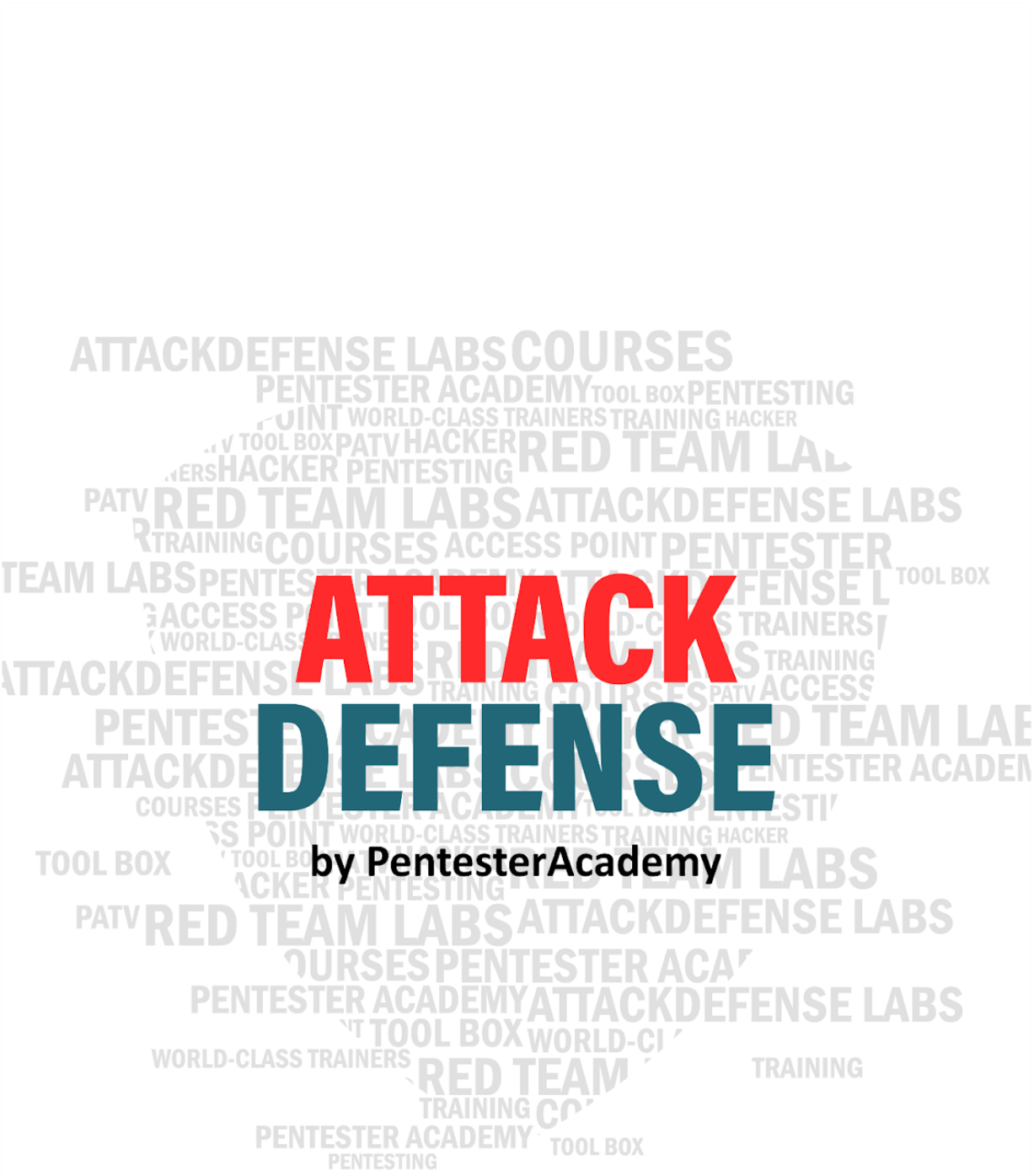

ATTACK
DEFENSE
by PentesterAcademy

Name	Local File Inclusion
URL	https://www.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: Local File Inclusion 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

