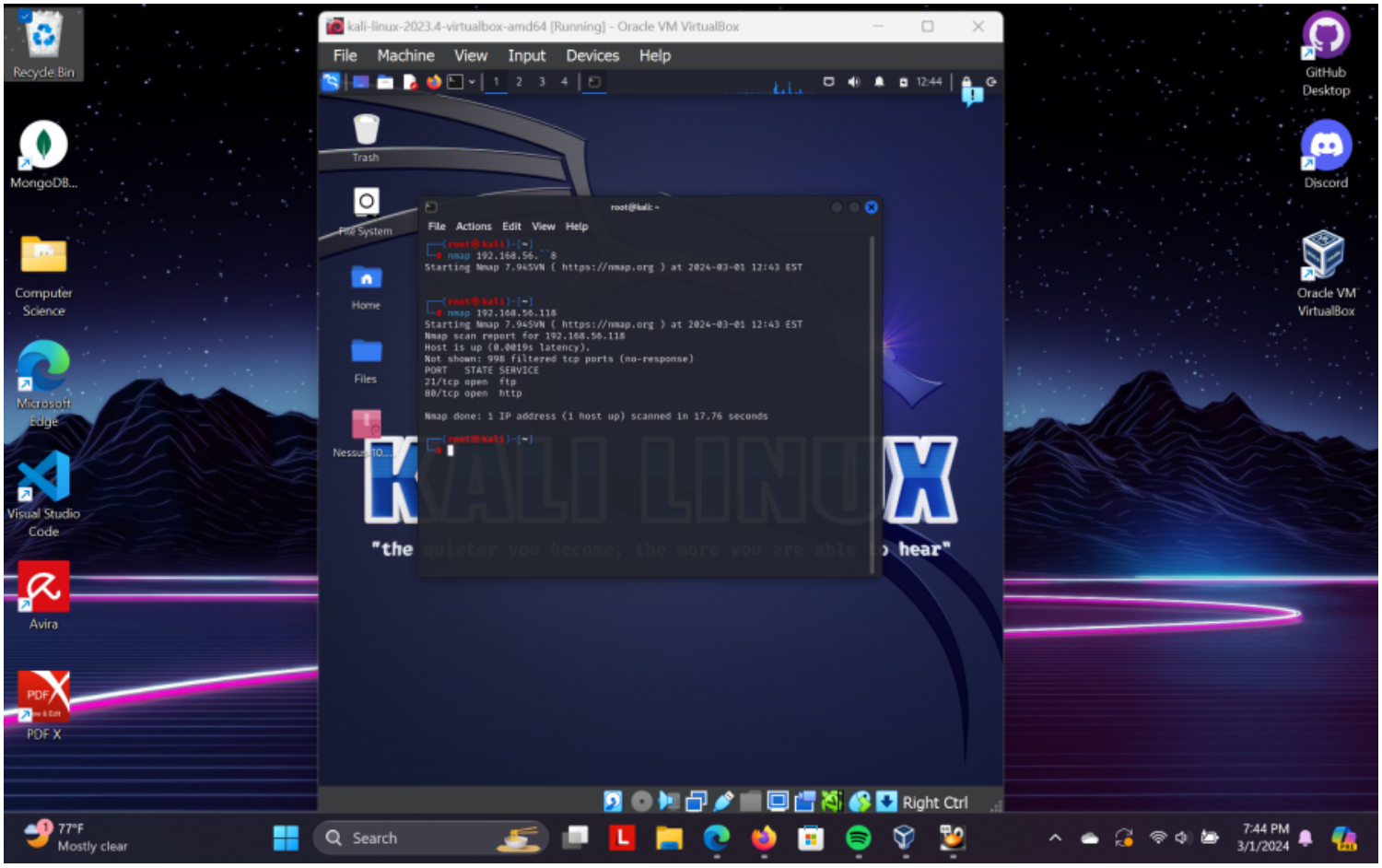
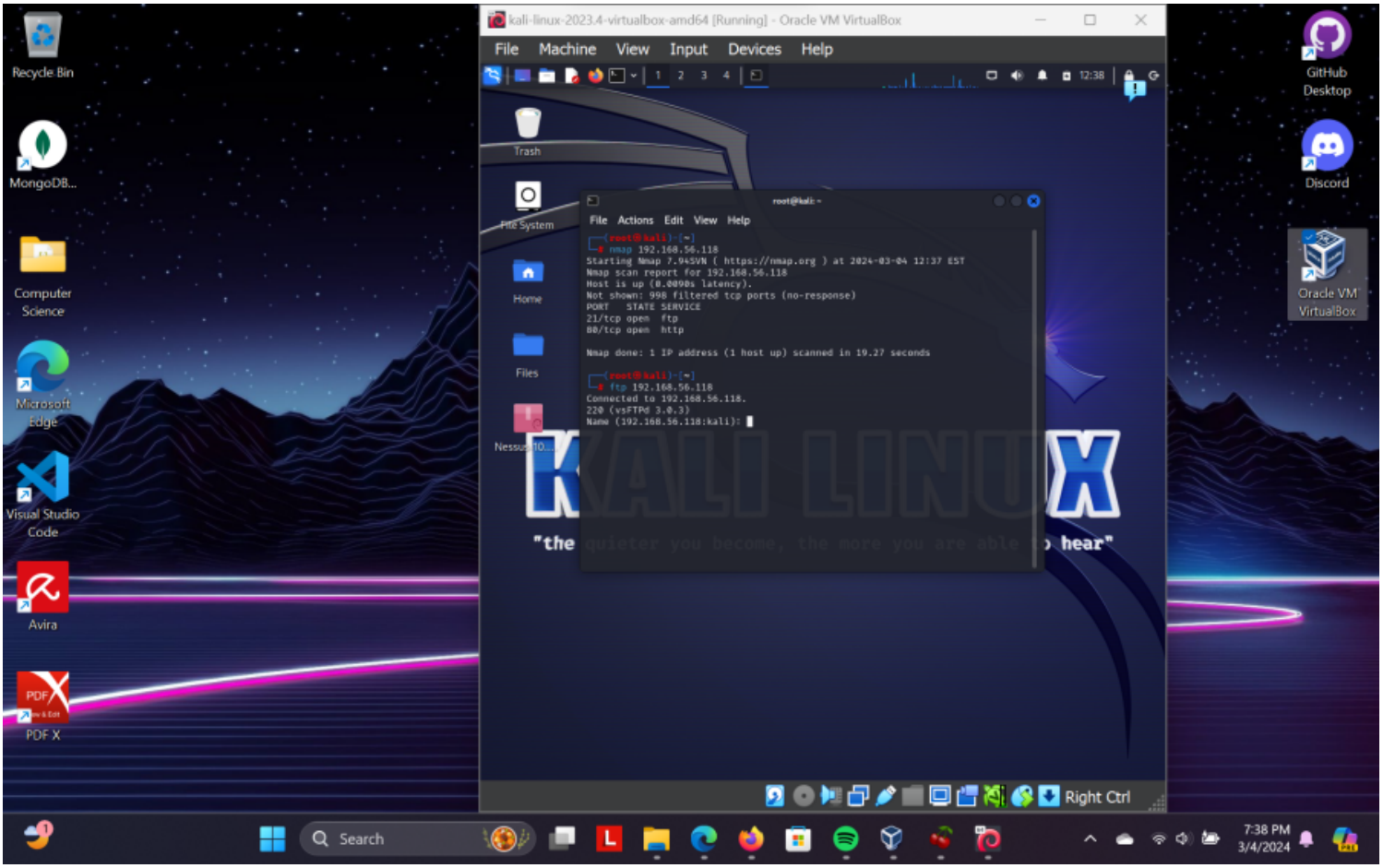
Scanning IP address



Using nmap for inital port scan:
This command will provide information about open ports, potentially revealing services running on those ports. Which in our case are port 80 (HTTP) and port 21 (FTP).
ⓘNMAP: Nmap scans the target host for open ports to identify which network services are running. It does this by sending various types of probes to the target ports (e.g., TCP SYN, TCP Connect, UDP) to determine if they are open, closed, or filtered by a firewall.

