ATTACK
DEFENSE

by PentesterAcademy

Name	Improper Session Management
URL	https://attackdefense.com/challengedetails?cid=1899
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: Identifying IP address of the target machine

Command: ip addr

The IP address of the attacker machine is 192.171.105.2. The target machine is located at the IP address 192.171.105.3

**Step 2:** Identify the open ports on the target machine.

Command: nmap 192.171.105.3

```
root@attackdefense:~# nmap 192.171.105.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-03 08:00 IST
Nmap scan report for target-1 (192.171.105.3)
Host is up (0.000020s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 02:42:C0:AB:69:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
root@attackdefense:~#
```

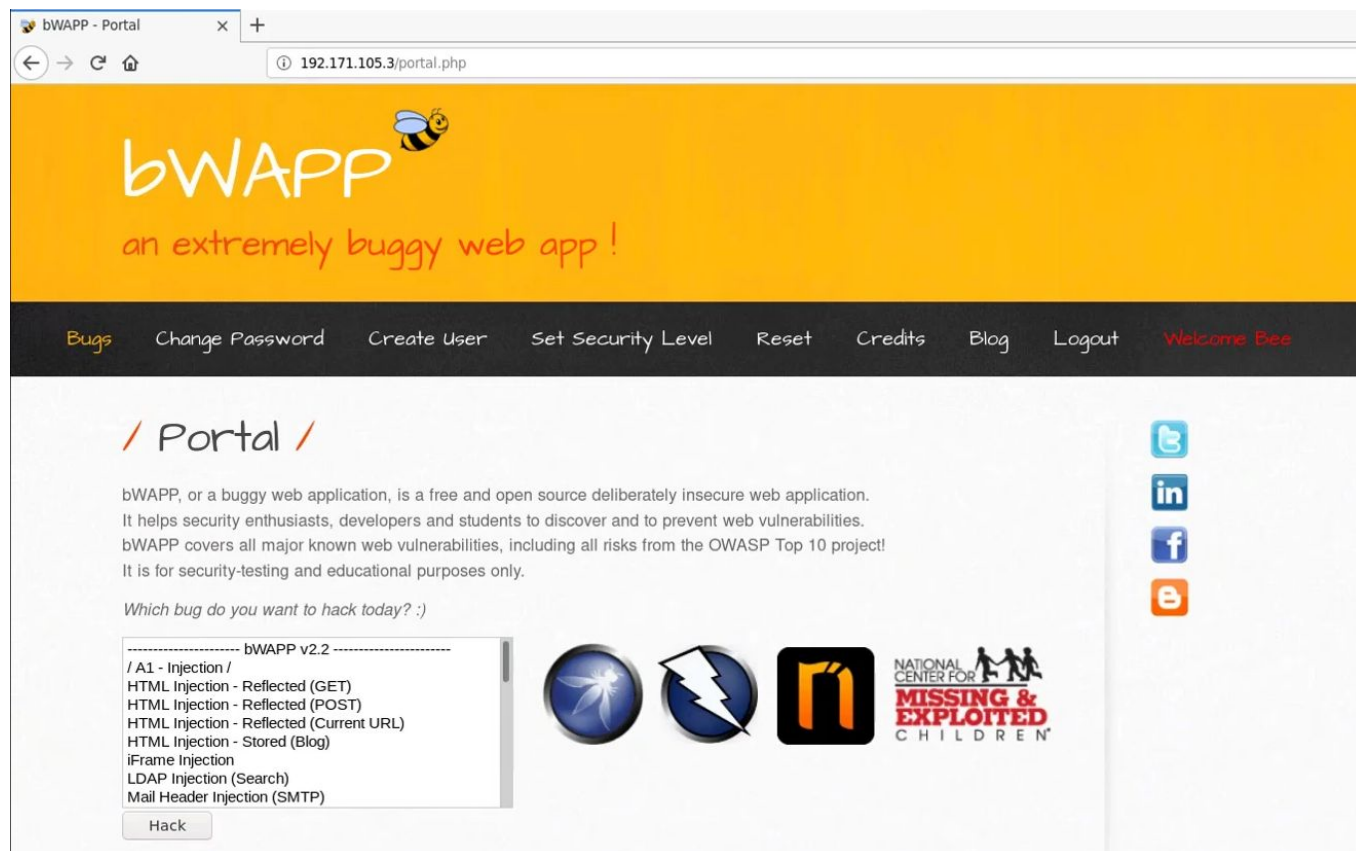Port 80 and 3306 are open on the target machine.