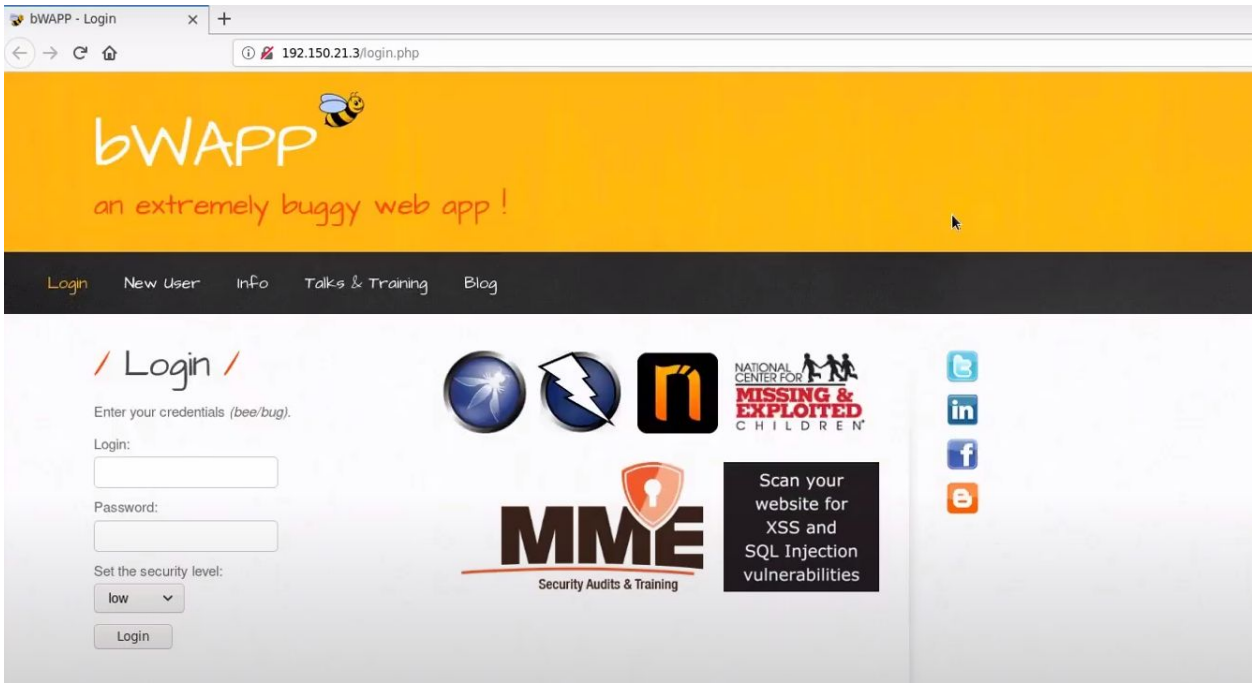
Command: nmap 192.150.21.3

```
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:~#
```