After scanning ip address 192.168.56.118:
Both ports 80 (HTTP) and 21 (FTP) were found open.

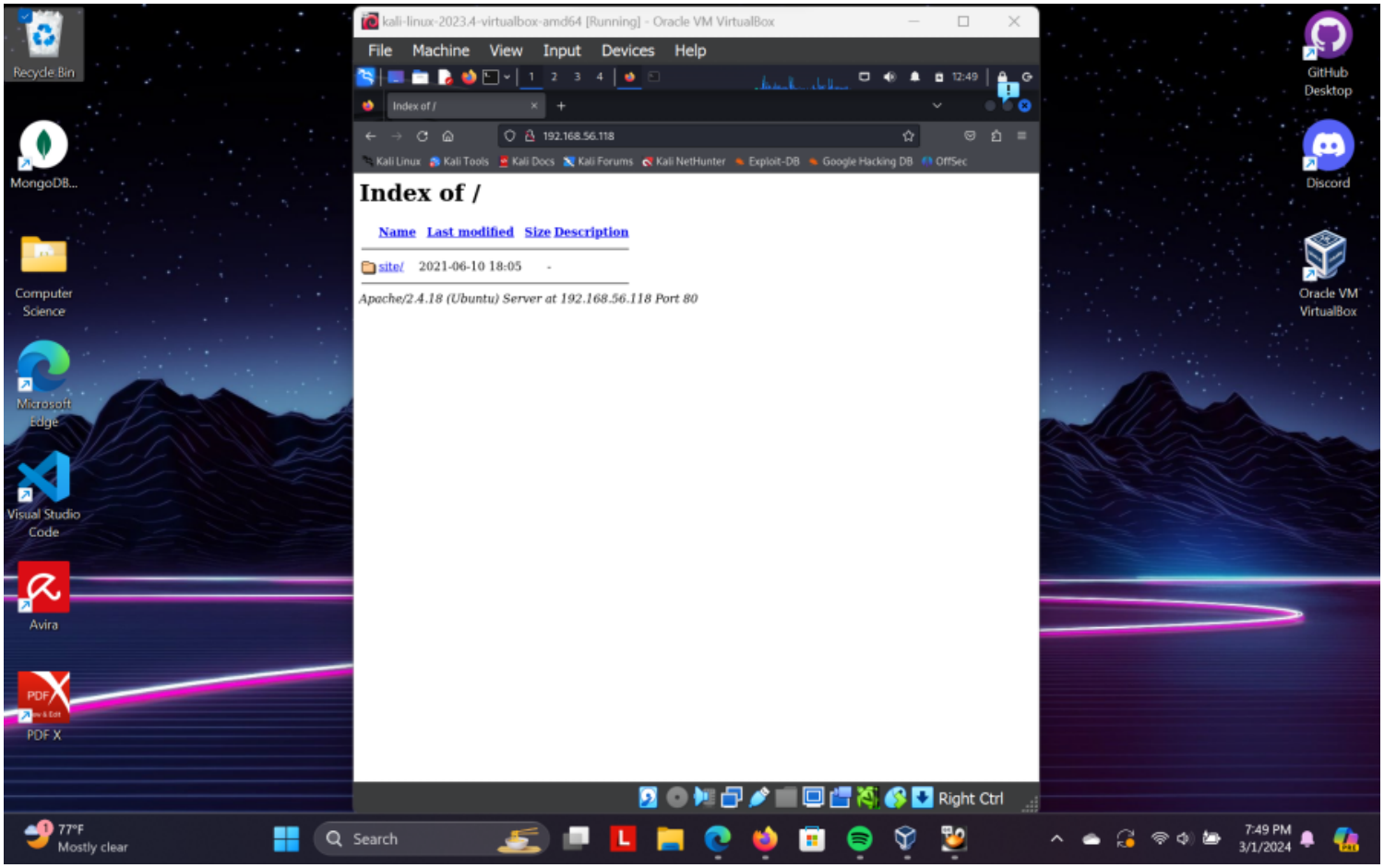


For Port 21:

When attempting to access the FTP server at 192.168.56.118 using the ftp command in the root command prompt on Kali Linux, no results were obtained. The command prompted for a username and password, which we currently do not possess. As a result, further exploration of the FTP server was not possible at that time.

For Port 80:

After discovering that port 80 was open during the scanning process, I decided to utilize a web browser to manually navigate to the IP address 192.168.56.118. By exploring the website for any accessible pages or directories, I successfully located an accessible page.



The next step is to navigate to http://192.168.56.118/site/

Enumeration

ⓘDirb is useful for uncovering additional entry points and potential vulnerabilities in web applications. By discovering hidden directories and files.

From the dirb scan results, it appears that several directories and files have been discovered within the /site directory on the web server at 192.168.56.118. :

