Lab 3: Perform Vulnerability Analysis using AI

Lab Scenario

As a professional ethical hacker or pen tester, you must acknowledge the limitations of conventional approaches in revealing all potential vulnerabilities. Therefore, you will utilize AI-driven vulnerability analysis tools to identify and assess security weaknesses in a simulated network environment.

Lab Objectives

- Perform vulnerability analysis using ShellGPT

Overview of vulnerability analysis using AI

Vulnerability Analysis with AI employs advanced algorithms to unearth hidden security flaws in networks. AI-driven tools extract comprehensive data, prioritize risks, and fortify defenses, empowering ethical hackers to anticipate and mitigate emerging threats effectively. This innovative approach enhances cybersecurity readiness by leveraging AI's precision and adaptability.

Task 1: Perform Vulnerability Analysis using ShellGPT

ShellGPT swiftly interprets and executes commands, conducting scans, identifying weaknesses, and suggesting mitigation strategies in real-time. Its adaptive nature facilitates dynamic navigation through complex systems, enhancing efficiency and precision in vulnerability analysis. By integrating ShellGPT, you can gain a powerful ally in their quest to safeguard digital ecosystems, leveraging AI's capabilities to uncover and address security risks with unparalleled speed and accuracy.

Here, we will use ShellGPT to discover potential vulnerabilites in the target.

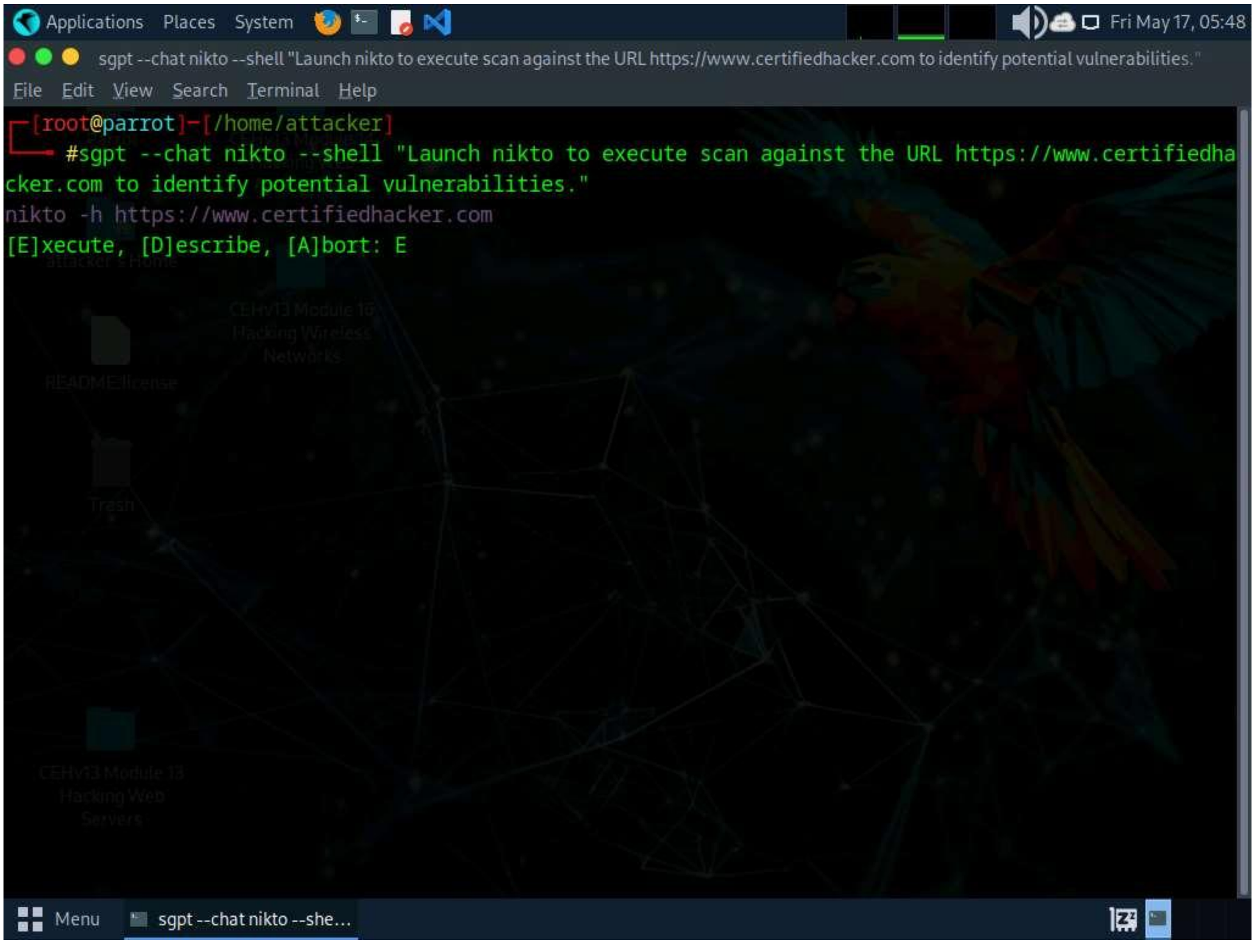
The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the 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 --chat nikto --shell "Launch nikto to execute a scan against the URL www.certifiedhacker.com to identify potential vulnerabilities."** to launch Nikto scan on the target website.

