Report

Task 1: Network Configuration

Figure 1

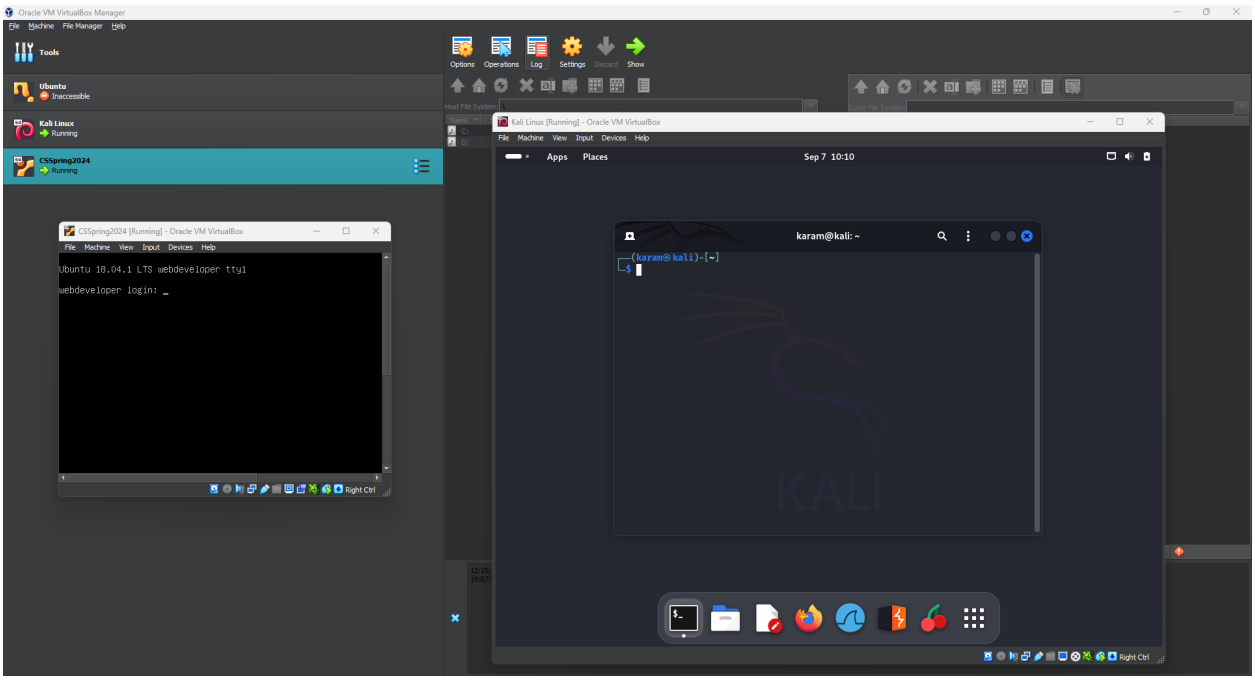


Table 1

VM	IP Address	Subnet mask	Default Gateway	Network Adapter
Kali Linux	192.168.100.35	255.255.255.0	192.168.100.1	Brigid Adapter
Target	192.168.100.37	255.255.255.0	192.168.100.1	Brigid Adapter

Task 2: Reconnaissance and Vulnerability Analysis

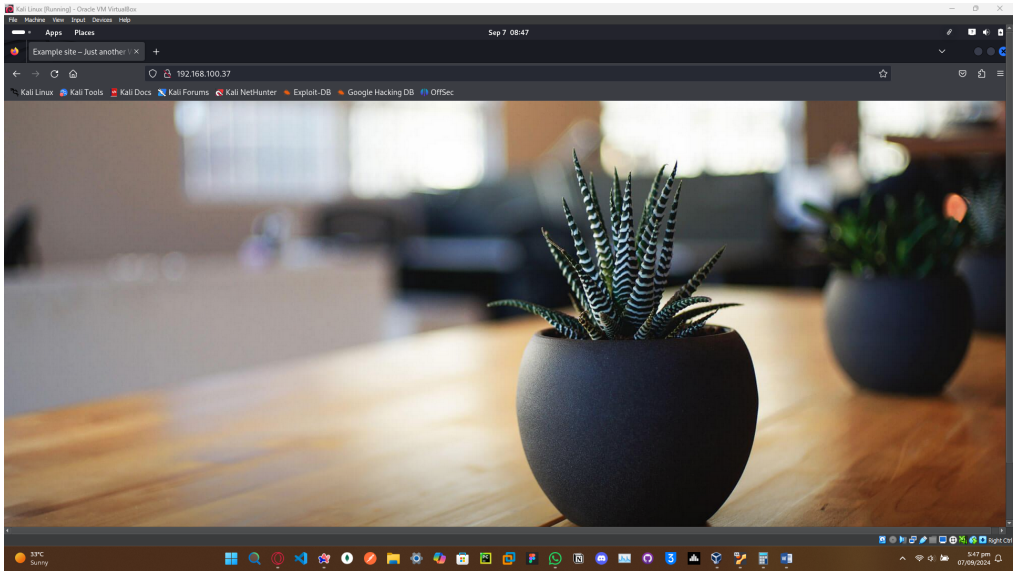
1. Identify the target machine's IP address
    a. I used the "sudo netdicover" on my home Wi-Fi but there were way too many devices