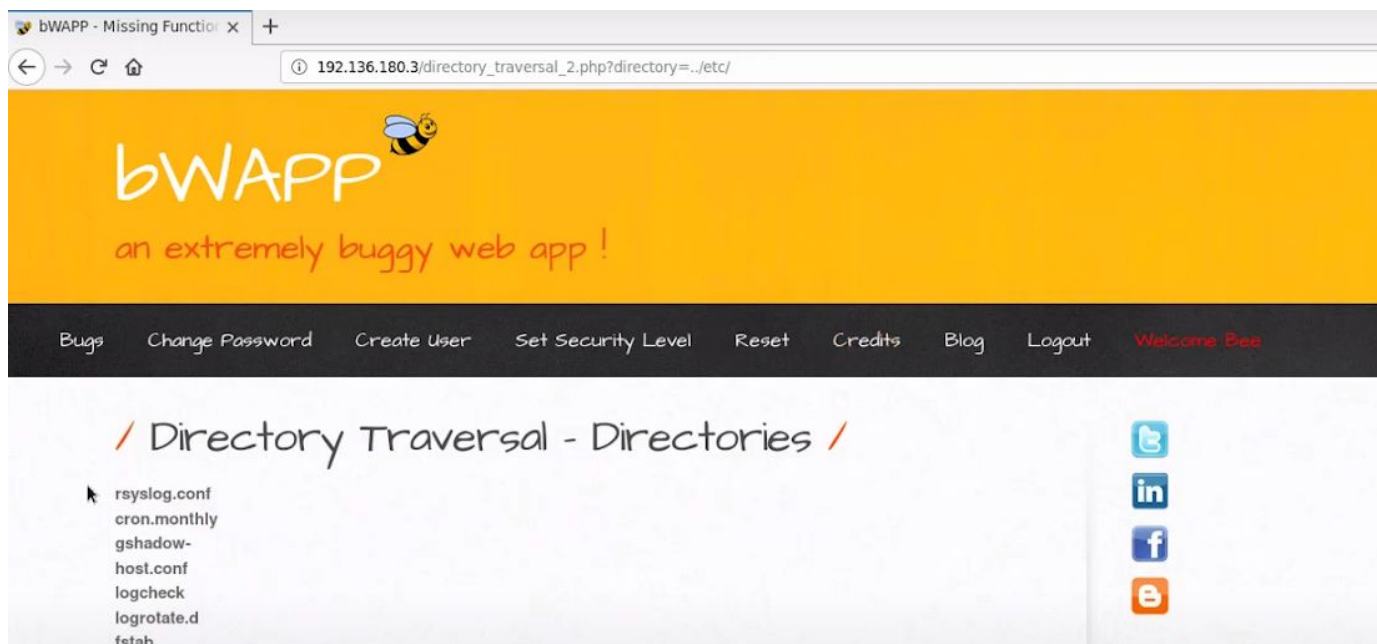
Step 5: From the Choose your bug dropdown, Select “**Directory Traversal - Directories**” exercise. Click on ‘Hack’.




Step 6: Modify the directory parameter and add “../” in the URL



Modify the directory parameter to “../etc/” to display the contents of /etc directory.





The Directory Traversal attack was successful.

References:

1. bWAPP (<http://www.itsecgames.com/>)