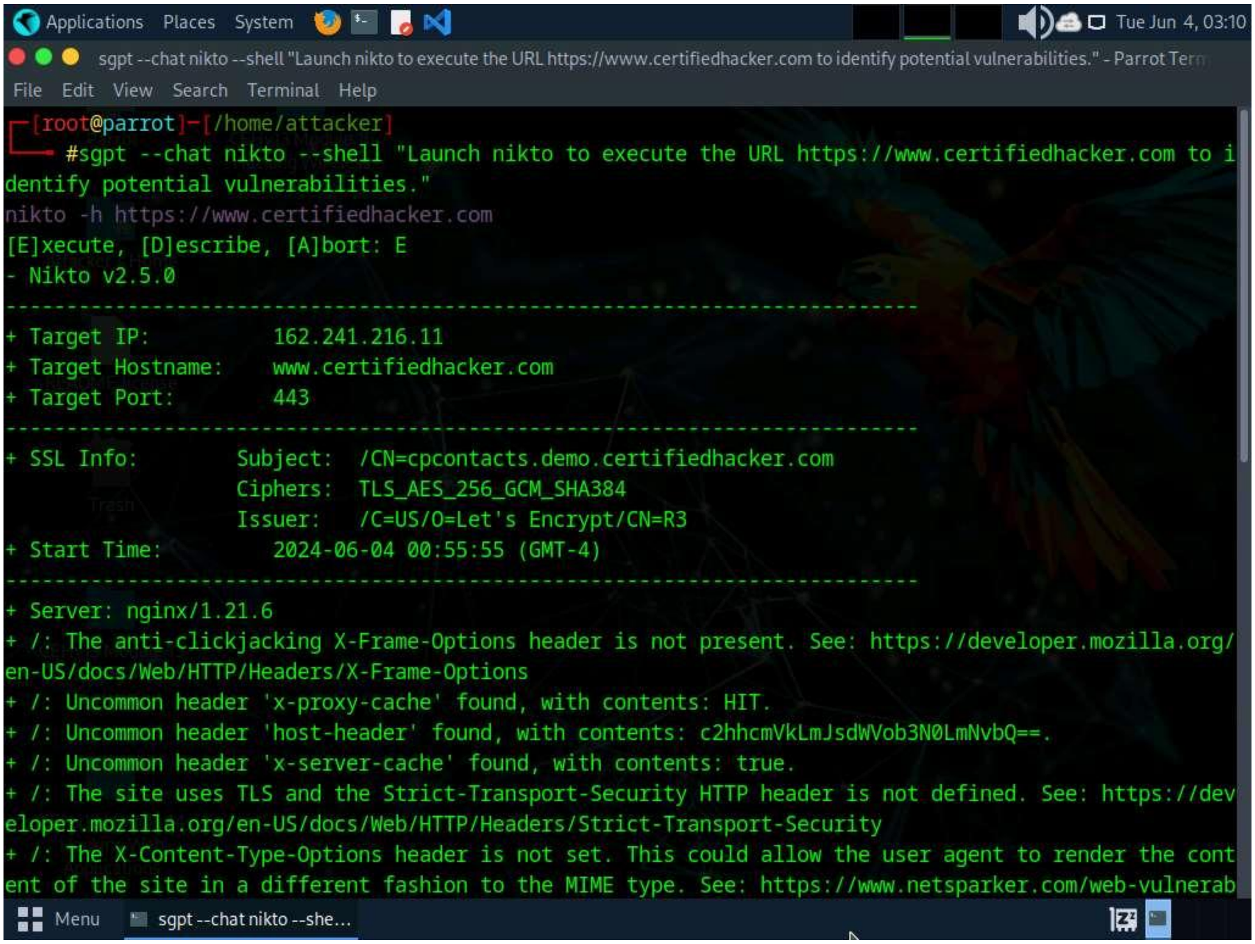
In the prompt, type **E** and press **Enter** to execute the command.



