

Lab 3: Perform a Web Server Hacking using AI

Lab Scenario

The objective of this lab is to simulate the process of hacking a web server using AI-driven tools and techniques. This exercise will involve footprinting, fingerprinting, and exploiting vulnerabilities to understand the security posture of the target web server.

Lab Objectives

- Perform Web Server Footprinting and Attacks using ShellGPT

Overview of Web Server Hacking using AI

In the realm of cybersecurity, the role of artificial intelligence (AI) has become increasingly significant, especially in the domain of ethical hacking. AI-powered tools and techniques provide ethical hackers with enhanced capabilities to discover vulnerabilities, automate attacks, and strengthen defenses. Web server hacking, a critical aspect of penetration testing, leverages AI to perform footprinting, fingerprinting, and exploitation more efficiently and effectively.

Task 1: Perform Web Server Footprinting and Attacks using ShellGPT

Web server footprinting and subsequent attacks are critical steps in penetration testing or ethical hacking to assess the security posture of a target organization. ShellGPT, an AI-driven tool, enhances these processes by automating information gathering, fingerprinting, and vulnerability identification tasks.

Here we will use ShellGPT to perform Webserver footprinting and attacks using ShellGPT.

The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the diverse environments in which it operates. As a result, you may observe differences in command syntax, execution, and results while performing this lab task.

1. Before starting this lab, click [Parrot Security](#) to switch to the **Parrot Security** machine and incorporate ShellGPT by following steps provided in [Integrate ShellGPT in Parrot Security Machine.pdf](#).

Alternatively, you can follow the steps to integrate **ShellGPT** provided in **Module 00: Integrate ShellGPT in Parrot Security Machine**.

2. To perform directory traversal using ShellGPT, run **sgpt --shell "Perform a directory traversal on target url https://certifiedhacker.com using gobuster"** command.

