

# 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.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "sgpt --shell \"Check if the target url www.certifiedhacker.com has web application firewall\" - Parrot Terminal". The terminal content displays the results of an Nmap scan and a WAF detection check:

```
[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]
#
```

The terminal window is part of a desktop environment with a dark theme. A sidebar on the left lists "CEHv13 Module 13 Hacking Web Servers" and "CEHv13 Module 14 Hacking Web Applications". The bottom of the screen shows the desktop environment's menu bar and taskbar.

3. 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.

4. To detect load balancers using ShellGPT run `sgpt --shell "Use load balancing detector on target domain yahoo.com."` command.

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

```
sapt--shell "Use load balancing detector on target domain yahoo.com." - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#sgpt --shell "Use load balancing detector on target domain yahoo.com."
lbd yahoo.com
[E]xecute, [D]escribe, [A]bort: E

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
Written by Stefan Behte (http://ge.mine.nu)
Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: FOUND
yahoo.com has address 74.6.231.20
yahoo.com has address 74.6.231.21
yahoo.com has address 74.6.143.25
yahoo.com has address 98.137.11.164
yahoo.com has address 98.137.11.163
yahoo.com has address 74.6.143.26

Checking for HTTP-Loadbalancing [Server]:
ATS Hacking Web
NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 13:09:42, 13:09:42, 13:09:43, 13:09:43, 13:09:48, 13:09:48, 13:09:48, 13:09:49, 13:09:49, 13:09:49, 13:09:49, 13:09:50, 13:09:50, 13:09:50, 13:09:50, 13:09:51, 13:09:51, 13:09:51, 13:09:51, 13:09:52, 13:09:52, 13:09:52, 13:09:52, 13:09:53, 13:09:53, 13:09:53, 13:09:53, 13:09:54, 13:09:54, 13:09:54, 13:09:54, 13:09:55, 13:09:55, 13:10:00, 13:10:01, 13:10:01, 13:10:01, 13:10:01, 13:10:07, 13:10:12, 13:10:12, 13:10:12, 13:10:18, 13:10:18
```

5. To identify server side technologies using ShellGPT run **sgpt --chat HWA --shell "Launch whatweb on the target website www.moviescope.com to perform website footprinting. Run a verbose scan and print the output. Save the results in file whatweb\_log.txt."** command.

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

To view the generated **whatweb\_log.txt** file contents, navigate to **/home/attacker** and double-click on **whatweb\_log.txt** file.

The screenshot shows a terminal window on a Linux system (Parrot OS) with a dark theme. The terminal title is "sgpt --chat HWA --shell". The command run is "sgpt --chat HWA --shell "Launch whatweb on the target website www.moviescope.com to perform website footprinting. Run a verbose scan and print the output. Save the results in file whatweb\_log.txt." The output of the command is displayed below:

```
[root@parrot]~[~/home/attacker]
[ ] #sgpt --chat HWA --shell "Launch whatweb on the target website www.moviescope.com to perform website 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], HTTPSserver[Microsoft-IIS/10.0], Meta-Author[EC-Council], Microsoft-IIS[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/
  Applications

[ HTTPSserver ]
  Menu  sgpt --chat HWA --sh...
```

6. Now run **sgpt --shell** "Perform the Vulnerability scan on the target url [www.moviescope.com](http://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.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "sgpt --shell \"Perform the Vulnerability scan on the target url www.moviescope.com\" - Parrot Terminal". The terminal window displays the output of the sgpt command, which is a wrapper for Nikto. The output includes the following details:

```
[E]xecute, [D]escribe, [A]bort: E
- Nikto v2.5.0      Hacking Wireless Networks
+ 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]
#
```

The terminal prompt shows the user is root and is in the /home/attacker directory. The command entered was "sgpt --shell".

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.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "sgpt--shell \"Perform the Vulnerability scan on the target url www.moviescope.com using nmap\" - Parrot Terminal". The terminal prompt is "[root@parrot]~[/home/attacker]". The command run is "#sgpt --shell \"Perform the Vulnerability scan on the target url www.moviescope.com using nmap\"". The output of the Nmap scan is displayed, showing the host 224.0.0.251 is up and has a NULL UDP avahi packet DoS vulnerability (CVE-2011-1002). It also lists ports 25/tcp (smtp) and 80/tcp (http) as open. A detailed analysis of port 80/tcp includes findings for SMTP vulns, DOM-based XSS, and ASP.NET status.

```
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.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title bar reads "sgpt --shell \"Use Sn1per tool and scan the target url www.moviescope.com for web vulnerabilities and save the result in file scan3.txt\" - Parr". The terminal content displays the execution of the command and the output of the Sn1per tool. The output includes configuration loading, saving loot to a file, and scanning the specified URL. The terminal window has a dark background with a network graph watermark. The bottom status bar shows "GATHERING DNS INFO".

```
[root@parrot]~[~/home/attacker]
[ ] #sgpt --shell "Use Sn1per tool and scan the target url www.moviescope.com for web vulnerabilities and save the result in file scan3.txt"
sniper -t www.moviescope.com -w scan3.txt
[E]xecute, [D]escribe, [A]bort: E
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/scan3.txt [OK]
[*] Scanning www.moviescope.com [OK]
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/scan3.txt [OK]
[*] Scanning www.moviescope.com [OK]

+ -- --=[https://sn1persecurity.com
+ -- --=[Sn1per v9.2 by @xer0dayz
CEHv13 Module 14
=====x[2024-05-22](07
:27)x*
GATHERING DNS INFO
```

9. To identify files of a web application run **sgpt --shell "Scan the web content of target url www.moviescope.com using Dirb"** command.

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

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "sgpt --shell \"Scan the web content of the target url www.moviescope.com using Dirb\" - Parrot Terminal". The terminal window displays the following command and its output:

