

# Lab 4: Perform Web Application Hacking using AI

## Lab Scenario

Hacking web applications using AI involves leveraging advanced machine learning techniques to exploit vulnerabilities in web applications. This approach can automate and enhance the traditional methods of penetration testing and vulnerability assessment.

The labs in this exercise demonstrate how to perform web application hacking using AI.

## Lab Objectives

- Perform web application hacking using ShellGPT

## Overview of Web Application Hacking using AI

Web application hacking using AI represents a sophisticated evolution in cyber threats, leveraging advanced machine learning algorithms and techniques to identify vulnerabilities, create exploits, bypass defenses, and extract sensitive information from web applications.

### Task 1: Perform Web Application Hacking using ShellGPT

Web application hacking with ShellGPT involves leveraging AI-generated commands to exploit vulnerabilities, execute code injections, bypass security measures like WAFs, and extract sensitive data. It automates attack vectors, adapts to defenses, and poses a sophisticated threat requiring advanced defensive strategies.

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. After incorporating the ShellGPT API in Parrot Security Machine, in the terminal window run **sgpt --shell "Check if the target url www.certifiedhacker.com has web application firewall"** command to detect WAF using ShellGPT.

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

```
Applications Places System [Icons] [Volume] [Network] [Battery] Wed May 22, 06:27
sgpt --shell "Check if the target url www.certifiedhacker.com has web application firewall" - Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]~/home/attacker
#sgpt --shell "Check if the target url www.certifiedhacker.com has web application firewall"
nmap -p 80,443 --script http-waf-detect www.certifiedhacker.com
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 06:26 EDT
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.14s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
| http-waf-detect: IDS/IPS/WAF detected:
|_www.certifiedhacker.com:443/?p4yl04d3=<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 12.74 seconds
[root@parrot]~/home/attacker
#
```

- Now, run **sgpt --shell "Check if the target url https://www.certifiedhacker.com is protected with web application firewall using wafwoof"** command to check for WAF using wafwoof.

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



[illegible]

```
Applications Places System [Icons] [System Tray] Wed May 22, 06:55
sgpt --chat HWA --shell "Launch whatweb on the target website www.moviescope.com to perform website footprinting. Run a verbose scan
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
#sgpt --chat HWA --shell "Launch whatweb on the target website www.moviescope.com to perform web
site footprinting. Run a verbose scan and print the output. Save the results in file whatweb_log.txt.
"
whatweb -v www.moviescope.com | tee whatweb_log.txt
[E]xecute, [D]escribe, [A]bort: E
WhatWeb report for http://www.moviescope.com
Status      : 200 OK
Title       : Login - MovieScope
IP          : 10.10.1.19
Country     : RESERVED, ZZ

Summary     : ASP.NET[4.0.30319], HTTPServer[Microsoft-IIS/10.0], Meta-Author[EC-Council], Microsoft-II
S[10.0], Modernizr, PasswordField[txtpwd], Script, X-Powered-By[ASP.NET]

Detected Plugins:
[ ASP.NET ]
    ASP.NET is a free web framework that enables great Web
    applications. Used by millions of developers, it runs some
    of the biggest sites in the world.

    Version      : 4.0.30319 (from X-AspNet-Version HTTP header)
    Google Dorks: (2)
    Website      : https://www.asp.net/

[ HTTPServer ]
```

6. Now run **sgpt --shell "Perform the Vulnerability scan on the target url **www.moviescope.com**"** command to identify web application vulnerabilities on a target website.