In the prompt type **E** and press **Enter** to execute the command.

```
Applications Places System [Icons] [System Tray] Wed May 22, 01:14
sgpt --shell "Perform a directory traversal on target url https://certifiedhacker.com using gobuster" - Parrot Terminal
File Edit View Search Terminal Help

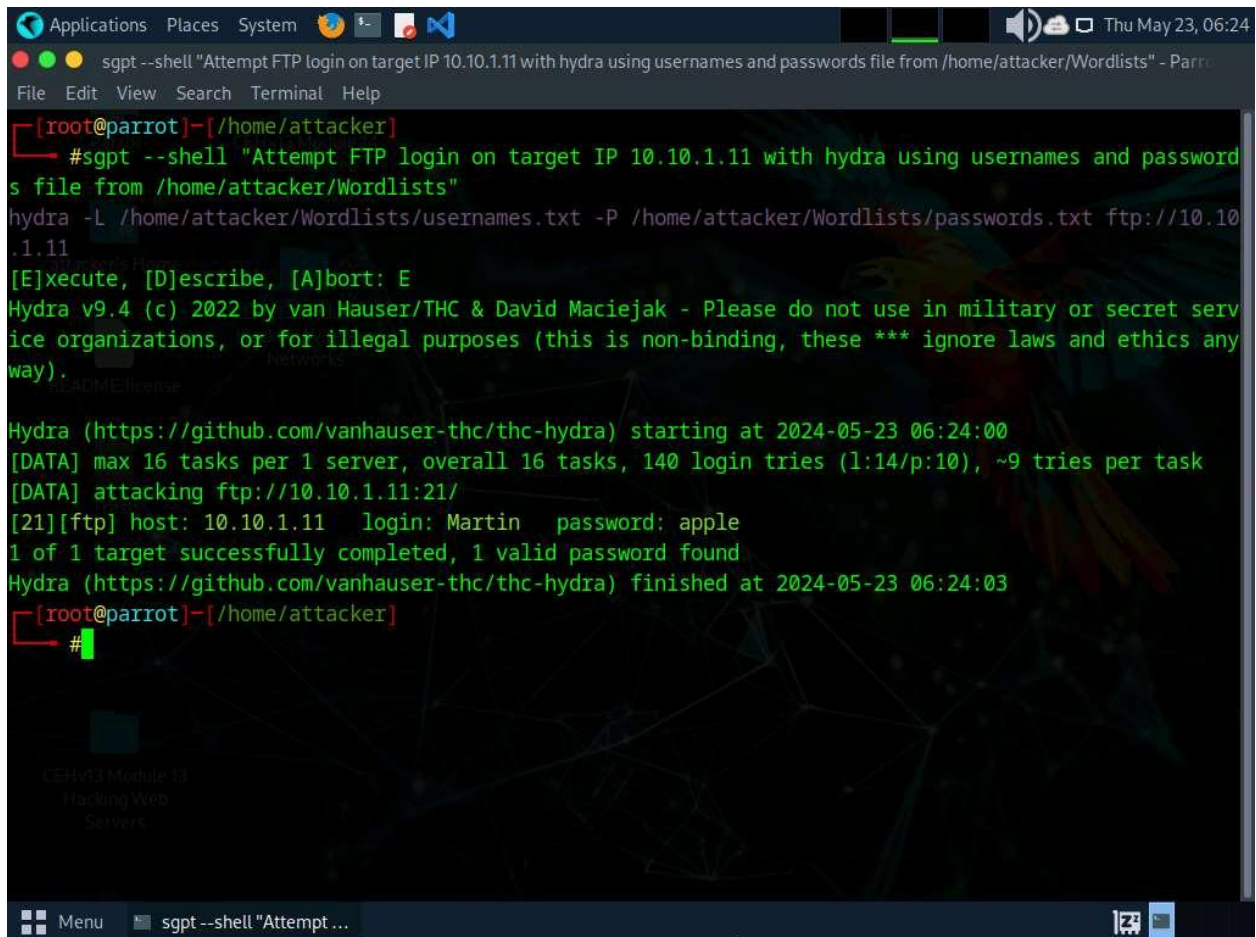
[root@parrot]~/home/attacker
#sgpt --shell "Perform a directory traversal on target url https://certifiedhacker.com using gobuster"

gobuster dir -u https://certifiedhacker.com -w /usr/share/wordlists/dirb/common.txt
[E]xecute, [D]escribe, [A]bort: E

=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          https://certifiedhacker.com
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2024/05/22 01:13:10 Starting gobuster
=====
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/blog (Status: 301)
/cgi-bin (Status: 301)
/cgi-bin/ (Status: 403)
/cgi-sys (Status: 301)
/controlpanel (Status: 200)
/cpanel (Status: 200)
```

3. To perform FTP bruteforce attack run **sgpt --shell "Attempt FTP login on target IP 10.10.1.11 with hydra using usernames and passwords file from /home/attacker/Wordlists"** command.