that I was unable to find the target device so I used my mobile hotpot and then again ran the command but it was way to slow so I used the "ifconfig" command to get the info related adaptor and then used the command with specific IP range and device adaptor "sudo netdicover –i eth0 –r 192.168.100.0/24" then easily, I got the device, it was only one device named "PCS Systemtechnik GmbH" with an IP of "192.168.100.37".
2. Determine the open ports and running services

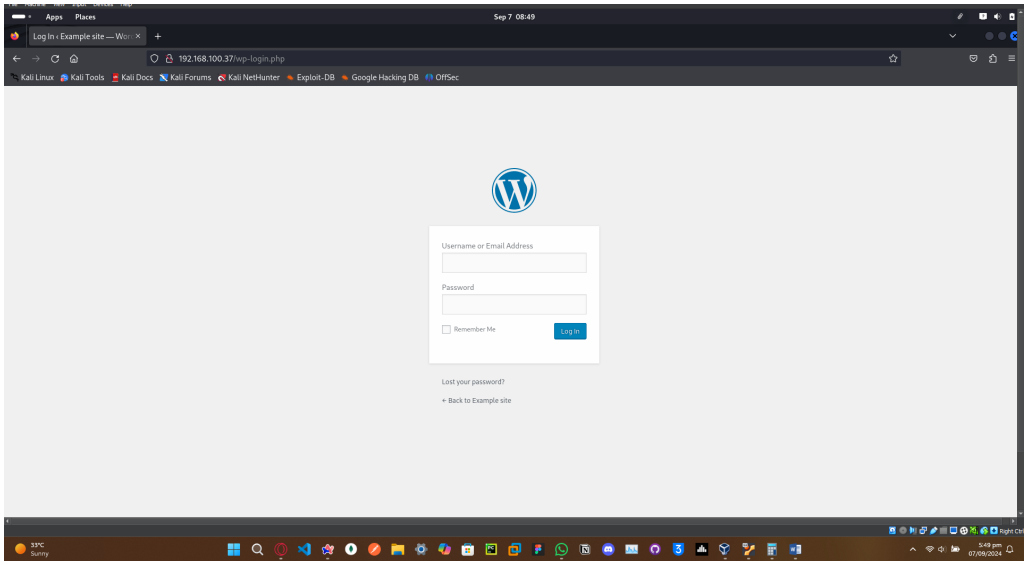
a.