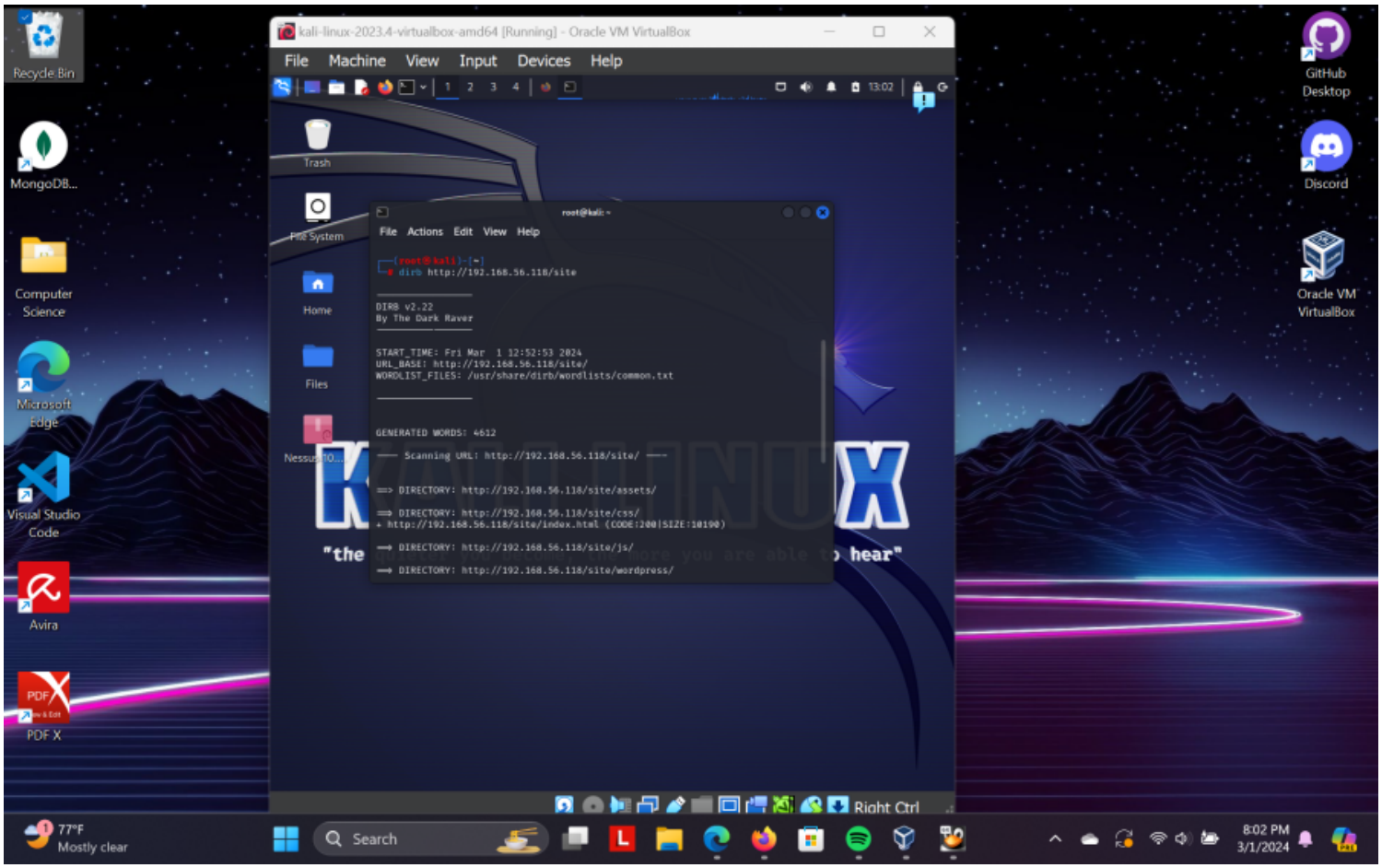
1. **Directories:**

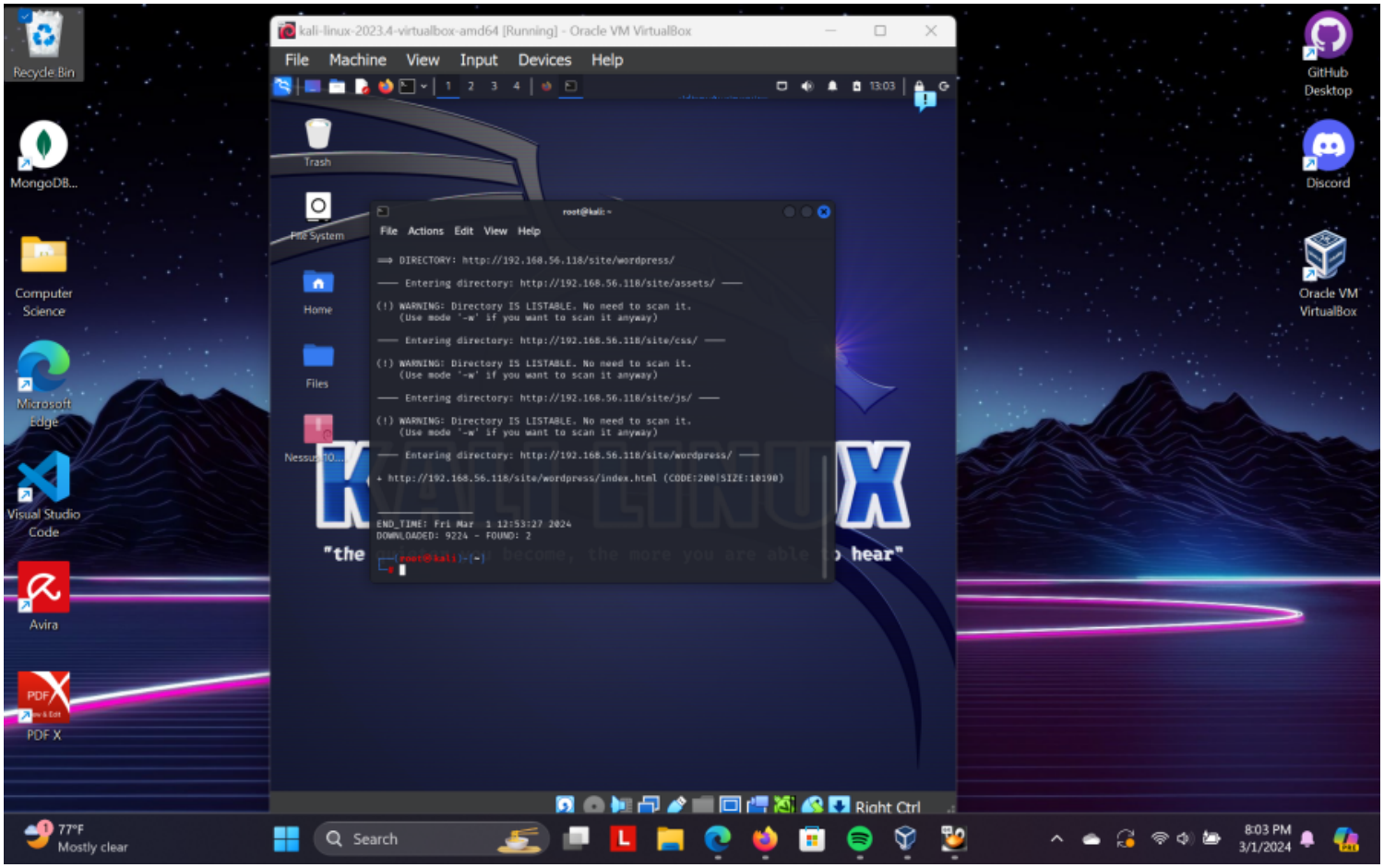
- /site/assets/
- /site/css/
- /site/js/
- /site/wordpress/