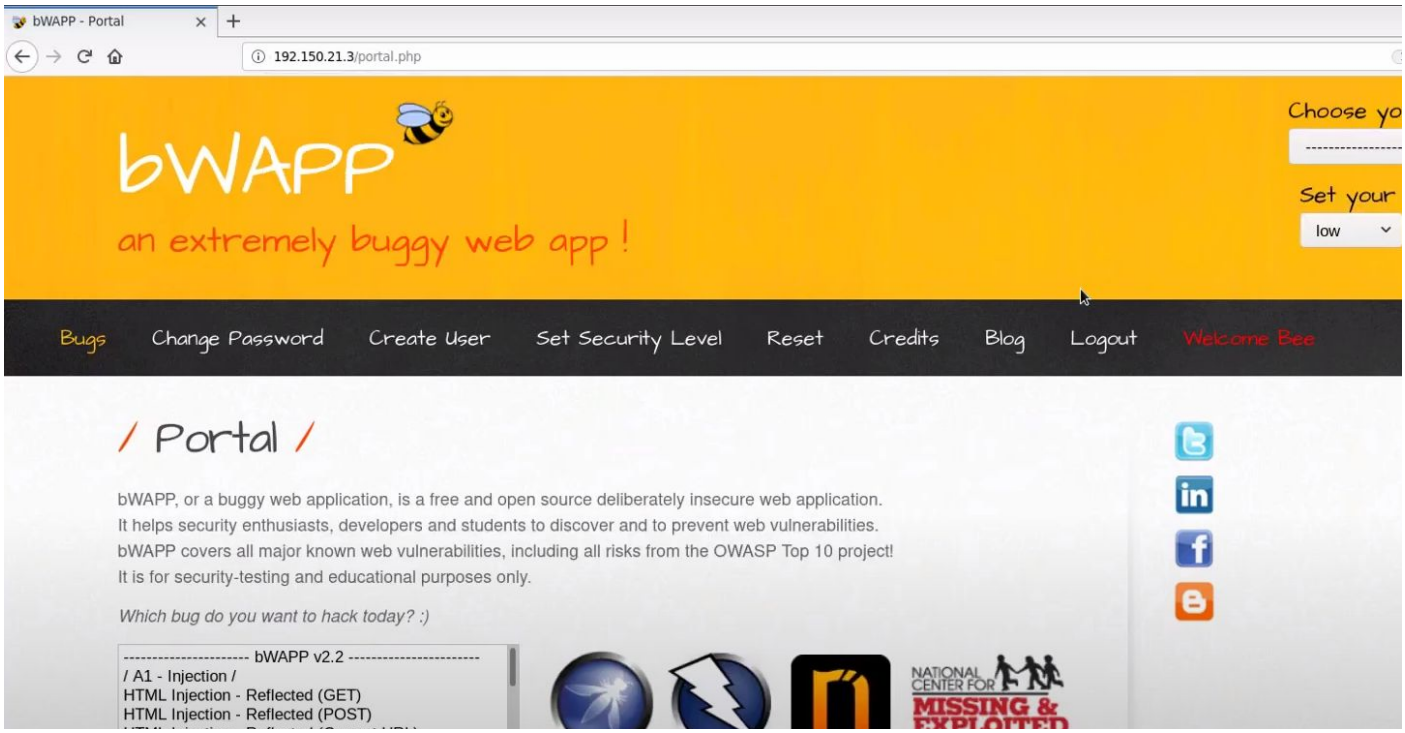
Port 80 and 3306 are open

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

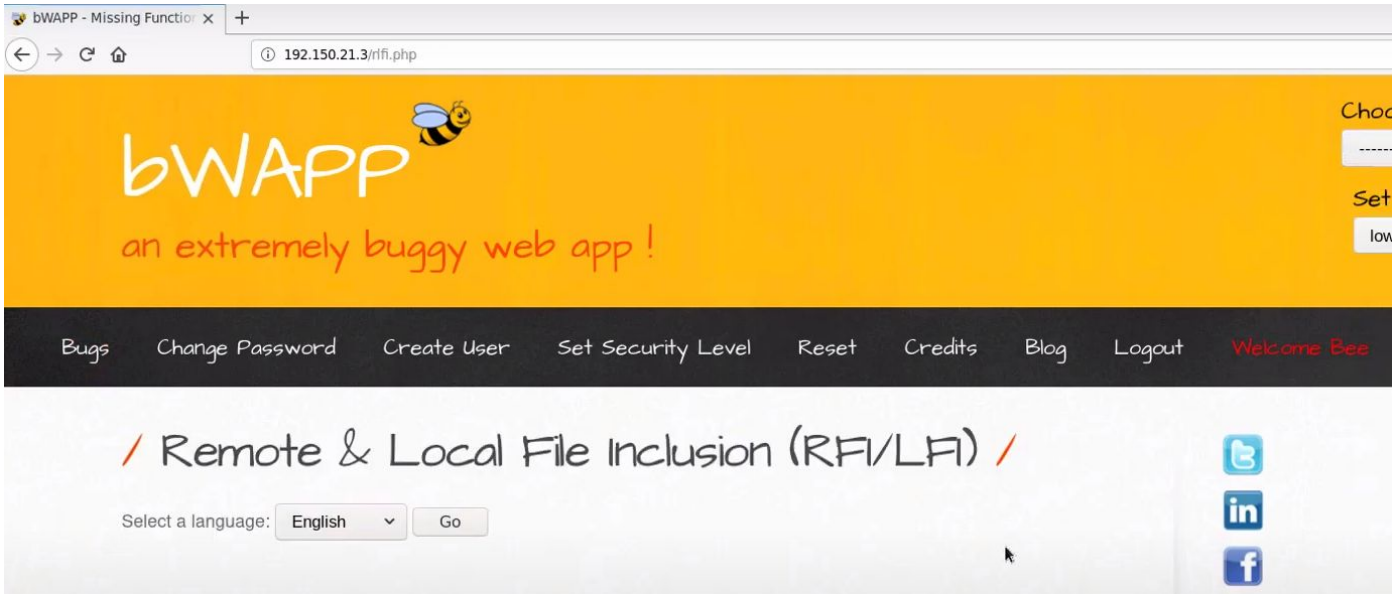


An instance of bWAPP is running at port 80 of the target.