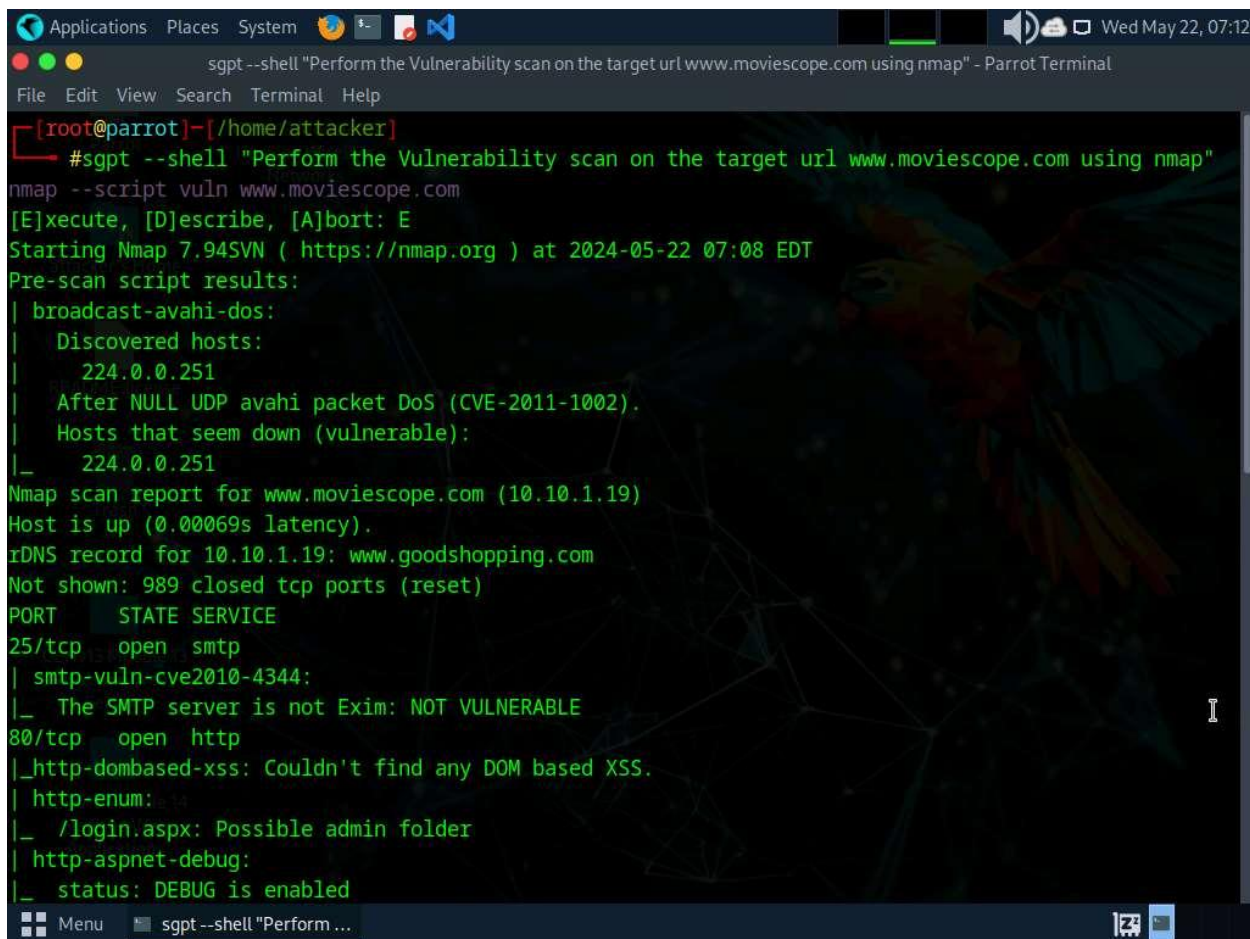
In the prompt type **E** and press **Enter** to execute the command.



```
Applications Places System [Icons] [System Tray] Wed May 22, 07:06
sgpt --shell "Perform the Vulnerability scan on the target url www.moviescope.com" - Parrot Terminal
File Edit View Search Terminal Help
[~]xecute, [D]escribe, [A]bort: E
- Nikto v2.5.0
-----
+ Target IP: 10.10.1.19
+ Target Hostname: www.moviescope.com
+ Target Port: 80
+ Start Time: 2024-05-22 07:05:46 (GMT-4)
-----
+ Server: Microsoft-IIS/10.0
+ /: Retrieved x-aspnet-version header: 4.0.30319.
+ /: Retrieved x-powered-by header: ASP.NET.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ 8232 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2024-05-22 07:06:03 (GMT-4) (17 seconds)
-----
+ 1 host(s) tested
[~root@parrot]~[/home/attacker]
#
```

7. Run **sgpt --shell "Perform the Vulnerability scan on the target url www.moviescope.com using nmap"** command to perform web application scanning using Nmap.

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



```
[root@parrot]~/home/attacker
#sgpt --shell "Perform the Vulnerability scan on the target url www.moviescope.com using nmap"
nmap --script vuln www.moviescope.com
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 07:08 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|   Hosts that seem down (vulnerable):
|_   224.0.0.251
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00069s latency).
rDNS record for 10.10.1.19: www.goodshopping.com
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
80/tcp    open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /login.aspx: Possible admin folder
| http-aspnet-debug:
|_  status: DEBUG is enabled
```

8. To perform a vulnerability scan on web application using Sniper tool run **sgpt --shell "Use Sn1per tool and scan the target url www.moviescope.com for web vulnerabilities and save result in file scan3.txt"** command.