- **Files:**

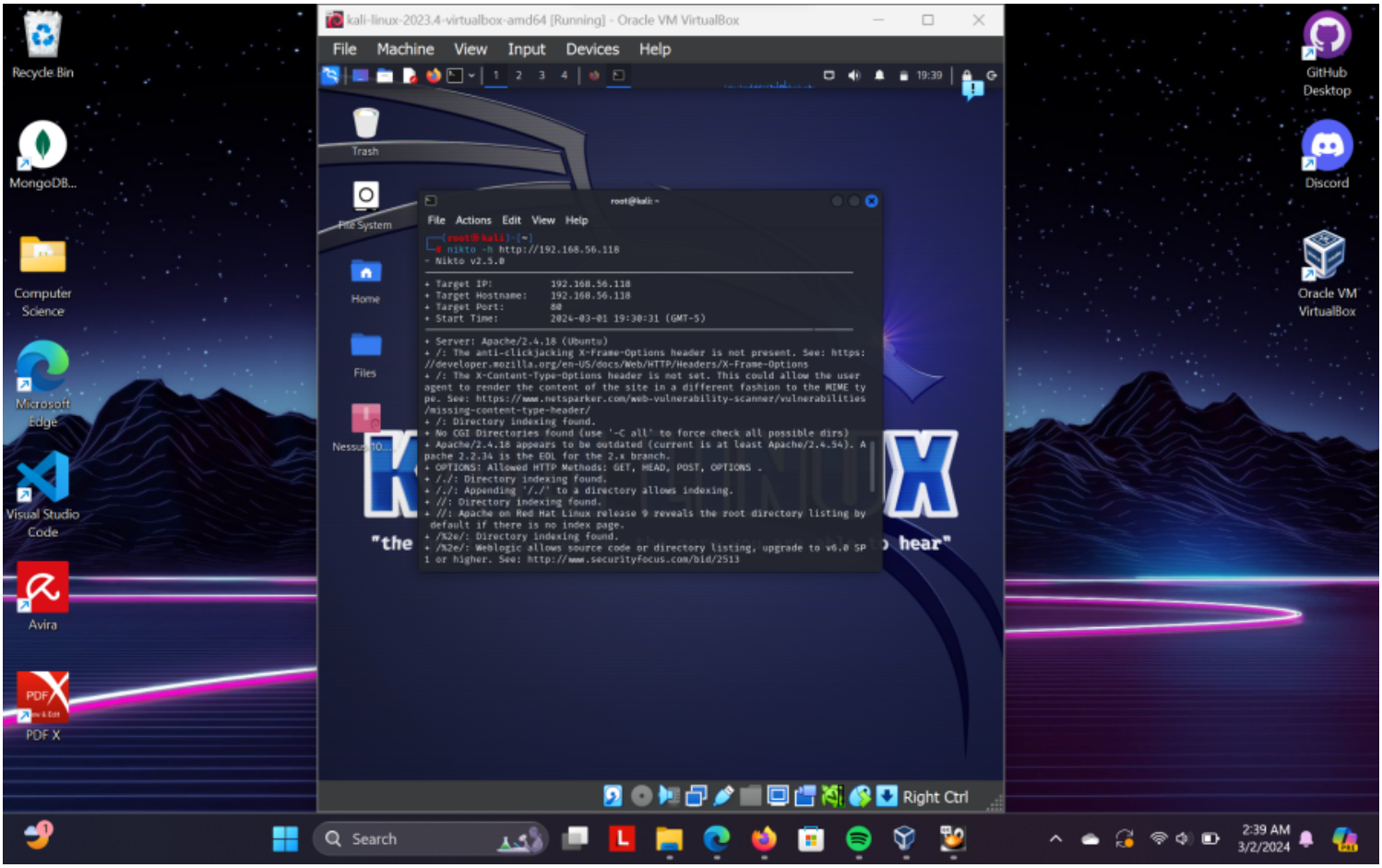
◇ /site/index.html

◇ /site/wordpress/index.html





ⓘ Nikto scan results provide valuable information about potential vulnerabilities and misconfigurations on the target web server.



• **Server Information:**
• Server: Apache/2.4.18 (Ubuntu)
• The server version appears to be outdated. Current versions of Apache are at least Apache/2.4.54.

• **Security Headers:**

◇ The anti-clickjacking X-Frame-Options header is not present.

◇ The X-Content-Type-Options header is not set.

◇ These missing headers could potentially leave the website vulnerable to clickjacking attacks and MIME sniffing attacks.

• **Directory Indexing:**

◇ Directory indexing is enabled on the root directory (/), which means that users can see the contents of directories if no index file (e.g., index.html) is present.

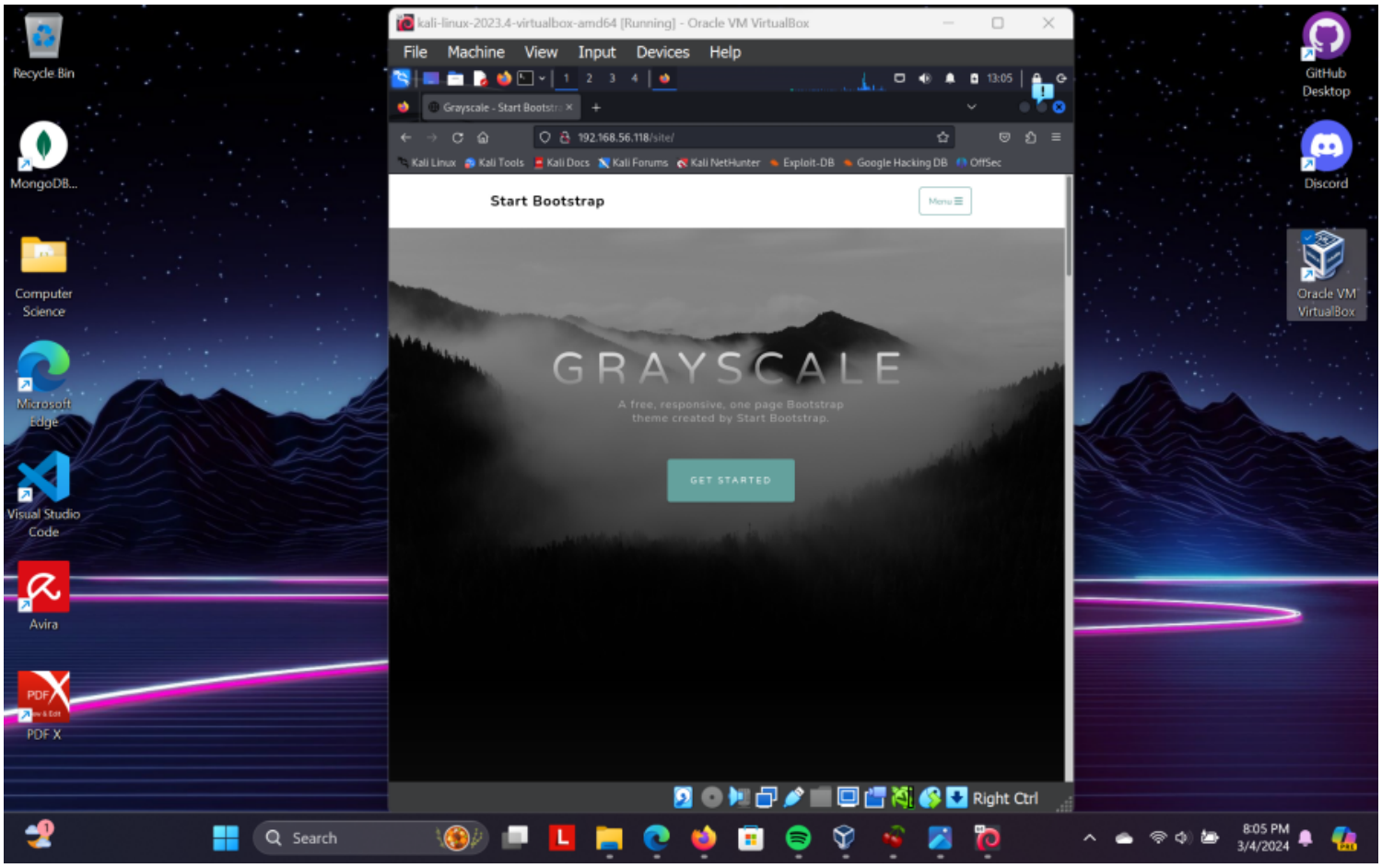
◇ Several variations of directory indexing were found, including /./, //, /%2e/, and ///.

◇

• **Total Requests:**
• Total requests made: 8102
• No errors were encountered during the scan.