Applications Places System
Fri May 17, 05:48
sgpt --chat nikto --shell "Launch nikto to execute scan against the URL https://www.certifiedhacker.com to identify potential vulnerabilities."
File Edit View Search Terminal Help
Menu
sgpt --chat nikto --she...

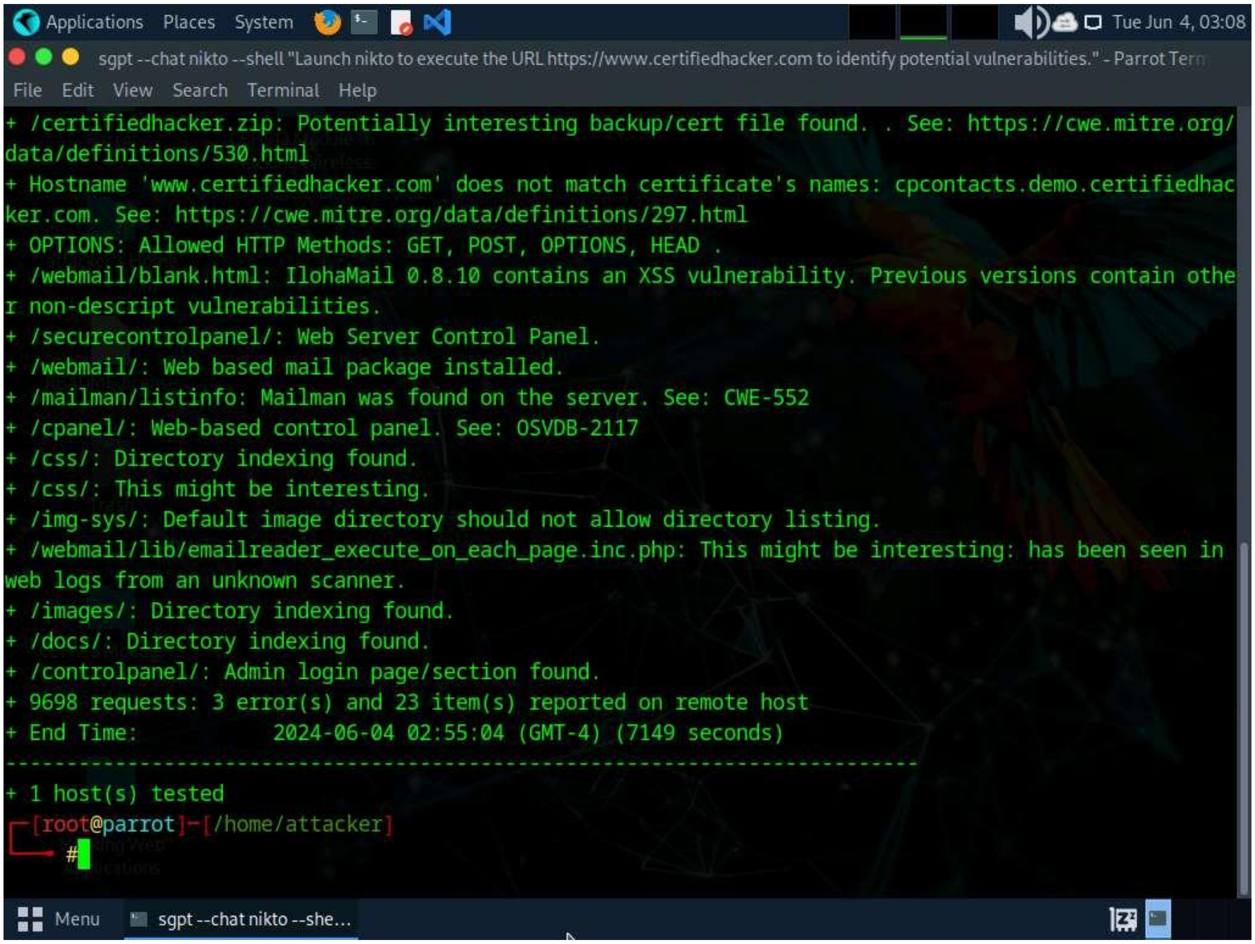
```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat nikto --shell "Launch nikto to execute scan against the URL https://www.certifiedhacker.com to identify potential vulnerabilities."
nikto -h https://www.certifiedhacker.com
[E]xecute, [D]escribe, [A]bort: E
```

3. Scan result appears displaying the discovered vulnerabilities in the target website (here, **www.certifiedhacker.com**), as shown in the screenshot.