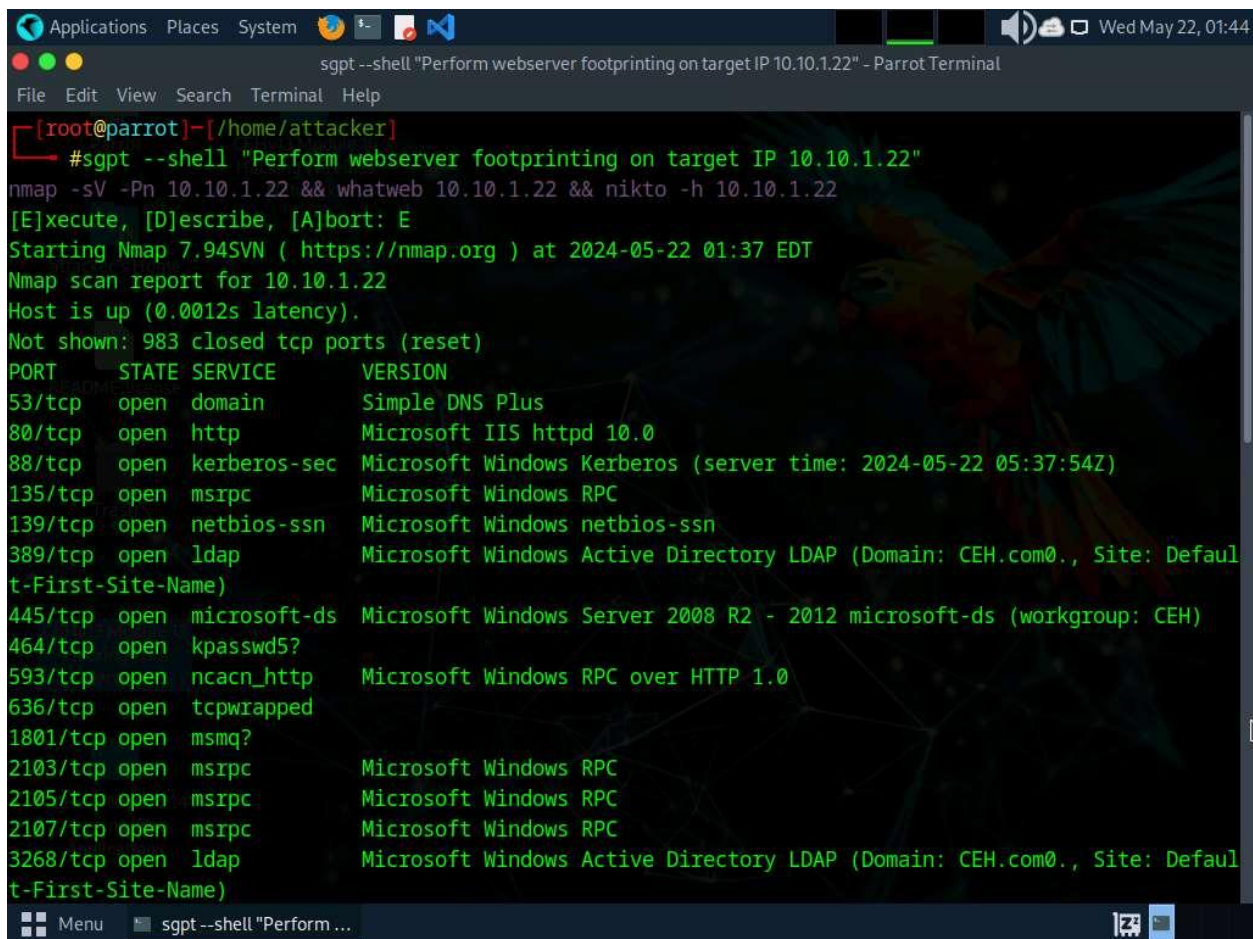
In the prompt type **E** and press **Enter** to execute the command.



```
[root@parrot]~/home/attacker
#sgpt --shell "Attempt FTP login on target IP 10.10.1.11 with hydra using usernames and passwords file from /home/attacker/Wordlists"
hydra -L /home/attacker/Wordlists/usernames.txt -P /home/attacker/Wordlists/passwords.txt ftp://10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-23 06:24:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 140 login tries (l:14/p:10), ~9 tries per task
[DATA] attacking ftp://10.10.1.11:21/
[21][ftp] host: 10.10.1.11 login: Martin password: apple
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-23 06:24:03
[root@parrot]~/home/attacker
#
```

4. To perform webserver footprinting on target IP address using ShellGPT, run **sgpt --shell "Perform webserver footprinting on target IP 10.10.1.22"** command.

In the prompt type **E** and press **Enter** to execute the command.