Searching for Vulnerabilities

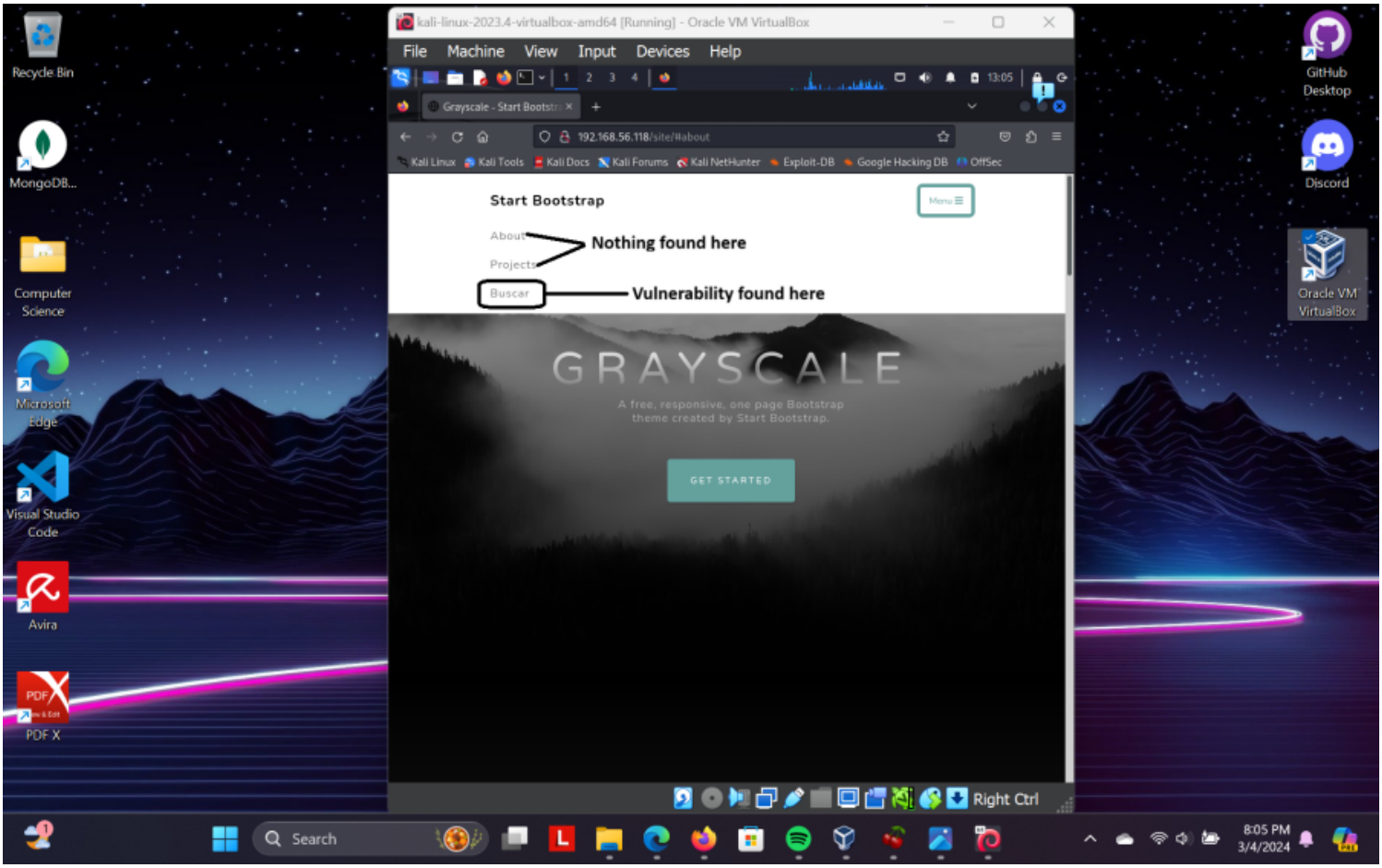
After navigating to http://192.168.56.118/site/, I began examining the website closely, meticulously searching for any potential vulnerabilities or weaknesses.



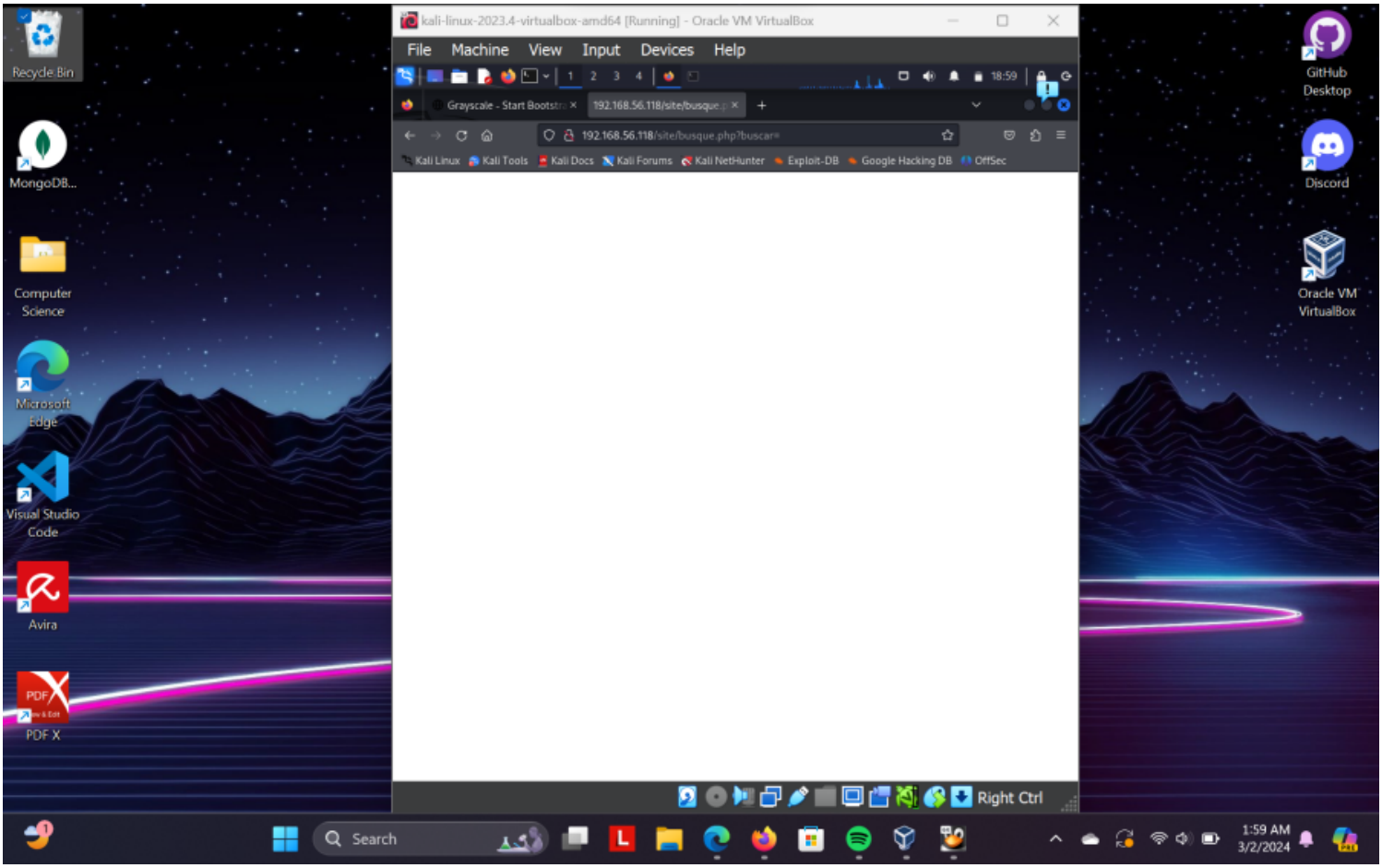
Site I was navigated to

The website primarily consisted of a menu with options for 'About', 'Projects', and 'Buscar'.