Applications Places System
Tue Jun 4, 03:10
sgpt --chat nikto --shell "Launch nikto to execute the URL https://www.certifiedhacker.com to identify potential vulnerabilities." - Parrot Term
File Edit View Search Terminal Help
Menu
sgpt --chat nikto --she...

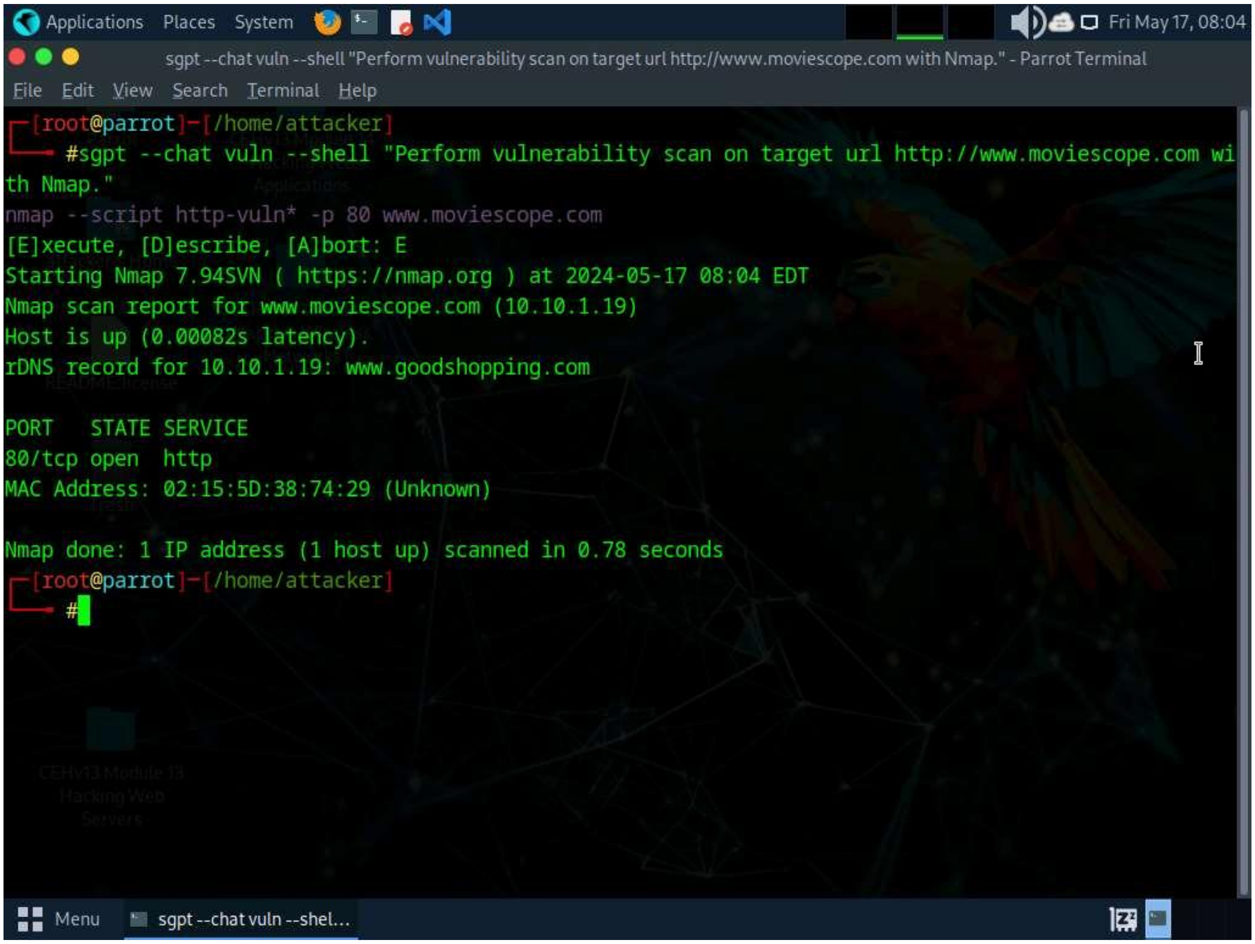
```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat nikto --shell "Launch nikto to execute the URL https://www.certifiedhacker.com to i
dentify potential vulnerabilities."
nikto -h https://www.certifiedhacker.com
[E]xecute, [D]escribe, [A]bort: E
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=cpcontacts.demo.certifiedhacker.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Start Time:         2024-06-04 00:55:55 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.21.6
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/
en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-proxy-cache' found, with contents: HIT.
+ /: Uncommon header 'host-header' found, with contents: c2hhcmVkLmJsdWVob3N0LmNvbQ==.
+ /: Uncommon header 'x-server-cache' found, with contents: true.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://dev
eloper.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the cont
ent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerab
```