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





```
Applications Places System [Icons] [Volume] [Network] [Battery] Wed May 22, 08:12
sgpt --shell "Scan the web content of the target url www.moviescope.com using Dirb" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker]
#sgpt --shell "Scan the web content of the target url www.moviescope.com using Dirb"
dirb http://www.moviescope.com
[E]xecute, [D]escribe, [A]bort: E

-----
attacker's Home
DIRB v2.22
By The Dark Raver
-----
README license

START_TIME: Wed May 22 08:11:41 2024
URL_BASE: http://www.moviescope.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

CEH v13 Module 13
---- Scanning URL: http://www.moviescope.com/ ----
==> DIRECTORY: http://www.moviescope.com/css/
==> DIRECTORY: http://www.moviescope.com/db/
==> DIRECTORY: http://www.moviescope.com/DB/
==> DIRECTORY: http://www.moviescope.com/images/
==> DIRECTORY: http://www.moviescope.com/Images/
==> DIRECTORY: http://www.moviescope.com/js/
==> DIRECTORY: http://www.moviescope.com/twitter/

Menu sgpt --shell "Scan the ... [Zoom] [Close]
```

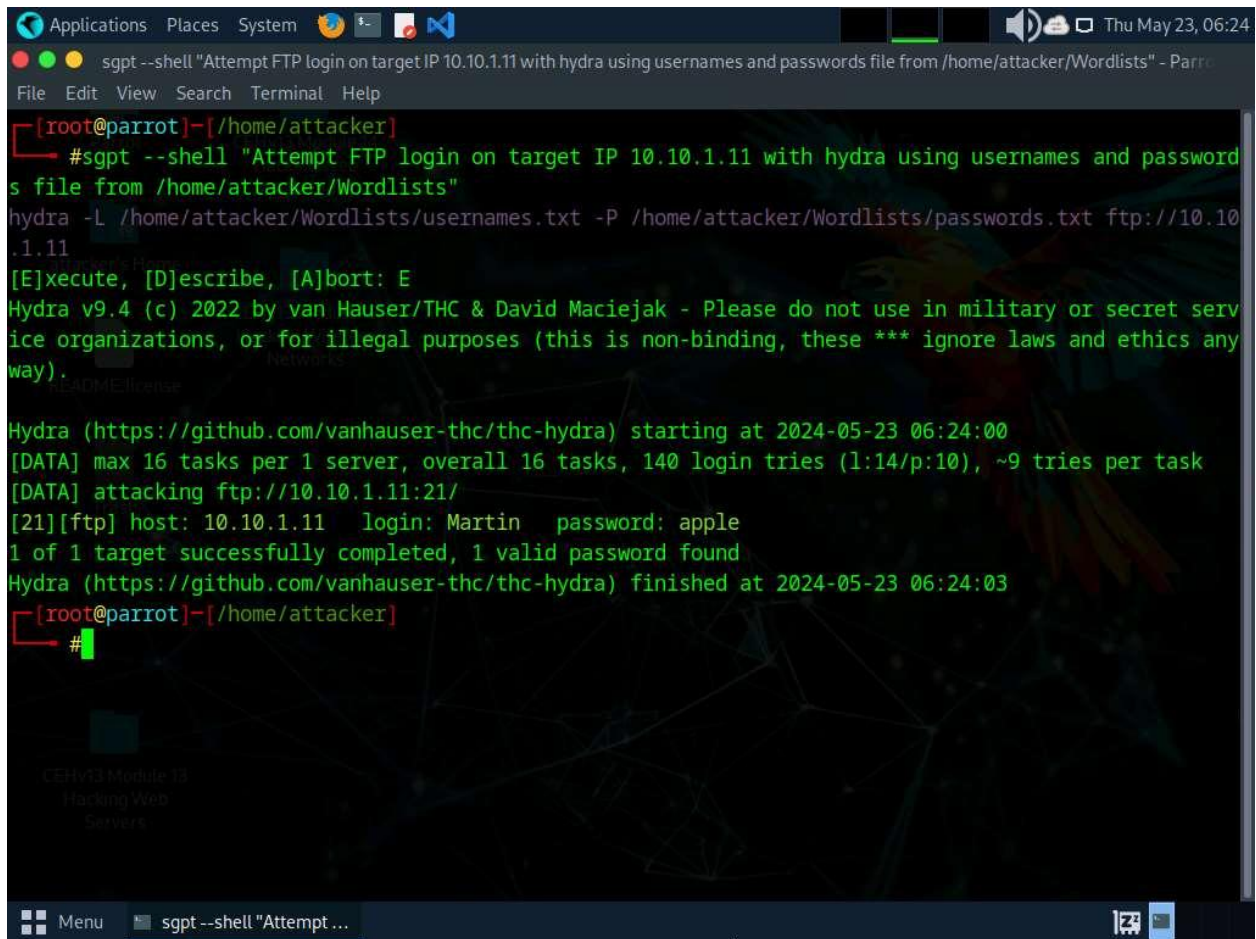
10. Run **sgpt --shell "Scan the web content of target url www.moviescope.com using Gobuster"** command to identify directories using Gobuster.