While examining the 'About' and 'Projects' sections, I found no noteworthy information. At this point, my attention shifted to the only remaining option, 'Buscar', confirming my suspicions.



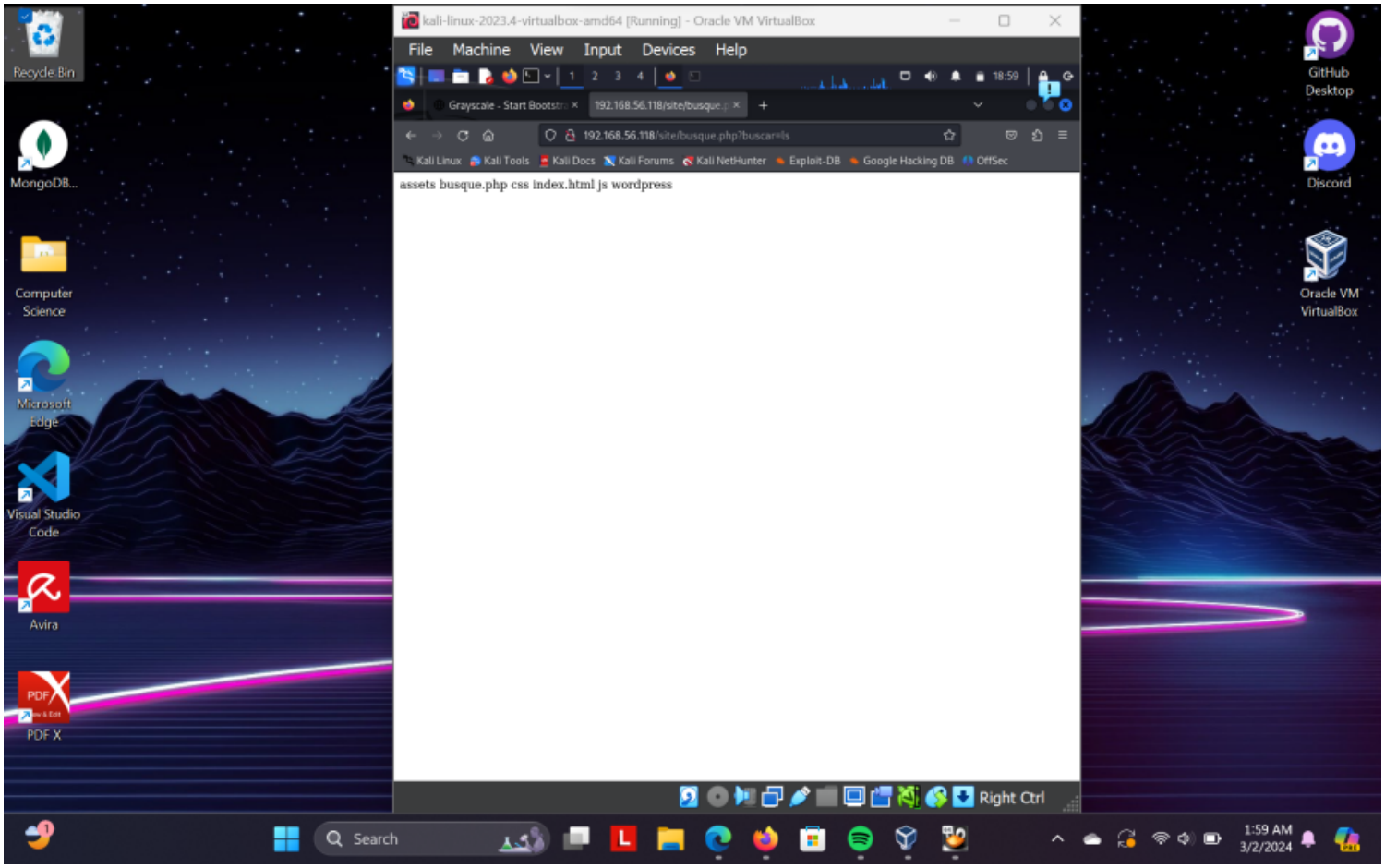
How I confirmed my theory:
Upon clicking the 'Buscar' option (http://192.168.56.118/site/busque.php?buscar=), the link redirected to an empty page. This suggests that either the search functionality is not implemented correctly or there may be an issue with the server-side script responsible for handling the search functionality.


kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.56.118/site/busque.php?buscar=
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Right Ctrl
Recycle Bin
MongoDB...
Computer Science
Microsoft Edge
Visual Studio Code
Avira
PDF X
GitHub Desktop
Discord
Oracle VM VirtualBox
Search
1:59 AM
3/2/2024