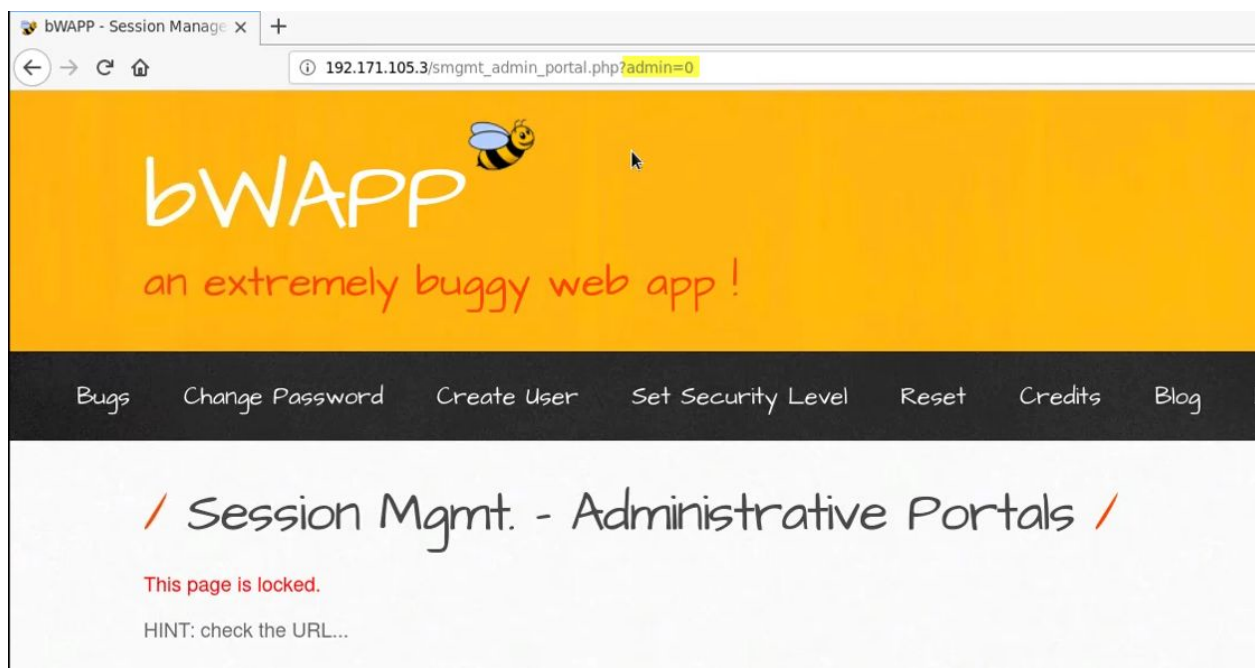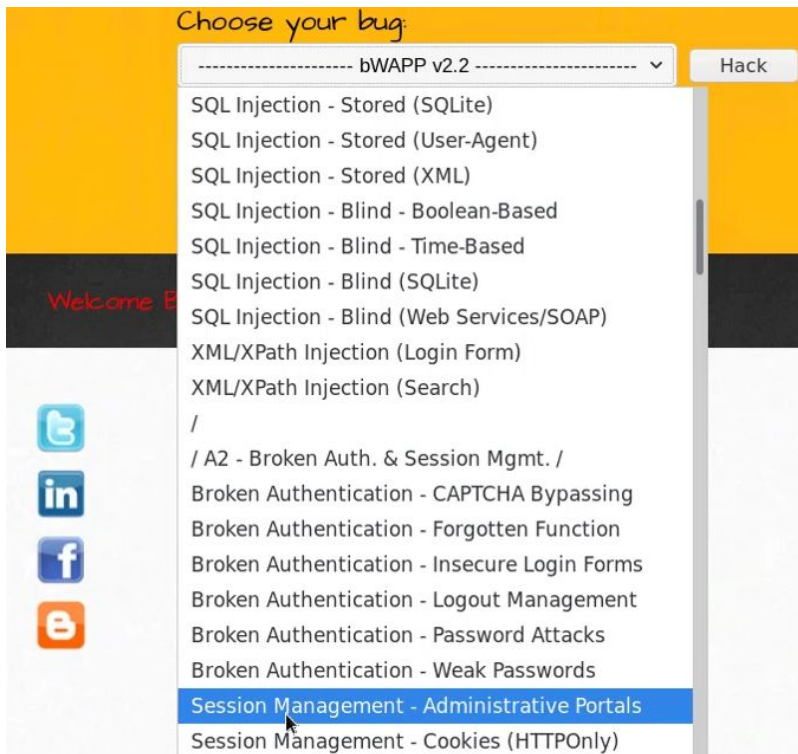**Step 3:** Accessing the web application in Mozilla Firefox.
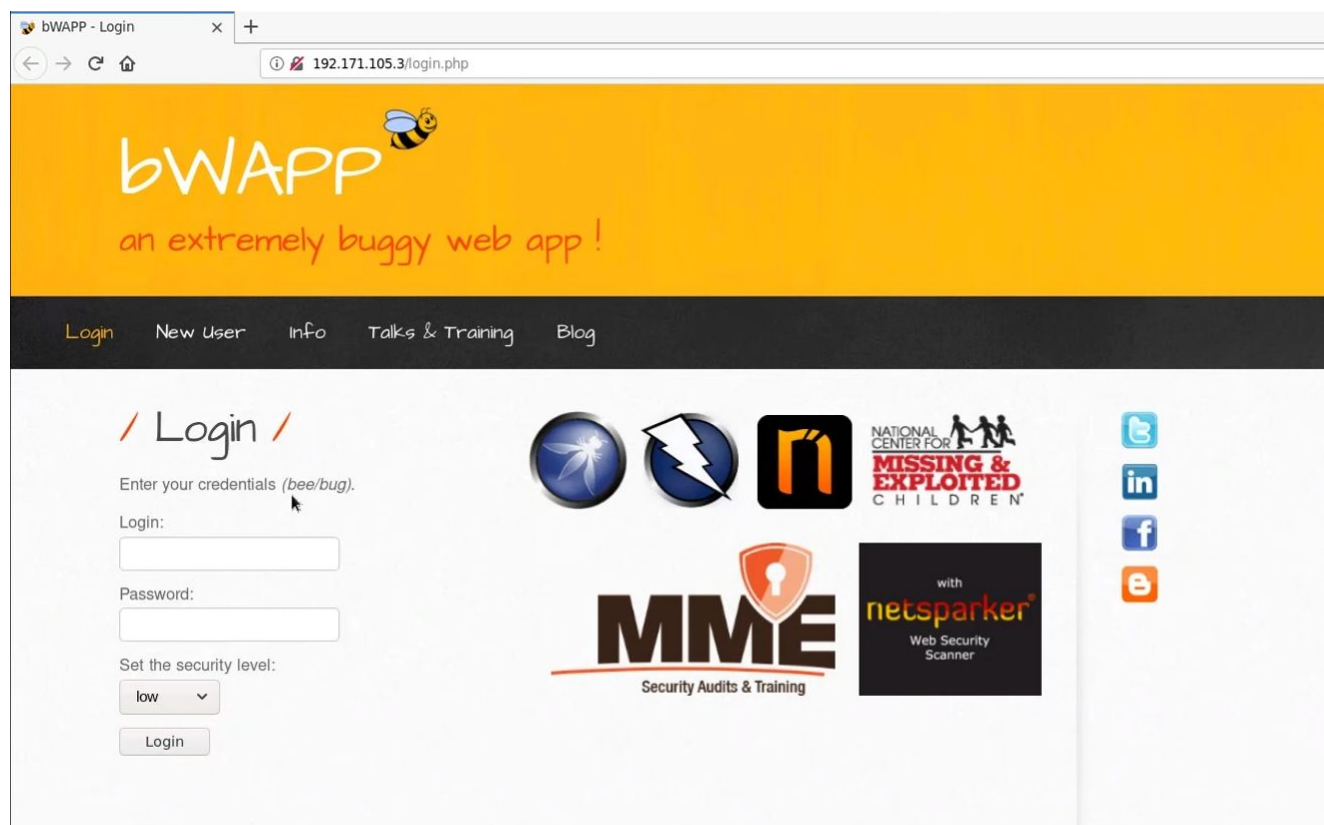