Applications Places System
Tue Jun 4, 03:08
sgpt --chat nikto --shell "Launch nikto to execute the URL https://www.certifiedhacker.com to identify potential vulnerabilities." - Parrot Term
File Edit View Search Terminal Help
Menu
sgpt --chat nikto --she...

```
+ /certifiedhacker.zip: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/
data/definitions/530.html
+ Hostname 'www.certifiedhacker.com' does not match certificate's names: cpcontacts.demo.certifiedhac
ker.com. See: https://cwe.mitre.org/data/definitions/297.html
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability. Previous versions contain othe
r non-descript vulnerabilities.
+ /securecontrolpanel/: Web Server Control Panel.
+ /webmail/: Web based mail package installed.
+ /mailman/listinfo: Mailman was found on the server. See: CWE-552
+ /cpanel/: Web-based control panel. See: OSVDB-2117
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /img-sys/: Default image directory should not allow directory listing.
+ /webmail/lib/emailreader_execute_on_each_page.inc.php: This might be interesting: has been seen in
web logs from an unknown scanner.
+ /images/: Directory indexing found.
+ /docs/: Directory indexing found.
+ /controlpanel/: Admin login page/section found.
+ 9698 requests: 3 error(s) and 23 item(s) reported on remote host
+ End Time:           2024-06-04 02:55:04 (GMT-4) (7149 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

Nikto scan takes long time to complete. You can terminate the scan, by pressing **Ctrl + Z**.

4. In the terminal, run **sgpt --chat vuln --shell "Perform vulnerability scan on target url http://www.moviescope.com with Nmap"** command to perform vulnerability scan on the target website. The result appears displaying open ports and services running on the target website.


Applications
Places
System
Fri May 17, 08:04
sgpt --chat vuln --shell "Perform vulnerability scan on target url http://www.moviescope.com with Nmap." - Parrot Terminal
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat vuln --shel...

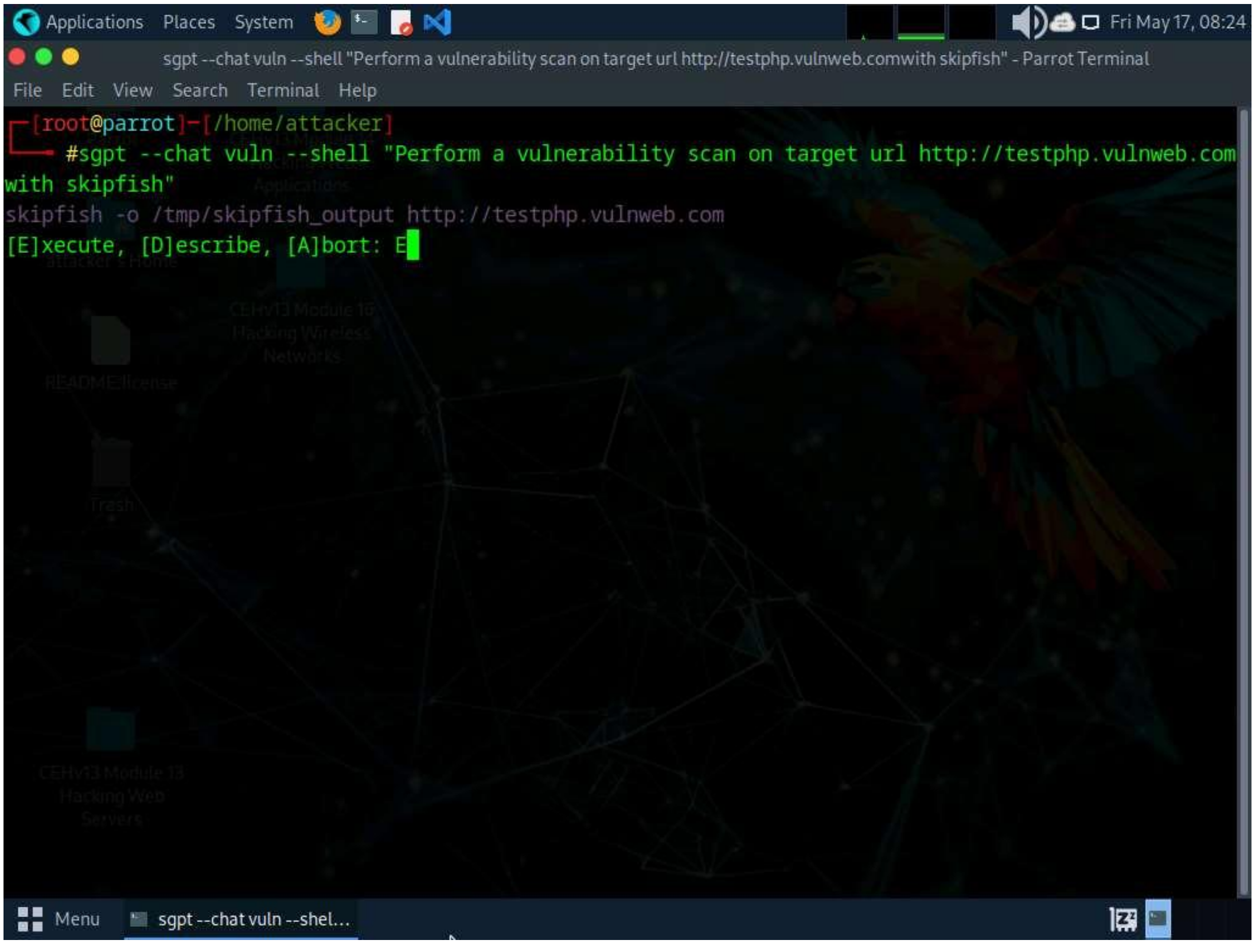
```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat vuln --shell "Perform vulnerability scan on target url http://www.moviescope.com wi
th Nmap."
nmap --script http-vuln* -p 80 www.moviescope.com
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 08:04 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00082s latency).
rDNS record for 10.10.1.19: www.goodshopping.com