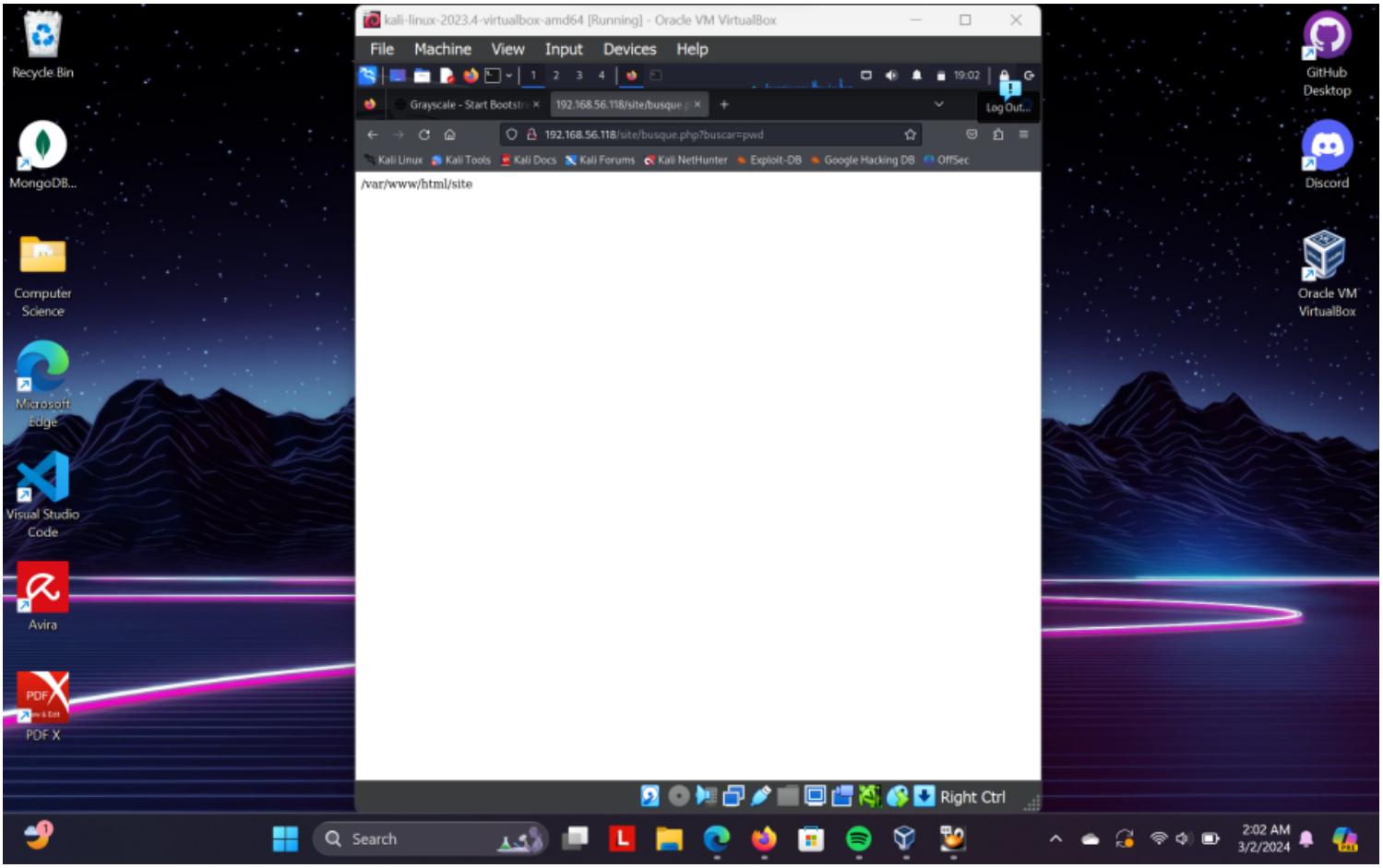
Exploiting

I made the decision to exploit the (http://192.168.56.118/site/busque.php?buscar=) link in an attempt to determine if it could provide me with access to potential usernames and passwords.

Furthermore, I attempted to utilize the 'ls' (list directory) command to enumerate the directory contents of 'Buscar'. Through this action, it became apparent that there exists a potential vulnerability in the URL parameter 'buscar' of the 'busque.php' script, likely stemming from inadequate input validation. 👇



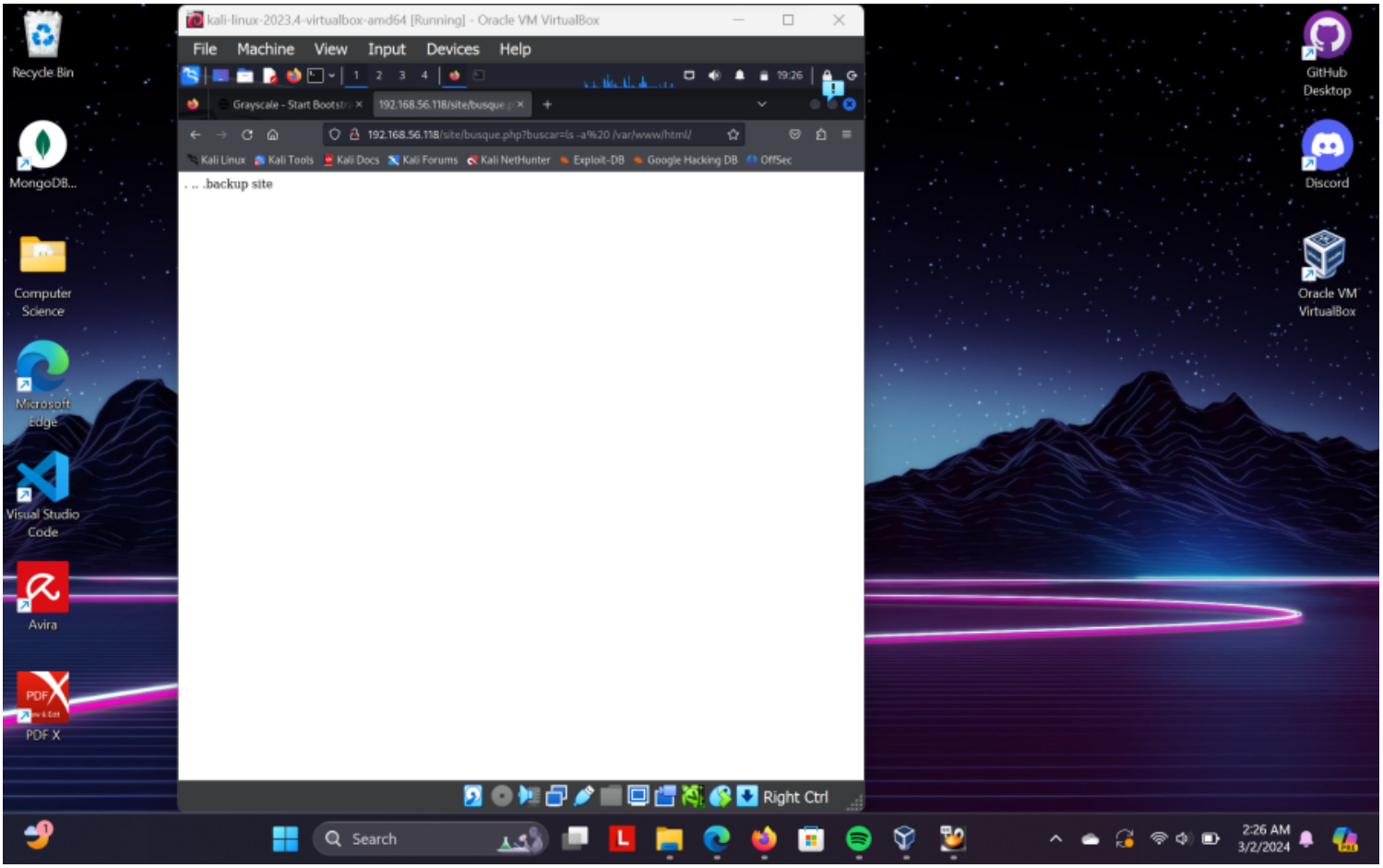
I made the decision to utilize the pwd command (print working directory) by accessing the URL http://192.168.56.118/site/busque.php?buscar=pwd. This action successfully resulted in displaying the current directory path of the server.
ⓘIn Unix-like systems, the pwd command stands for "print working directory." When executed in a shell, it displays the current directory path.



After determining that the current directory of the server is /var/www/html/, I proceeded to use the ls command once more to list its contents, including any hidden files or directories.