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

```
Applications Places System [Icons] [System Tray] Wed May 22, 08:17
sgpt --shell "Scan the web content of target url www.moviescope.com using Gobuster" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker]
#sgpt --shell "Scan the web content of target url www.moviescope.com using Gobuster"
gobuster dir -u http://www.moviescope.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: http://www.moviescope.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 08:17:16 Starting gobuster
=====
/css (Status: 301)
/db (Status: 301)
/DB (Status: 301)
/images (Status: 301)
/Images (Status: 301)
/js (Status: 301)
/twitter (Status: 301)
=====
2024/05/22 08:17:18 Finished
Menu sgpt --shell "Scan the ... [Icons]
```

11. 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.



```
Applications Places System Thu May 23, 06:24
sgpt --shell "Attempt FTP login on target IP 10.10.1.11 with hydra using usernames and passwords file from /home/attacker/Wordlists" - Parrot
File Edit View Search Terminal Help
[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
#
```

12. Run **sgpt --chat wah --shell "create and run a custom script for web application footprinting and vulnerability scanning. The target url is [www.certifiedhacker.com](http://www.certifiedhacker.com)"** to automate web application hacking tasks with custom scripts.

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

```
Applications  Places  System  Wed May 22, 08:23
sgpt --chat wah --shell "create and run a custom script for web application footprinting and vulnerability scanning. The target url is www.cer
File Edit View Search Terminal Help
[root@parrot]~/home/attacker]
#sgpt --chat wah --shell "create and run a custom script for web application footprinting and vu
lnerability scanning. The target url is www.certifiedhacker.com"
echo '#!/bin/bash
target="www.certifiedhacker.com"

# Web Application Footprinting
echo "Starting web application footprinting for $target"
whatweb $target
wafw00f $target

# Vulnerability Scanning
echo "Starting vulnerability scanning for $target"
nikto -h $target
nmap -sV --script=http-vuln* $target

# Save results
mkdir -p ~/scans/$target
whatweb $target > ~/scans/$target/footprinting.txt
wafw00f $target >> ~/scans/$target/footprinting.txt
nikto -h $target > ~/scans/$target/vulnerability_scan.txt
nmap -sV --script=http-vuln* $target >> ~/scans/$target/vulnerability_scan.txt

echo "Scanning completed for $target"
' > footprint_vuln_scan.sh && chmod +x footprint_vuln_scan.sh && ./footprint_vuln_scan.sh
[E]xecute, [D]escribe, [A]bort: E
Menu  sgpt --chat wah --shel...
```



```
Applications Places System sgpt --chat wah --shell "create and run a custom script for web application footprinting and vulnerability scanning. The target url is www.cer
File Edit View Search Terminal Help
http://www.certifiedhacker.com [301 Moved Permanently] Apache, Country[UNITED STATES][US], HTTPServer