```
[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
[CEHv9 Module]
---- 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/
```

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.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "sgpt -shell "Scan the web content of target url www.moviescope.com using Gobuster"- Parrot Terminal". The terminal window displays the following command and its output:

```
[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
```

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.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal output is as follows:

```
Applications Places System 🌐 📁 🚫 🌐
● ● ● 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).
[README] [License]

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]
└─#
```

The terminal window has a dark blue background with a network graph watermark. The title bar shows the command being run: "sgpt --shell "Attempt FTP login on target IP 10.10.1.11 with hydra using usernames and passwords file from /home/attacker/Wordlists" - Parrot". The desktop environment includes icons for Applications, Places, System, and various system status indicators like battery and signal strength.

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"** to automate web application hacking tasks with custom scripts.

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

```
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.certifiedhacker.com"
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 vulnerability 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

CEHv13 Module 14
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 Terminal Help Wed May 22, 08:24
sgpt --chatwah --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
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 Permanently]
https://www.certifiedhacker.com/ [200 OK] Country[UNITED STATES][US], HTTPServer[nginx/1.21.6], IP[162.241.216.11], JQuery[1.4], Meta-Author[Parallelus], PasswordField[RevealPassword], Script[text/javascript], Title[Certified Hacker], UncommonHeaders[host-header,x-server-cache,x-proxy-cache], nginx[1.21.6]

README license
( 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
```

Applications Places System

Wed May 22, 08:39

sgpt --chatwah --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: c2hhcmVkLmJsdWob3N0LmNvbQ==
+ 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).

```

Menu sgpt --chatwah --shel...

A screenshot of a Linux desktop environment. The terminal window shows the output of an Nmap scan for the host www.certifiedhacker.com (162.241.216.11). The output includes information about open ports (21/tcp, 22/tcp, 25/tcp, 26/tcp, 53/tcp, 80/tcp, 110/tcp, 143/tcp, 443/tcp, 465/tcp, 587/tcp, 646/tcp, 993/tcp) and their corresponding services (ftp, ssh, smtp, domain, http, pop3, imap, ssl/http). It also shows the Apache server header and various SSL/TLS services (ssl/smtp, ssl/imap). A note indicates an error in a script execution.

```
+ 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/smtp?
587/tcp   open     tcpwrapped
646/tcp   filtered ldp
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 🌐 ⚡ 🛡️ 🎯 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

target = "www.certifiedhacker.com"

# 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())
CEHv13 Module 14
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

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

manently]

CEHv13 Module 10

https://www.certifiedhacker.com/ [200 OK] Country[UNITED STATES][US], HTTPServer[nginx/1.21.6], IP[162.241.216.11], JQuery[1.4], Meta-Author[Parallelus], PasswordField[RevealPassword], Script[text/javascript], Title[Certified Hacker], UncommonHeaders[host-header,x-server-cache,x-proxy-cache], nginx[1.21.6]

attacker's Home

W00f!

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

CEHv13 Module 14

[\*] Checking https://www.certifiedhacker.com

[+] The site https://www.certifiedhacker.com is behind ModSecurity (SpiderLabs) WAF.

[~] Number of requests: 2

```
Applications Places System 🌐 ⚡ 🗑️ 🖥️ 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 w...
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: c2hhcmVkLmJsdWVob3N0LmNvbQ==
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): 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 --shel...
```

```
+ 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        Apache httpd
110/tcp   open     pop3         Dovecot pop3d
143/tcp   open     imap         Dovecot imapd
443/tcp   open     ssl/http    Apache httpd
| http-server-header:
|_ Apache/2.4.41
|_ 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)
```

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](http://www.certifiedhacker.com)" command.

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

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 then use this information to perform vulnerability scanning on target url is www.certifiedhacker.com"

```
[root@parrot]~[/home/attacker]
[ ] #sgpt --chat wah --shell "create and run a custom python script which will run web application f
ootprinting tasks to gather information and then use this information to perform vulnerability scanni
ng 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}')"
```

File Edit View Search Terminal Help

Trash

Servers

Hacking Web

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

```
Applications Places System 🌐 ⚙️ 🗃️ 🎨 Terminal Help
● ● ● sgpt --chatwah --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,
Menu sgpt --chatwah --shel...
```

The screenshot shows a terminal window with a dark background and light-colored text. At the top, there's a menu bar with icons for Applications, Places, System, and a few others. The title bar says "sgpt --chat wah --shell" and "Thu May 23, 01:10". The main area of the terminal displays the output of a web application scanner. It starts with "Nmap done: 1 IP address (1 host up) scanned in 150.80 seconds" and "Starting vulnerability scanning on: www.certifiedhacker.com". Then it shows "Nikto Scan Results: - Nikto v2.5.0" followed by several sections of scan details, including target information, server details, and various security findings. The terminal ends with "1 host(s) tested" and the prompt "[root@parrot]#".

```
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: c2hhcmVkLmJsdWob3N0LmNvbQ==.
+ 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
[root@parrot]#
```

15. To perform Web application fuzz testing using ShellGPT run **sgpt --shell "Fuzz the target url [www.moviescope.com](http://www.moviescope.com) using Wfuzz tool"** command.

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

The screenshot shows a terminal window on a Parrot Security OS desktop environment. The terminal title is "sgpt --shell \"Fuzz the target url www.moviescope.com using Wfuzz tool\" - Parrot Terminal". The command run was "wfuzz -c -z file,/usr/share/wordlists/wfuzz/general/common.txt --hc 404 http://www.moviescope.com/FUZZ". The output indicates that the fuzzing process has completed 951 requests. A table summarizes the results:

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

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.