```
karam@kali: ~
┌──(karam㉿kali)-[~]
└─$ sudo nmap 192.168.100.37
[sudo] password for karam:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-07 08:19 EDT
Nmap scan report for 192.168.100.37
Host is up (0.00050s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:CC:54:C9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

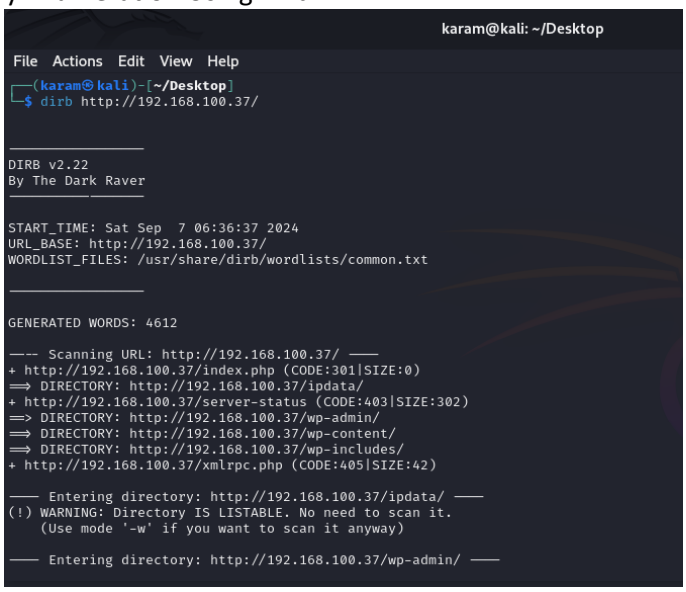
b. I used the command "sudo nmap 192.168.100.37" to find the open ports which is port 80 aka http port running http service and port 22 the port running TCP service.

3. Identify Vulnerabilities in Web Application
   a. As I find out that the service is http and the IP is 192.168.100.37 so I went to the browser and typed http://192.168.100.37/ and it took me to the webpage .
   b. 
   c. There I found out a login page on the link http://192.168.100.37/wp-login.php.

d. 

e. I tried to use the common username and password combos like admin/admin, admin/password etc but failed.

4. Directory Enumeration Using Dirb

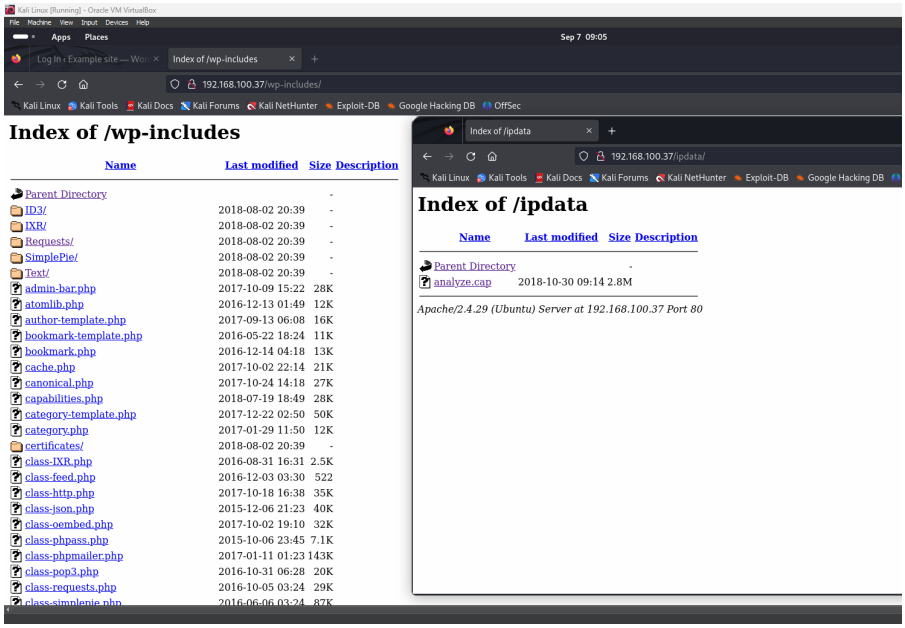
a. 

b. I used the command “dirb http://192.168.100.37/” to search for hidden directories or files that may contain sensitive information.

c. I didn’t understand what this info is representing so I asked GPT about it.

d. 1. **Directories and Files Found:**
   - `http://192.168.100.37/index.php`: This is a page that redirects (HTTP status 301) but doesn't display content.