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:15:5D:38:74:29 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

5. Run **sgpt --chat vuln --shell “Perform a vulnerability scan on target url http://testphp.vulnweb.com with skipfish”** to scan the target URL using skipfish tool.

If a prompt appears, enter any key to continue the scanning process.

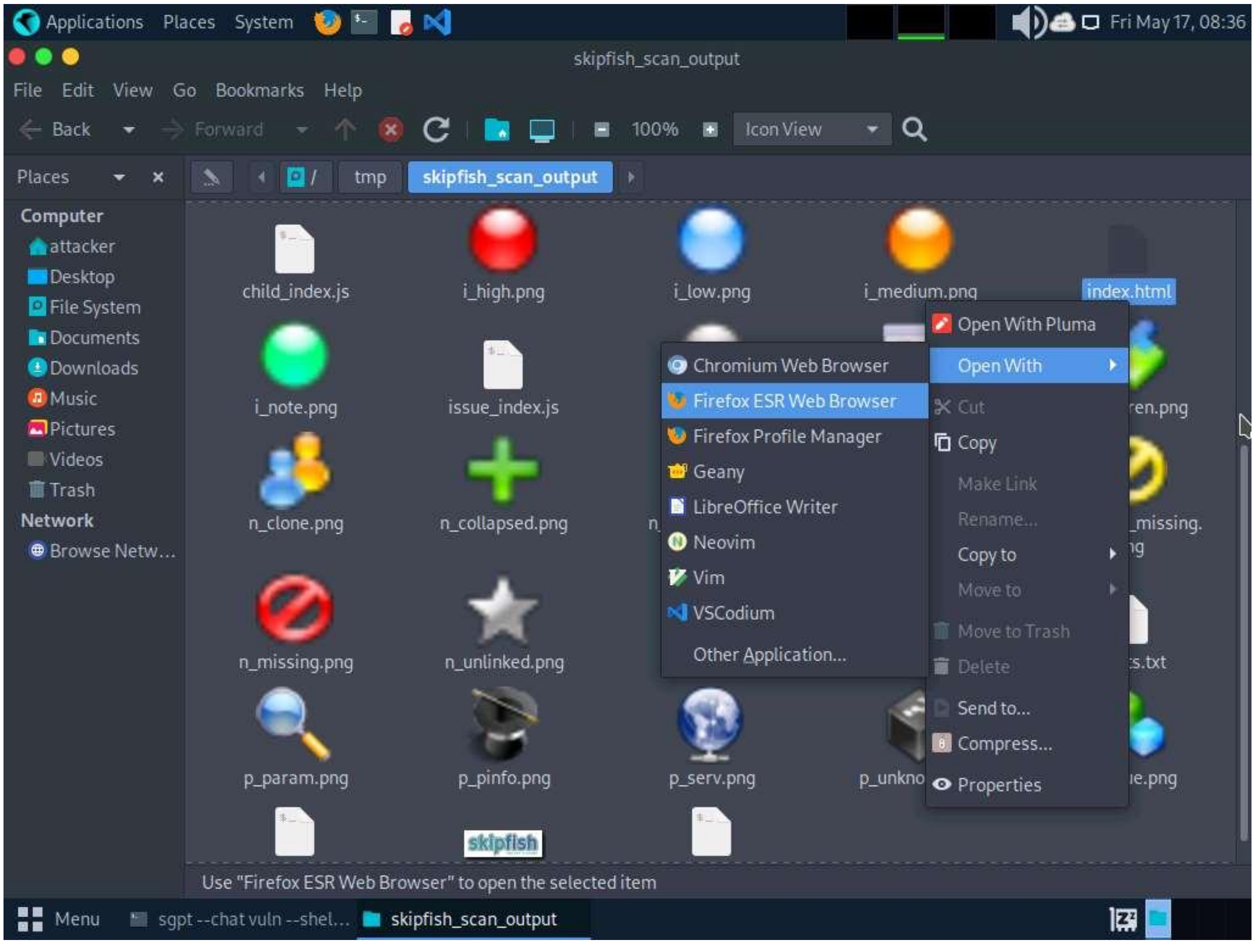


Applications Places System
Fri May 17, 08:24
sgpt --chat vuln --shell "Perform a vulnerability scan on target url http://testphp.vulnweb.comwith skipfish" - Parrot Terminal
File Edit View Search Terminal Help
Menu
sgpt --chat vuln --shel...