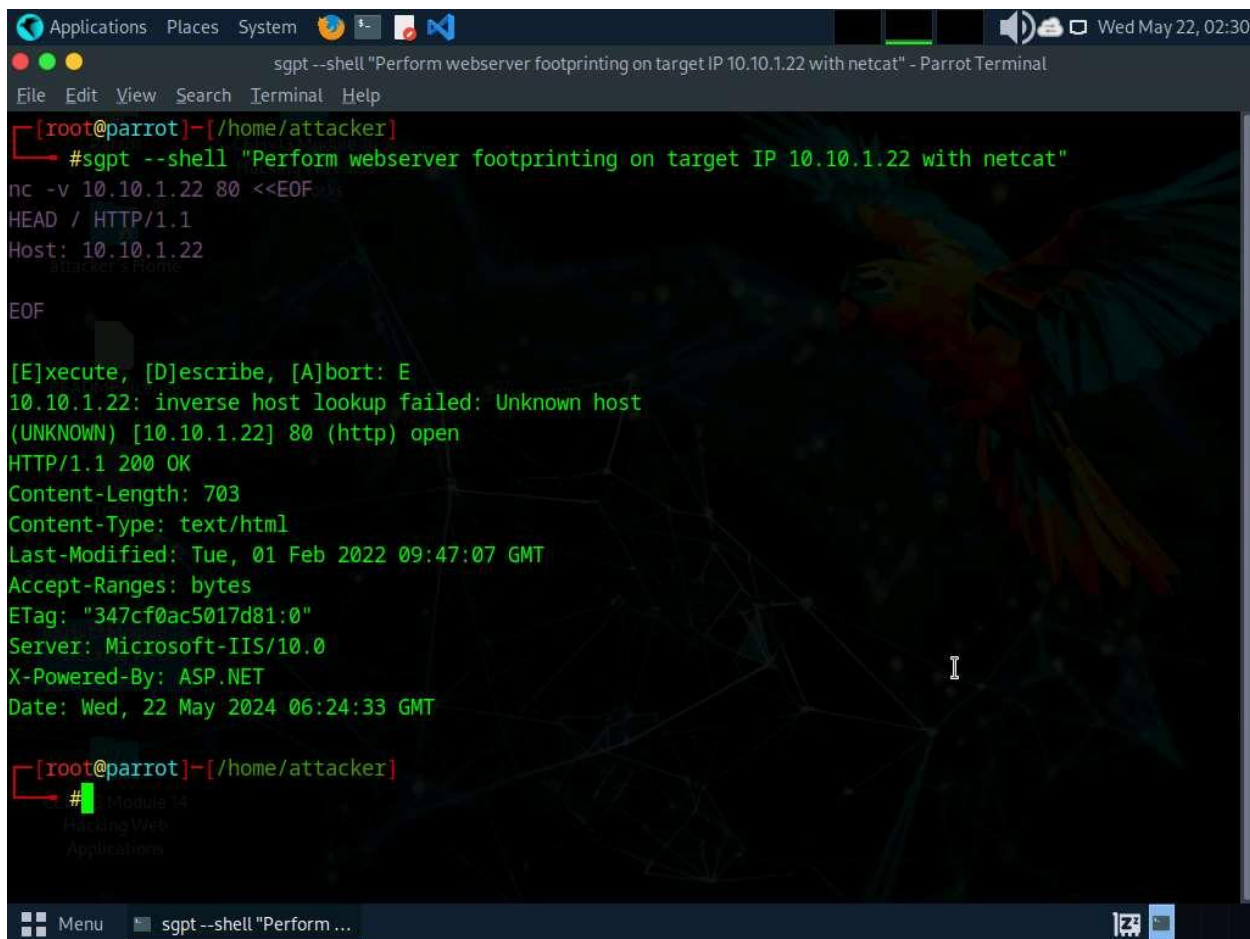


The screenshot shows a Parrot Terminal window with the title bar "sgpt --shell 'Perform webserver footprinting on target IP 10.10.1.22' - Parrot Terminal". The terminal content is as follows:

```
[root@parrot]~/home/attacker]
#sgpt --shell "Perform webserver footprinting on target IP 10.10.1.22"
nmap -sV -Pn 10.10.1.22 && whatweb 10.10.1.22 && nikto -h 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 01:37 EDT
Nmap scan report for 10.10.1.22
Host is up (0.0012s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
80/tcp    open  http             Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2024-05-22 05:37:54Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (Domain: CEH.com0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CEH)
464/tcp   open  kpasswd5?        Microsoft Windows RPC
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1801/tcp  open  msmq?
2103/tcp  open  msrpc            Microsoft Windows RPC
2105/tcp  open  msrpc            Microsoft Windows RPC
2107/tcp  open  msrpc            Microsoft Windows RPC
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: CEH.com0., Site: Default-First-Site-Name)
```