   - `http://192.168.100.37/ipdata/`: This directory is found and is listable.
   - `http://192.168.100.37/server-status`: Access is forbidden (HTTP status 403).
   - `http://192.168.100.37/wp-admin/`: This is a WordPress admin directory.
   - `http://192.168.100.37/wp-content/`: This is where WordPress stores content like themes and plugins.
   - `http://192.168.100.37/wp-includes/`: Contains WordPress core files, and it is listable.
   - `http://192.168.100.37/xmlrpc.php`: This file is present but returns a method not allowed status (HTTP status 405).

e. By this I get to know that I Dirb has found three list able directories (wp-admin ,wp-includes ,ipdata) out of which two (wp-includes ,ipdata) are discoverable and one (wp-admin) requires login credentials.

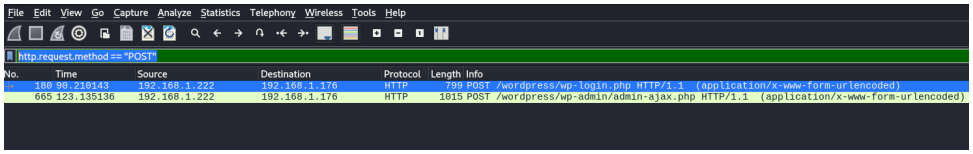
f. 

g. There was nothing in the wp-include as it contained all the static files that doesn't give any info generally.

h. In ipdata I found a Wireshark file named as analyze.cap and opened it.

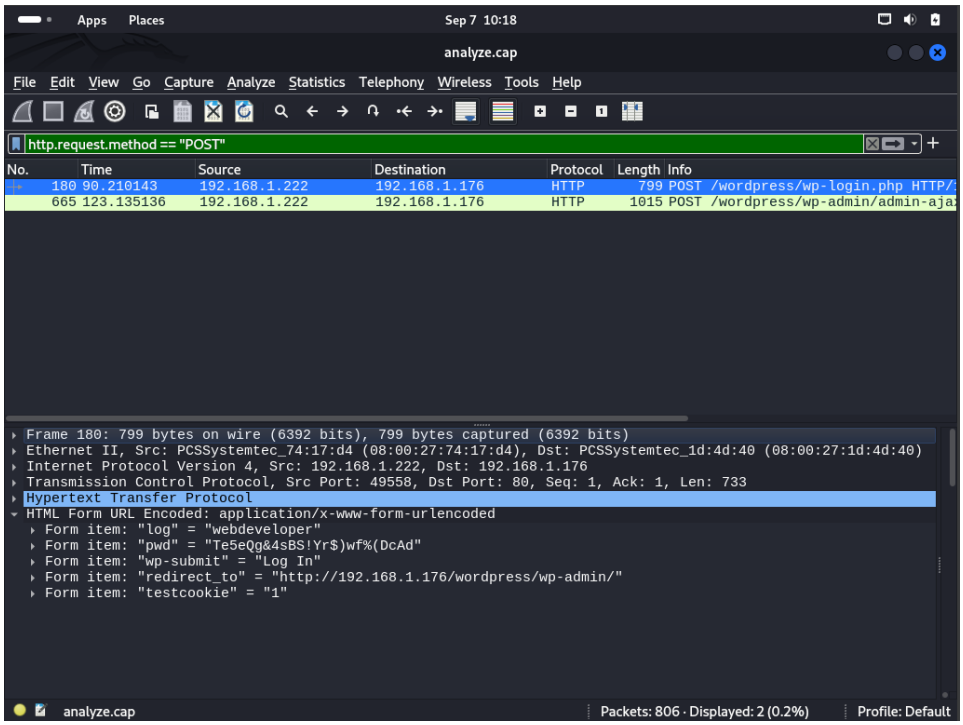
i. Then I checked the http:post methods because usually forms are submit using this type of request.

j. I used the Wireshark filter and used the command http.request.method == "POST".