[Apache], IP[162.241.216.11], RedirectLocation[https://www.certifiedhacker.com/], Title[301 Moved Per
manently]
https://www.certifiedhacker.com/ [200 OK] Country[UNITED STATES][US], HTTPServer[nginx/1.21.6], IP[16
2.241.216.11], JQuery[1.4], Meta-Author[Parallelus], PasswordField[RevealPassword], Script[text/javas
cript], Title[Certified Hacker], UncommonHeaders[host-header,x-server-cache,x-proxy-cache], nginx[1.21
.6]

( Woof! )

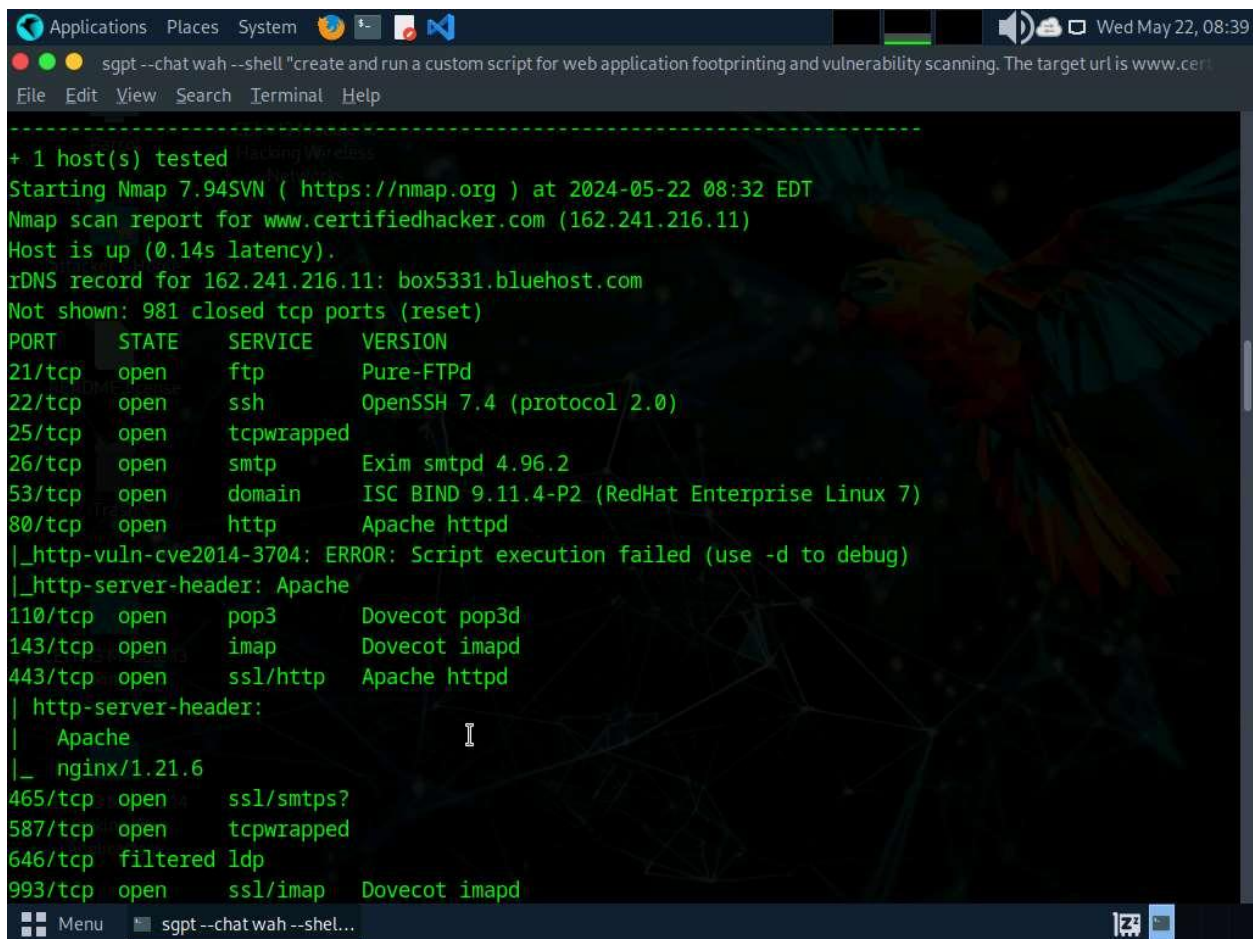
( ) ; |==| ( )
/ ( ' / \
( / ) / | \
\ ( _ _ ) / | \

~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.certifiedhacker.com
[+] The site https://www.certifiedhacker.com is behind ModSecurity (SpiderLabs) WAF.
[~] Number of requests: 2
Starting vulnerability scanning for www.certifiedhacker.com

Menu sgpt --chat wah --shell...
```

```
Applications Places System [Icons] [System Tray] Wed May 22, 08:39
sgpt --chat wah --shell "create and run a custom script for web application footprinting and vulnerability scanning. The target url is www.certifiedhacker.com"
File Edit View Search Terminal Help
[~] Number of requests: 2
Starting vulnerability scanning for www.certifiedhacker.com
- Nikto v2.5.0
-----
+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 80
+ Start Time: 2024-05-22 08:23:27 (GMT-4)
-----
+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.certifiedhacker.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Uncommon header 'host-header' found, with contents: c2hhcmVkJmJsdWVob3N0LmNvbQ==.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time: 2024-05-22 08:32:50 (GMT-4) (563 seconds)
-----
+ 1 host(s) tested
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 08:32 EDT
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.14s latency).
```



```
-----
+ 1 host(s) tested
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 08:32 EDT
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.14s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 981 closed tcp ports (reset)
PORT      STATE      SERVICE      VERSION
21/tcp    open       ftp          Pure-FTPD
22/tcp    open       ssh          OpenSSH 7.4 (protocol 2.0)
25/tcp    open       tcpwrapped
26/tcp    open       smtp         Exim smtpd 4.96.2
53/tcp    open       domain       ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp    open       http         Apache httpd
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Apache
110/tcp   open       pop3         Dovecot pop3d
143/tcp   open       imap         Dovecot imapd
443/tcp   open       ssl/http     Apache httpd
| http-server-header:
|   Apache
|_  nginx/1.21.6
465/tcp   open       ssl/smtps?
587/tcp   open       tcpwrapped
646/tcp   filtered  ldap
993/tcp   open       ssl/imap     Dovecot imapd
```

13. To create a custom python script for web application scanning run **sgpt --chat wah --shell "create and run a custom python script for web application footprinting and vulnerability scanning. The target url is www.certifiedhacker.com"** command.