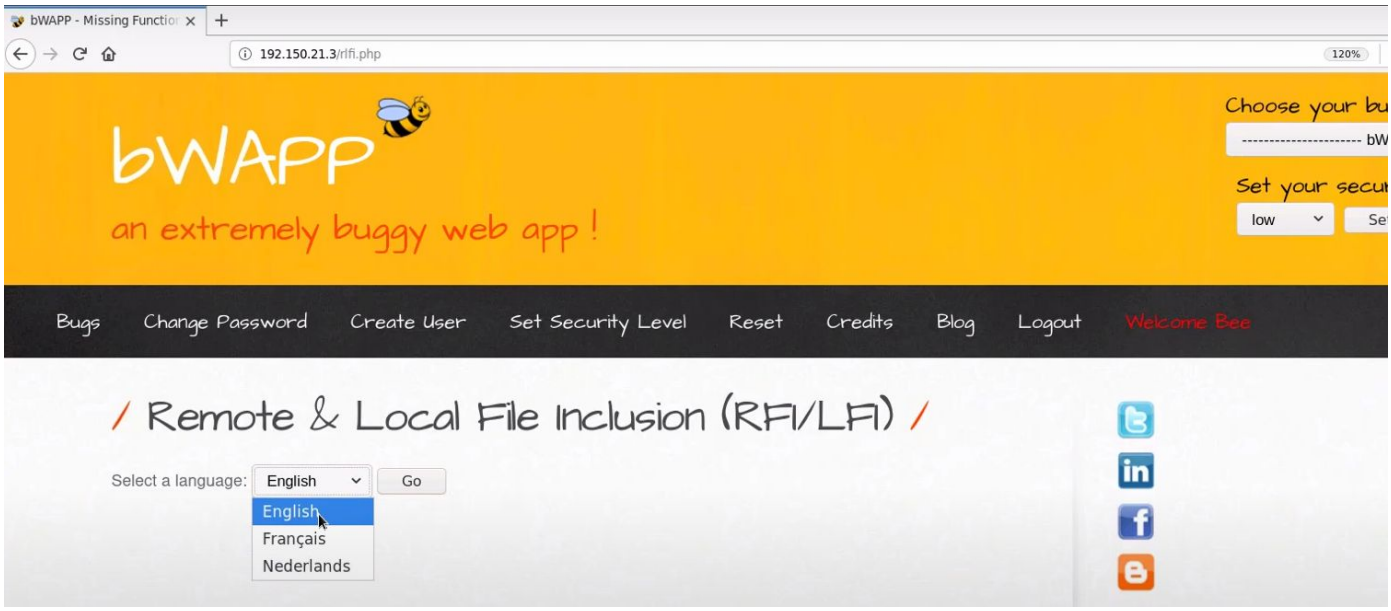
Step 4: Log in to the application using **bee:bug** credentials.



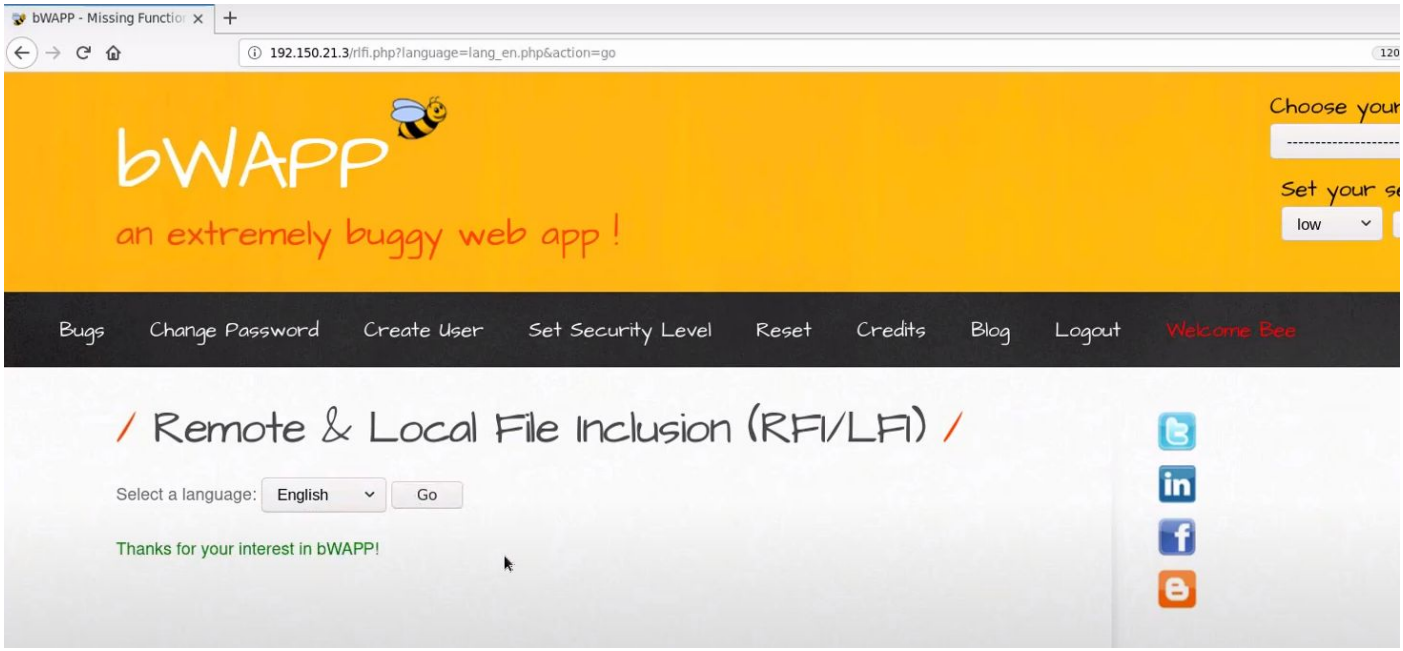
Step 5: From the Choose your bug dropdown, Select "**Remote & Local File Inclusion (RFI/LFI)**" exercise.