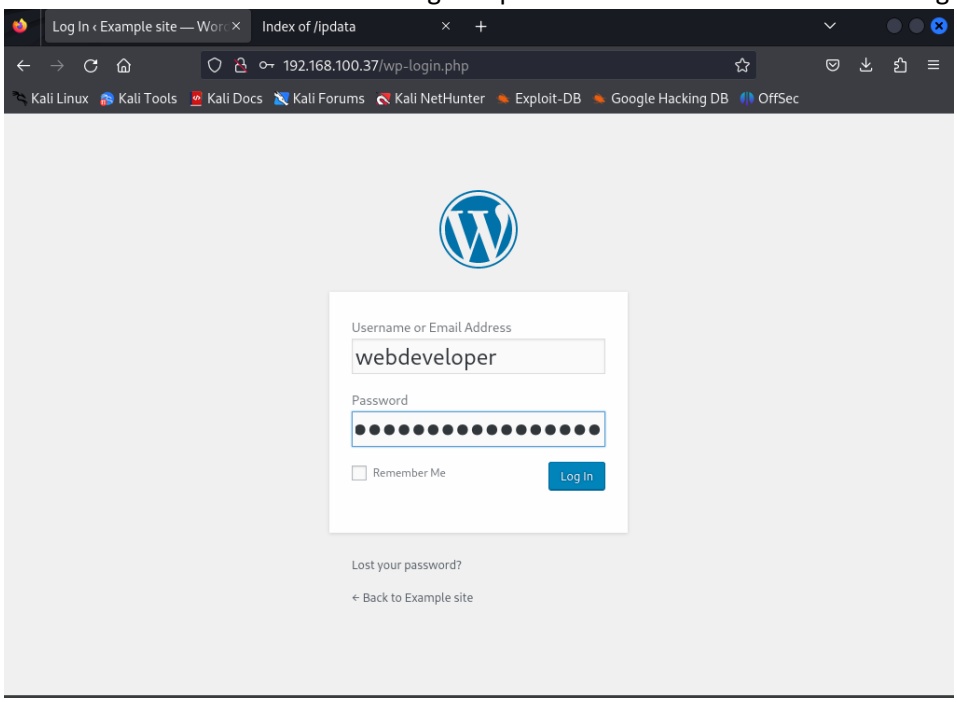
k. 

l. As by the length info it was obvious the second packet had something to do with the "admin-ajax.php" so I clicked it and opened its details.

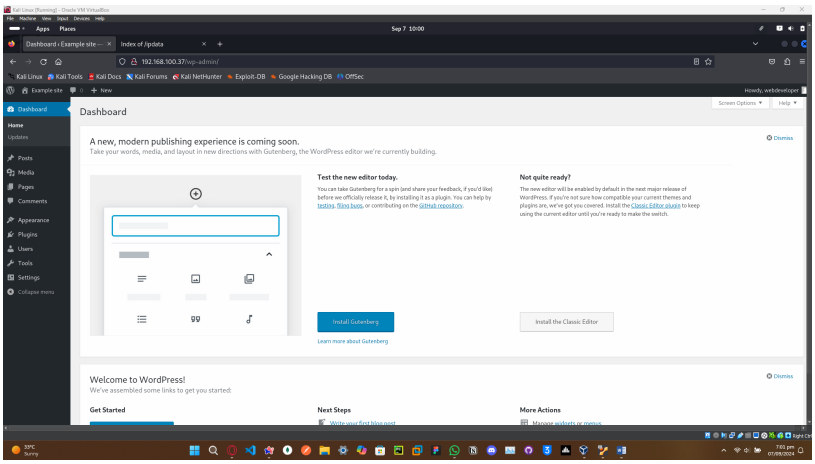
m. After searching around under the heading HTML Form URL-encoded, I found some info as shown in the pic below.

n. 

o. There were form items named as log and pwd and when I used them on the login page.

p. 

q. After using it as login credentials, I was on the dashboard as shown below.

r. 

Conclusion

- **Login**: webdeveloper
- **Password**: Te5eQg&4sBS!Yr$)wf%(DcAd

This concludes the analysis and demonstrates the process of identifying a target machine, discovering vulnerabilities, and successfully exploiting them to gain access.