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

```
Applications  Places  System  [Icons]  [Volume]  [Network]  [Battery]  Wed May 22, 08:45
sgpt --chat wah --shell "create and run a custom python script for web application footprinting and vulnerability scanning. The target url is www.certifiedhacker.com"
File Edit View Search Terminal Help

[root@parrot]~/home/attacker
#sgpt --chat wah --shell "create and run a custom python script for web application footprinting
and vulnerability scanning. The target url is www.certifiedhacker.com"
echo 'import os

# Web Application Footprinting
print(f"Starting web application footprinting for {target}")
os.system(f"whatweb {target}")
os.system(f"wafw00f {target}")

# Vulnerability Scanning
print(f"Starting vulnerability scanning for {target}")
os.system(f"nikto -h {target}")
os.system(f"nmap -sV --script=http-vuln* {target}")

# Save results
os.makedirs(f"~/scans/{target}", exist_ok=True)
with open(f"~/scans/{target}/footprinting.txt", "w") as footprint_file:
    footprint_file.write(os.popen(f"whatweb {target}").read())
    footprint_file.write(os.popen(f"wafw00f {target}").read())

with open(f"~/scans/{target}/vulnerability_scan.txt", "w") as vuln_scan_file:
    vuln_scan_file.write(os.popen(f"nikto -h {target}").read())
    vuln_scan_file.write(os.popen(f"nmap -sV --script=http-vuln* {target}").read())'

Menu  sgpt --chat wah --shel...
```



```
Applications Places System [Icons] [System Tray] Wed May 22, 08:47
sgpt --chat wah --shell "create and run a custom python script for web application footprinting and vulnerability scanning. The target url is www
File Edit View Search Terminal Help
manently]
https://www.certifiedhacker.com/ [200 OK] Country[UNITED STATES][US], HTTPServer[nginx/1.21.6], IP[16
2.241.216.11], JQuery[1.4], Meta-Author[Parallelus], PasswordField[RevealPassword], Script[text/javas
cript], Title[Certified Hacker], UncommonHeaders[host-header,x-server-cache,x-proxy-cache], nginx[1.21
.6]
attacker's Home
( W00f! )
README license
Trash *===*
CERTIFIED HACKER
Hacking Tools
Servers
404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://www.certifiedhacker.com
[+] The site https://www.certifiedhacker.com is behind ModSecurity (SpiderLabs) WAF.
[~] Number of requests: 2
Menu sgpt --chat wah --shel...
```

```
Applications Places System [Icons] [System Tray] Wed May 22, 08:59
sgpt --chat wah --shell "create and run a custom python script for web application footprinting and vulnerability scanning. The target url is www
File Edit View Search Terminal Help
[*] Checking https://www.certifiedhacker.com
[+] The site https://www.certifiedhacker.com is behind ModSecurity (SpiderLabs) WAF.
[~] Number of requests: 2
Starting vulnerability scanning for www.certifiedhacker.com
- Nikto v2.5.0
-----
+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 80
+ Start Time: 2024-05-22 08:46:07 (GMT-4)
-----
+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.certifiedhacker.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Uncommon header 'host-header' found, with contents: c2hhcmVkJmJsdWVob3N0LmNvbQ==.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timout): Operation now in progress
+ Scan terminated: 19 error(s) and 3 item(s) reported on remote host
+ End Time: 2024-05-22 08:55:20 (GMT-4) (553 seconds)
-----
+ 1 host(s) tested
Menu sgpt --chat wah --shell...
```