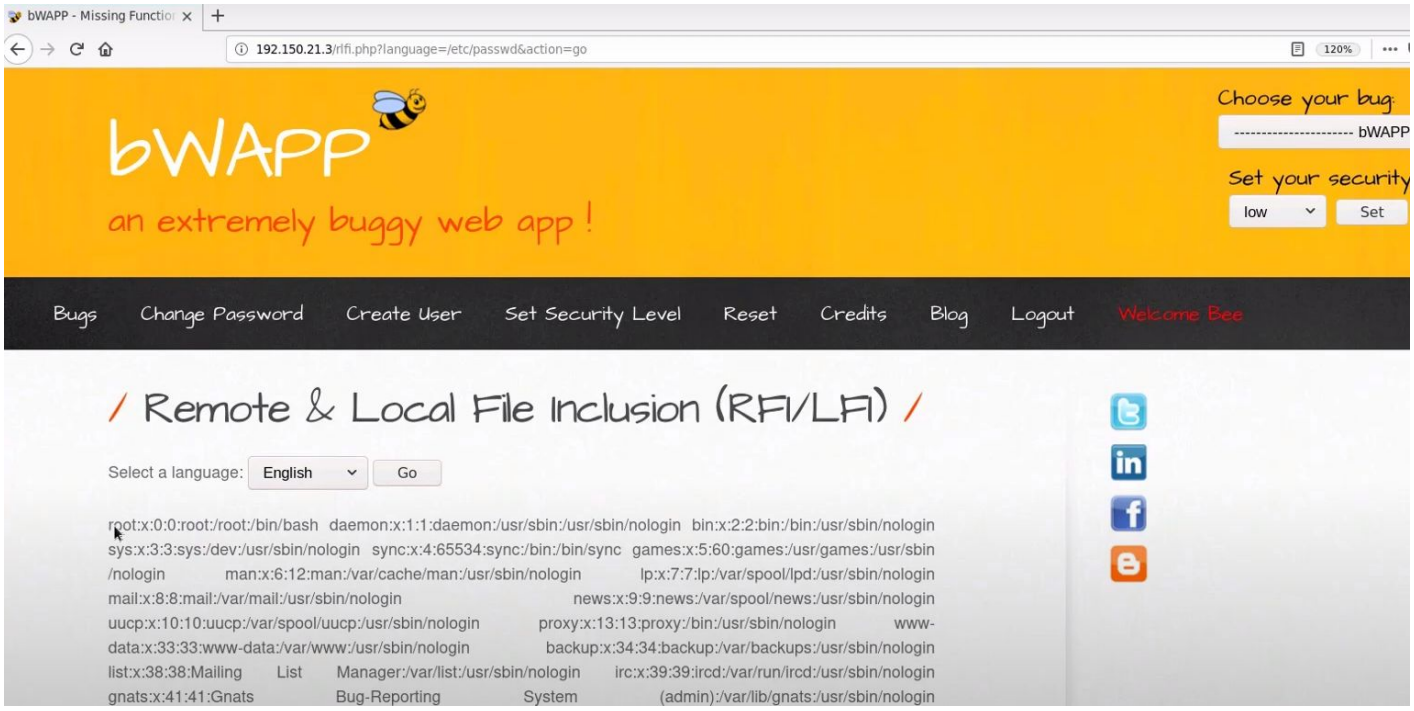
Step 6: Choose a language from the Dropdown menu.



Click on the Go button.



Step 7: Modify the language parameter in the URL and put “/etc/passwd” in the parameter.



The Local File Inclusion attack was successful.

References:

1. bWAPP (http://www.itsecgames.com/)
2. Mutillidae (https://sourceforge.net/projects/mutillidae/)