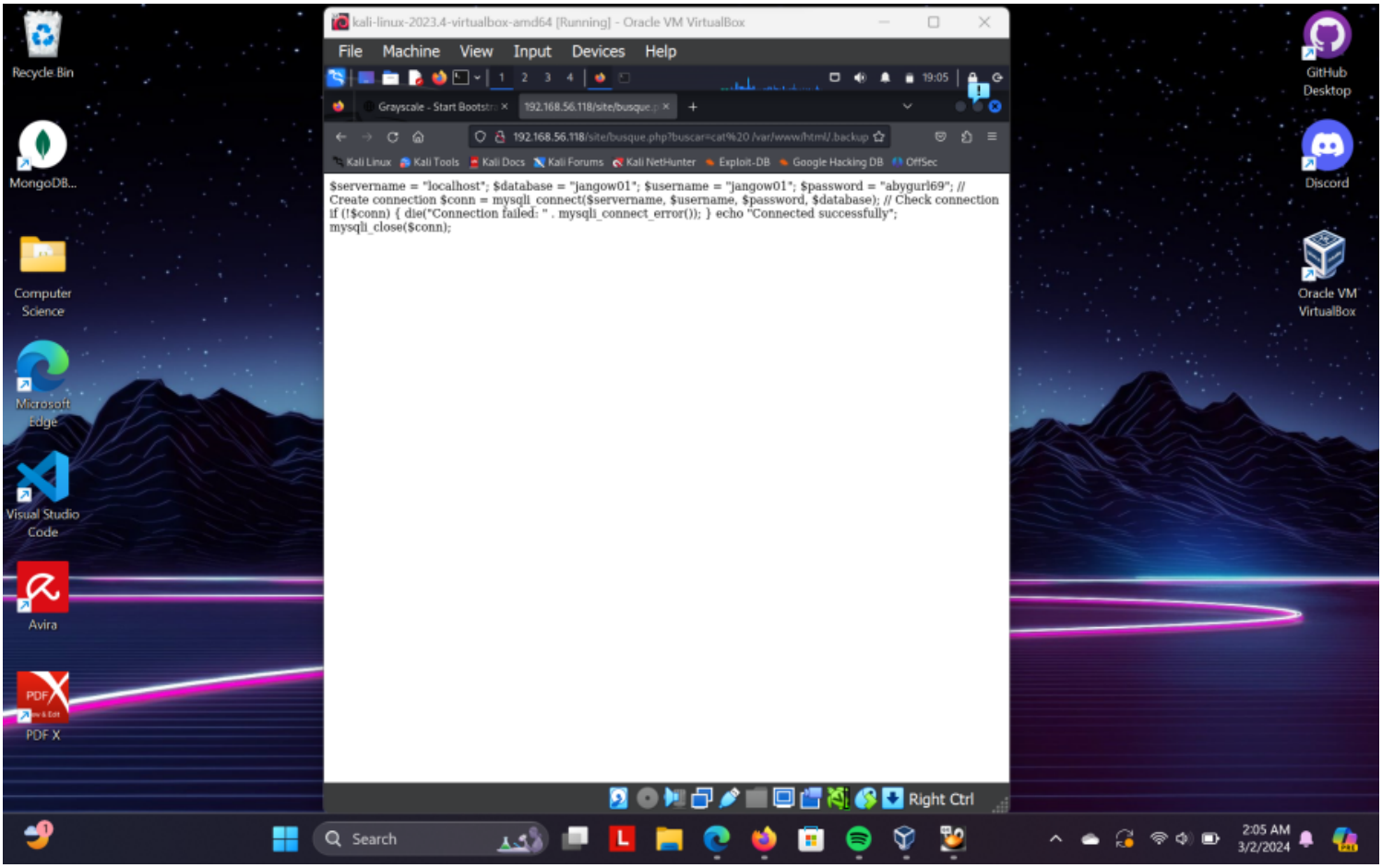
I discovered a directory named 'backup' within the '/var/www/html/' directory.

ⓘ -a is used to show hidden directories

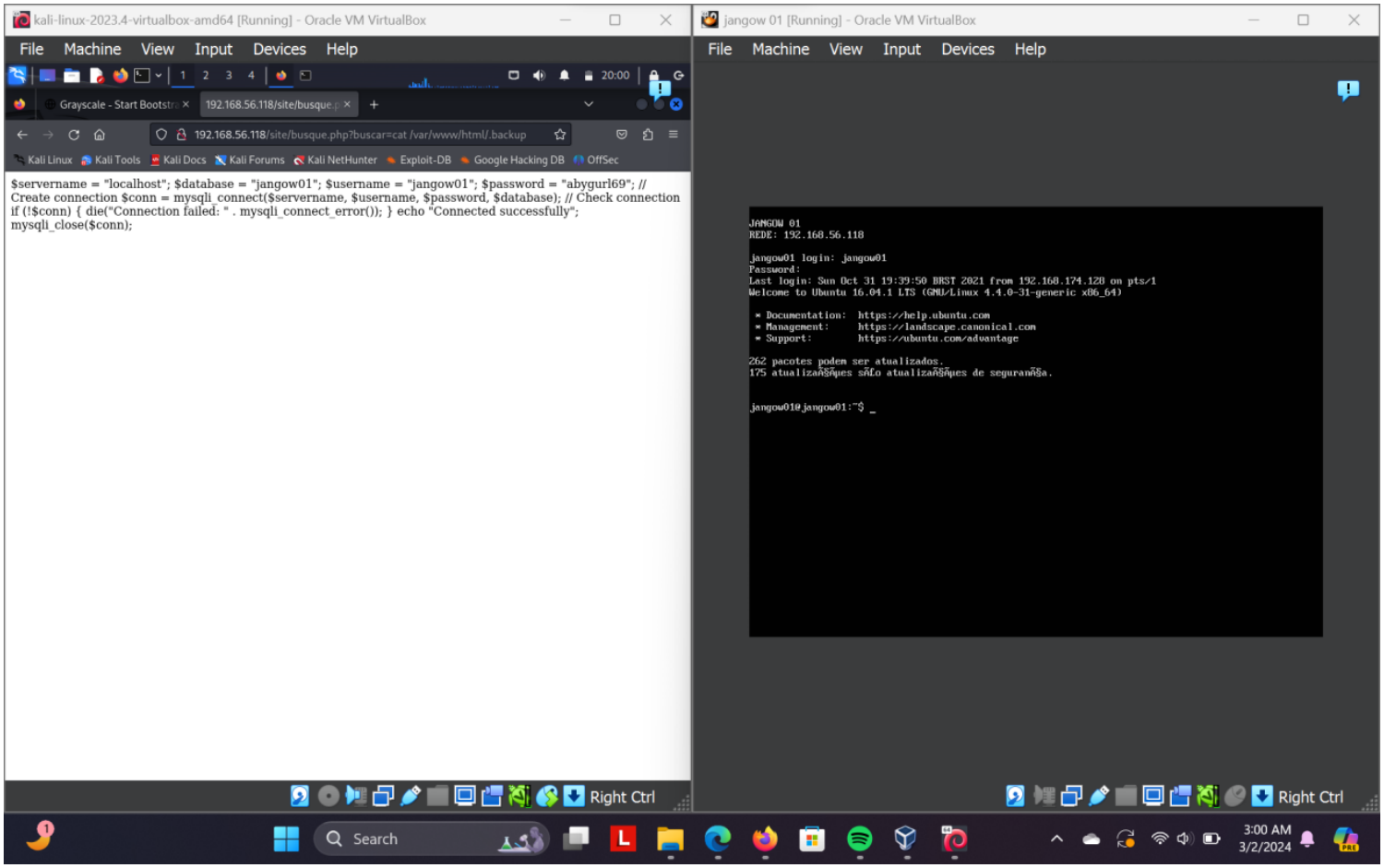


After discovering the hidden directory named 'backup' within '/var/www/html/', I attempted to access it by using the URL http://192.168.56.118/site/busque.php?buscar=ls -a /var/www/html/.backup.

My attempt to access the hidden directory 'backup' was successful. The page displayed database information, including a username and a password.


kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
192.168.56.118/site/busque.php?buscar=cat%20 /var/www/html/.backup
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
$servername = "localhost"; $database = "jangow01"; $username = "jangow01"; $password = "abygurl69"; // Create connection $conn = mysqli_connect($servername, $username, $password, $database); // Check connection if (!$conn) { die("Connection failed: " . mysqli_connect_error()); } echo "Connected successfully"; mysqli_close($conn);
Right Ctrl
Recycle Bin
MongoDB...
Computer Science
Microsoft Edge
Visual Studio Code
Avira
PDF X
GitHub Desktop
Discord
Oracle VM VirtualBox
Search
2:05 AM
3/2/2024

Logging In



After retrieving the username and password, I successfully logged into Jangow 01.🥳