Step 4: Logging into the web application. The login credentials are provided on the web page.
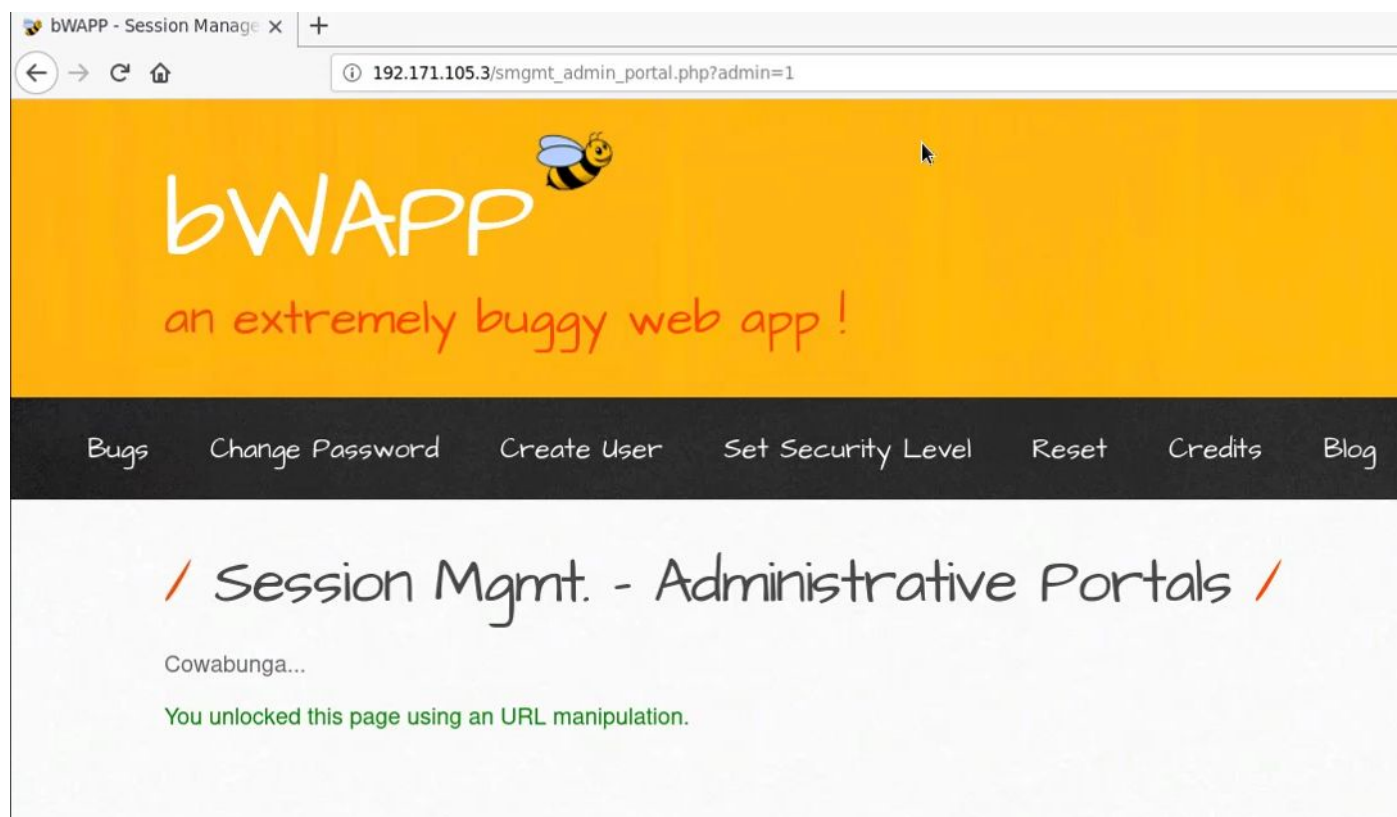
Username: bee
Password: bug

Step 5: Select "Session Management - Administrative Portals" from "Choose your bug" dropdown and click "Hack"

Step 6: Changing admin parameter value in the URL

GET Parameter: admin=1

Access to the administrative portal.

References:

1. bWAPP (http://itsecgames.blogspot.com/)