5. Run **sgpt --shell "Perform webserver footprinting on target IP 10.10.1.22 with netcat"** command to perform web server footprinting using netcat.

In the prompt type **E** and press **Enter** to execute the command.



```
Applications  Places  System  [Icons]  [Volume]  [Network]  [Battery]  Wed May 22, 02:30
sgpt --shell "Perform webservice footprinting on target IP 10.10.1.22 with netcat" - Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]~/home/attacker
#sgpt --shell "Perform webservice footprinting on target IP 10.10.1.22 with netcat"
nc -v 10.10.1.22 80 <<EOF
HEAD / HTTP/1.1
Host: 10.10.1.22
EOF

[E]xecute, [D]escribe, [A]bort: E
10.10.1.22: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.1.22] 80 (http) open
HTTP/1.1 200 OK
Content-Length: 703
Content-Type: text/html
Last-Modified: Tue, 01 Feb 2022 09:47:07 GMT
Accept-Ranges: bytes
ETag: "347cf0ac5017d81:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 22 May 2024 06:24:33 GMT

[root@parrot]~/home/attacker
# [Module 14]
Hacking Web
Applications
```

6. To perform website mirroring using ShellGPT, run **sgpt --shell "Mirror the target website certifiedhacker.com"** command.

Alternatively you can use Htttrack to mirror a target website, to do so run **sgpt --shell "Mirror the target website <https://certifiedhacker.com> with htttrack on desktop"** command.

In the prompt type **E** and press **Enter** to execute the command.