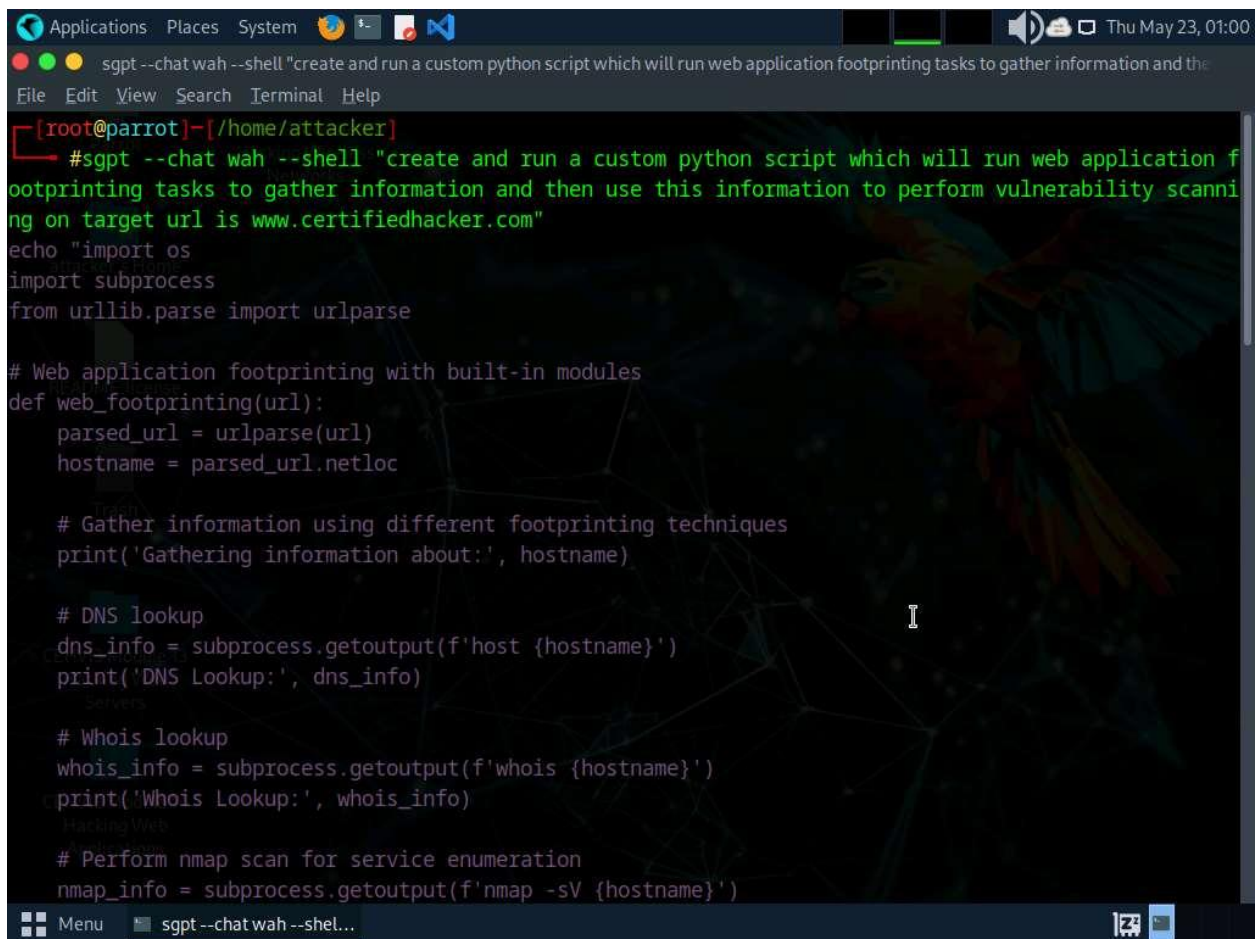
```
Applications Places System sgpt --chat wah --shell "create and run a custom python script for web application footprinting and vulnerability scanning. The target url is www.certifiedhacker.com"
File Edit View Search Terminal Help

-----
+ 1 host(s) tested
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 08:55 EDT
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.14s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 980 closed tcp ports (reset)
PORT      STATE      SERVICE      VERSION
21/tcp    open      ftp          Pure-FTPd
22/tcp    open      ssh         OpenSSH 7.4 (protocol 2.0)
25/tcp    open      smtp        Exim smtpd 4.96.2
26/tcp    open      smtp        Exim smtpd 4.96.2
53/tcp    open      domain      ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp    filtered  http
110/tcp   open      pop3        Dovecot pop3d
143/tcp   open      imap        Dovecot imapd
443/tcp   open      ssl/http    Apache httpd
| http-server-header:
|   Apache
|_  nginx/1.21.6
465/tcp   open      ssl/smtp    Exim smtpd 4.96.2
587/tcp   open      smtp        Exim smtpd 4.96.2
646/tcp   filtered  ldp
993/tcp   open      ssl/imap    Dovecot imapd
995/tcp   open      ssl/pop3    Dovecot pop3d
2222/tcp  open      ssh         OpenSSH 7.4 (protocol 2.0)

Menu sgpt --chat wah --shell...
```

14. To create a custom python script for web application scanning run **sgpt --chat wah --shell "create and run a custom python script which will run web application footprinting tasks to gather information and then use this information to perform vulnerability scanning on target url is www.certifiedhacker.com"** command.