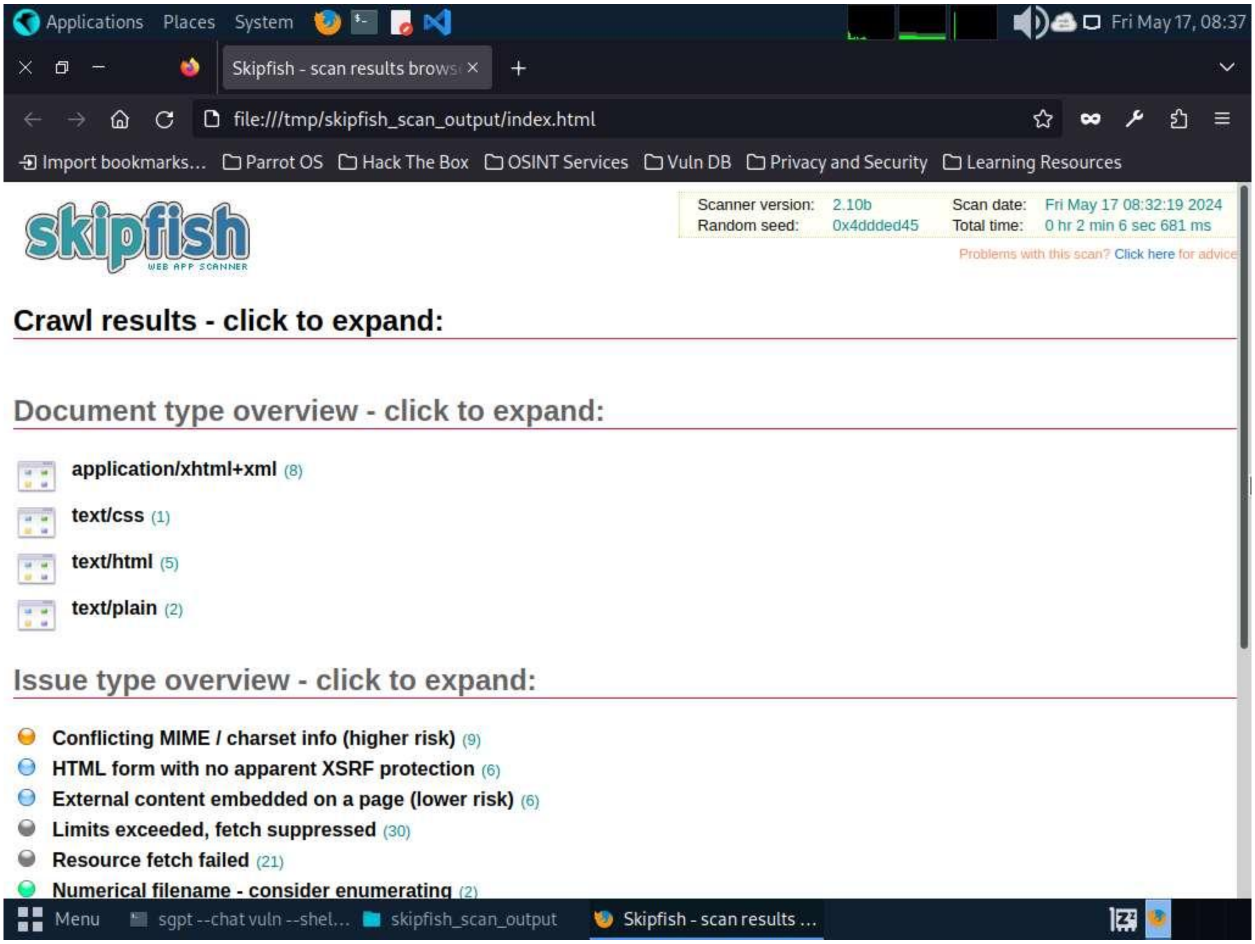
```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat vuln --shell "Perform a vulnerability scan on target url http://testphp.vulnweb.com
with skipfish"
skipfish -o /tmp/skipfish_output http://testphp.vulnweb.com
[E]xecute, [D]escribe, [A]bort: E
```

6. The skipfish begins scanning the target url. After the successful completion of the scan, report is saved at the **/tmp/skipfish_scan_output/** location, named as **index.html**. Navigate to the location, right-click on **index.html** and open with **Firefox ESR Web Browser**, as shown in the screenshot.

The location of scan report might differ. You can view the location in the skipfish command generated by ShellGPT.



7. Firefox browser window appears displaying the complete scan report, as shown in the screenshot.


Applications Places System
Fri May 17, 08:37
Skipfish - scan results brows
file:///tmp/skipfish_scan_output/index.html
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
skipfish WEB APP SCANNER
Menu
sgpt --chat vuln --shel...
skipfish_scan_output
Skipfish - scan results ...

Scanner version: 2.10b Scan date: Fri May 17 08:32:19 2024
Random seed: 0x4dddded45 Total time: 0 hr 2 min 6 sec 681 ms

Problems with this scan? Click here for advice

Crawl results - click to expand:

Document type overview - click to expand:

- application/xhtml+xml (8)
- text/css (1)
- text/html (5)
- text/plain (2)

Issue type overview - click to expand:

- Conflicting MIME / charset info (higher risk) (9)
- HTML form with no apparent XSRF protection (6)
- External content embedded on a page (lower risk) (6)
- Limits exceeded, fetch suppressed (30)
- Resource fetch failed (21)
- Numerical filename - consider enumerating (2)

8. Apart from the aforementioned commands, you can further explore additional options within the ShellGPT tool and utilize various other tools to conduct vulnerability assessments on the target.

9. This concludes the demonstration of performing vulnerability assessment on the target system using ShellGPT.

10. Close all open windows and document all the acquired information.

Question 5.3.1.1

Write a prompt using ShellGPT to perform vulnerability scan on www.certifiedhacker.com website using Nikto vulnerability scanner. Enter the contents of Uncommon header ‘host header’ found during the vulnerability scan.