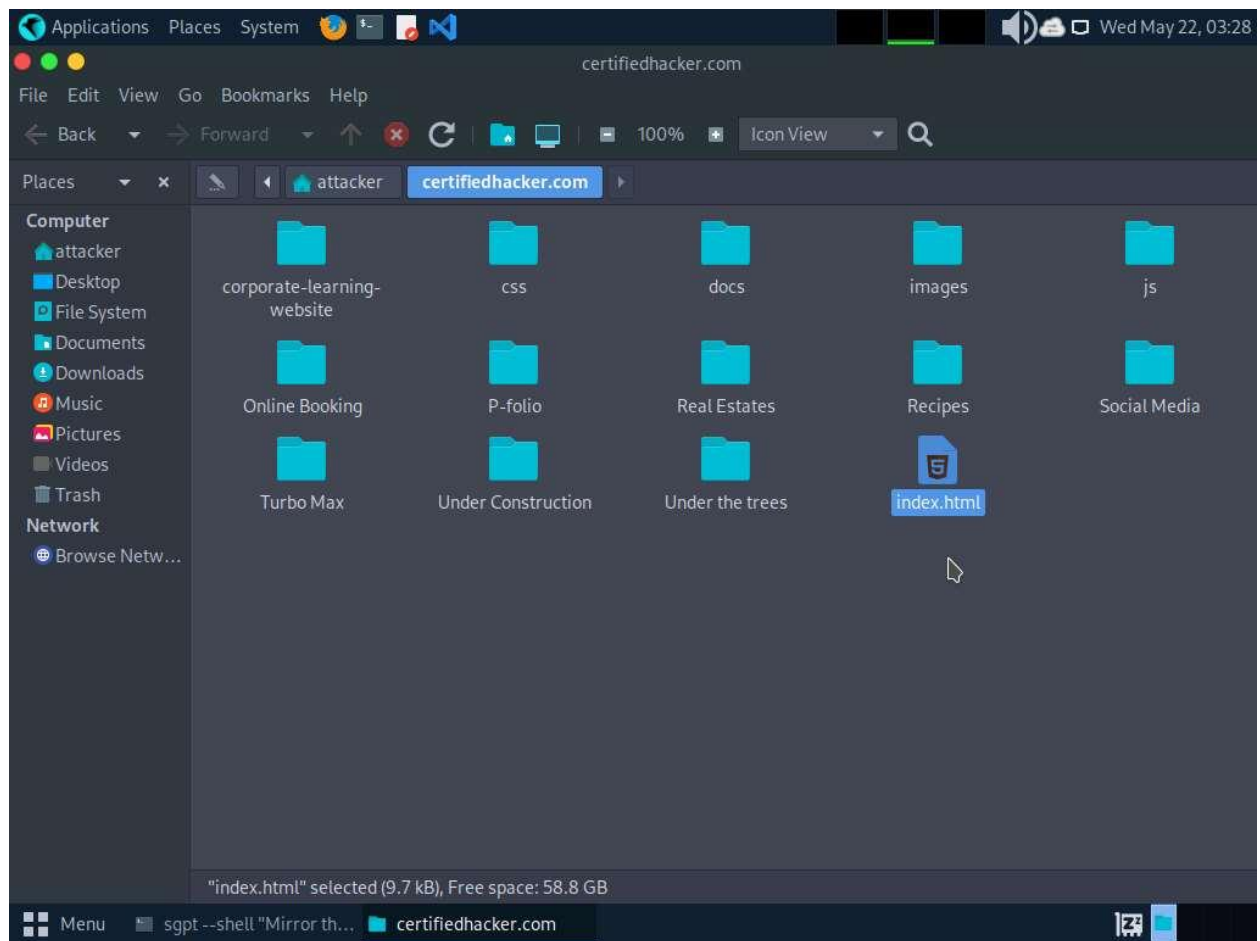
```
Applications Places System [Icons] [Volume] [Network] [Battery] Wed May 22, 03:26
sgpt --shell "Mirror the target website certifiedhacker.com" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
#sgpt --shell "Mirror the target website certifiedhacker.com"
wget --mirror --convert-links --adjust-extension --page-requisites --no-parent http://certifiedhacker
.com
[E]xecute, [D]escribe, [A]bort: E
--2024-05-22 03:24:06-- http://certifiedhacker.com/
Resolving certifiedhacker.com (certifiedhacker.com)... 162.241.216.11
Connecting to certifiedhacker.com (certifiedhacker.com)|162.241.216.11|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://certifiedhacker.com/ [following]
--2024-05-22 03:24:06-- https://certifiedhacker.com/
Connecting to certifiedhacker.com (certifiedhacker.com)|162.241.216.11|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9660 (9.4K) [text/html]
Saving to: 'certifiedhacker.com/index.html'

certifiedhacker.com/index 100%[=====] 9.43K --.-KB/s in 0.07s

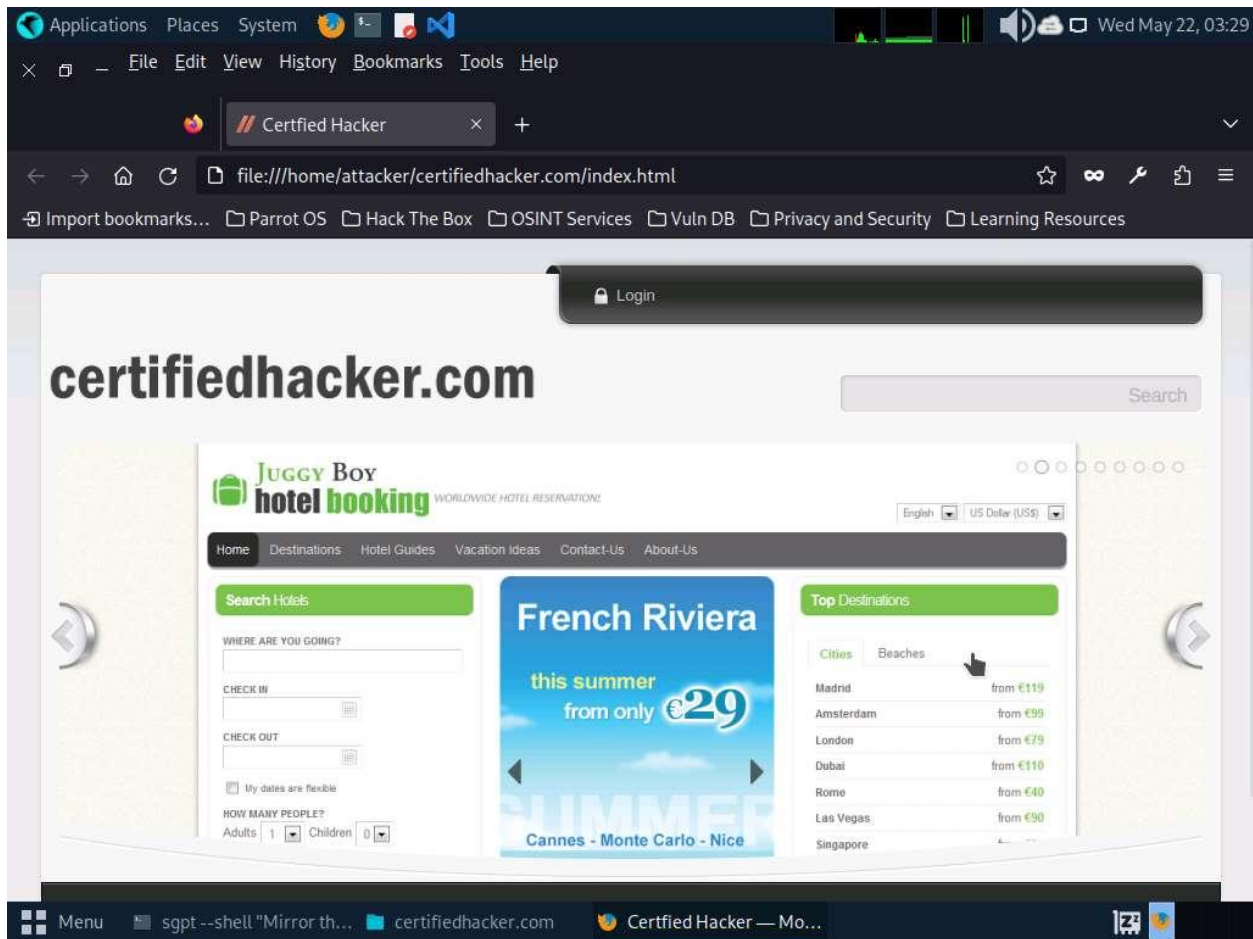
2024-05-22 03:24:07 (134 KB/s) - 'certifiedhacker.com/index.html' saved [9660/9660]

Loading robots.txt; please ignore errors.
--2024-05-22 03:24:07-- https://certifiedhacker.com/robots.txt
Reusing existing connection to certifiedhacker.com:443.
HTTP request sent, awaiting response... 404 Not Found
2024-05-22 03:24:07 ERROR 404: Not Found.
```

7. To view the mirrored website navigate to **Places -> Home Folder -> certifiedhacker.com** location and double-click on **index.html** file.



8. The mirrored certifiedhacker.com website opens up in Firefox browser.



9. Apart from the aforementioned commands, you can further use ShellGPT prompts to perform Web Server Hacking.
10. This concludes the demonstration of webserver footprinting and attacks using ShellGPT.
11. Close all open windows and document all the acquired information.

Question 13.3.1.1

In Parrot Security machine, use ShellGPT to write and execute a prompt to perform directory traversal attack on <https://certifiedhacker.com> website using gobuster. Enter the status code of /docs directory of certifiedhacker.com that is displayed in the gobuster tool