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



The image shows a terminal window with a dark background and a parrot illustration. The terminal title bar includes 'Applications', 'Places', 'System', and system icons. The prompt is '[root@parrot]~/home/attacker'. The command executed is '#sgpt --chat wah --shell "create and run a custom python script which will run web application footprinting tasks to gather information and then use this information to perform vulnerability scanning on target url is www.certifiedhacker.com"'. The script defines a function 'web\_footprinting(url)' that uses 'urllib.parse' to get the hostname and then performs 'DNS lookup', 'Whois lookup', and an 'nmap scan' using 'subprocess'.

```
Applications Places System Thu May 23, 01:00
sgpt --chat wah --shell "create and run a custom python script which will run web application footprinting tasks to gather information and the
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
#sgpt --chat wah --shell "create and run a custom python script which will run web application footprinting tasks to gather information and then use this information to perform vulnerability scanning on target url is www.certifiedhacker.com"
echo "import os
import subprocess
from urllib.parse import urlparse

# Web application footprinting with built-in modules
def web_footprinting(url):
    parsed_url = urlparse(url)
    hostname = parsed_url.netloc

    # Gather information using different footprinting techniques
    print('Gathering information about:', hostname)

    # DNS lookup
    dns_info = subprocess.getoutput(f'host {hostname}')
    print('DNS Lookup:', dns_info)

    # Whois lookup
    whois_info = subprocess.getoutput(f'whois {hostname}')
    print('Whois Lookup:', whois_info)

    # Perform nmap scan for service enumeration
    nmap_info = subprocess.getoutput(f'nmap -sV {hostname}')
```

Menu sgpt --chat wah --shel...



```
Applications  Places  System  Thu May 23, 01:01
sgpt --chat wah --shell "create and run a custom python script which will run web application footprinting tasks to gather information and the
File Edit View Search Terminal Help
Gathering information about: www.certifiedhacker.com
DNS Lookup: www.certifiedhacker.com is an alias for certifiedhacker.com.
certifiedhacker.com has address 162.241.216.11
certifiedhacker.com mail is handled by 0 mail.certifiedhacker.com.
Whois Lookup: No match for "WWW.CERTIFIEDHACKER.COM".
>>> Last update of whois database: 2024-05-23T04:58:16Z <<<

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
```

```
Applications Places System [Icons] [System Tray] Thu May 23, 01:10
sgpt --chat wah --shell "create and run a custom python script which will run web application footprinting tasks to gather information and the
File Edit View Search Terminal Help
Nmap done: 1 IP address (1 host up) scanned in 150.80 seconds
Starting vulnerability scanning on: www.certifiedhacker.com
Nikto Scan Results: - Nikto v2.5.0
-----
+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 80
+ Start Time: 2024-05-23 01:01:09 (GMT-4)
-----
+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.certifiedhacker.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Uncommon header 'host-header' found, with contents: c2hhcmVkJmJsdWVob3N0LmNvbQ==.
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 19 error(s) and 3 item(s) reported on remote host
+ End Time: 2024-05-23 01:10:09 (GMT-4) (540 seconds)
-----
+ 1 host(s) tested
[red@parrot]~[/home/attacker]
#
```

15. To perform Web application fuzz testing using ShellGPT run **sgpt --shell "Fuzz the target url www.moviescope.com using Wfuzz tool"** command.

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

```
Applications Places System [Icons] [Terminal] [Parrot] [Volume] [Network] [Battery] [Date: Wed May 22, 09:05]
sgpt --shell "Fuzz the target url www.moviescope.com using Wfuzz tool" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
#sgpt --shell "Fuzz the target url www.moviescope.com using Wfuzz tool"
wfuzz -c -z file,/usr/share/wordlists/wfuzz/general/common.txt --hc 404 http://www.moviescope.com/FUZZ
[E]xecute, [D]escribe, [A]bort: E
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
Target: http://www.moviescope.com/FUZZ
Total requests: 951

=====
ID      Response  Lines  Word    Chars   Payload
=====
000000224: 301        1 L    10 W    153 Ch  "css"
000000241: 301        1 L    10 W    152 Ch  "db"
000000413: 301        1 L    10 W    156 Ch  "images"
000000456: 301        1 L    10 W    152 Ch  "js"
=====
Total time: 0.648525
Processed Requests: 951
Menu sgpt --shell "Fuzz the t...
```

16. Apart from the aforementioned commands, you can further use ShellGPT prompts to perform Web Application Hacking.
17. This concludes the demonstration of Webserver footprinting and attacks using ShellGPT.
18. Close all open windows and document all the acquired information.

#### Question 14.4.1.1

Write a prompt using ShellGPT and execute it on the Parrot Security machine to check if website <https://www.certifiedhacker.com> is protected with a web application firewall using wafwoof. Enter the name of the web application firewall found during the scan.