Lab 3: Detect Web Application Vulnerabilities using Various Web Application Security Tools

Lab Scenario

When talking about web applications, organizations consider security to be a critical component, because web applications are a major source of attacks. Attackers try various application-level attacks to compromise the security of web applications to commit fraud or steal sensitive information.

Web application attacks, launched on port 80/443, go straight through the firewall, past the OS and network-level security, and into the heart of the application, where corporate data resides. Tailor-made web applications are often insufficiently tested, have undiscovered vulnerabilities, and are, therefore, easy prey for hackers.

A professional ethical hacker or pen tester needs to determine whether their organization's website is secure, before hackers download sensitive data, commit crimes using the website as a launchpad, or otherwise endanger the business. There are various web application security assessment tools available to scan, detect, and assess the security and vulnerabilities of web applications. These tools reveal the web application's security posture and are used to find ways to harden security and create robust web applications. These tools automate the process of accurate web-app security assessment, thus enabling cybersecurity staff to protect their business from impending hacker attacks!

The tasks in this lab will assist in discovering the underlying vulnerabilities and flaws in the target web application.

Lab Objectives

- Detect web application vulnerabilities using wapiti web application security scanner

Overview of Web Application Security

Web application security deals with securing websites, web applications, and web services. Web application security includes secure application development, input validation, creating and following security best practices, using WAF Firewall/IDS, and performing regular auditing of a network using web application security tools.

Web Application security tools are automated tools that scan web applications, normally from the outside, to look for security vulnerabilities such as XSS, SQL injection, command injection, path traversal, and insecure server configuration. This category of tools is frequently referred to as Dynamic Application Security Testing (DAST) Tools.

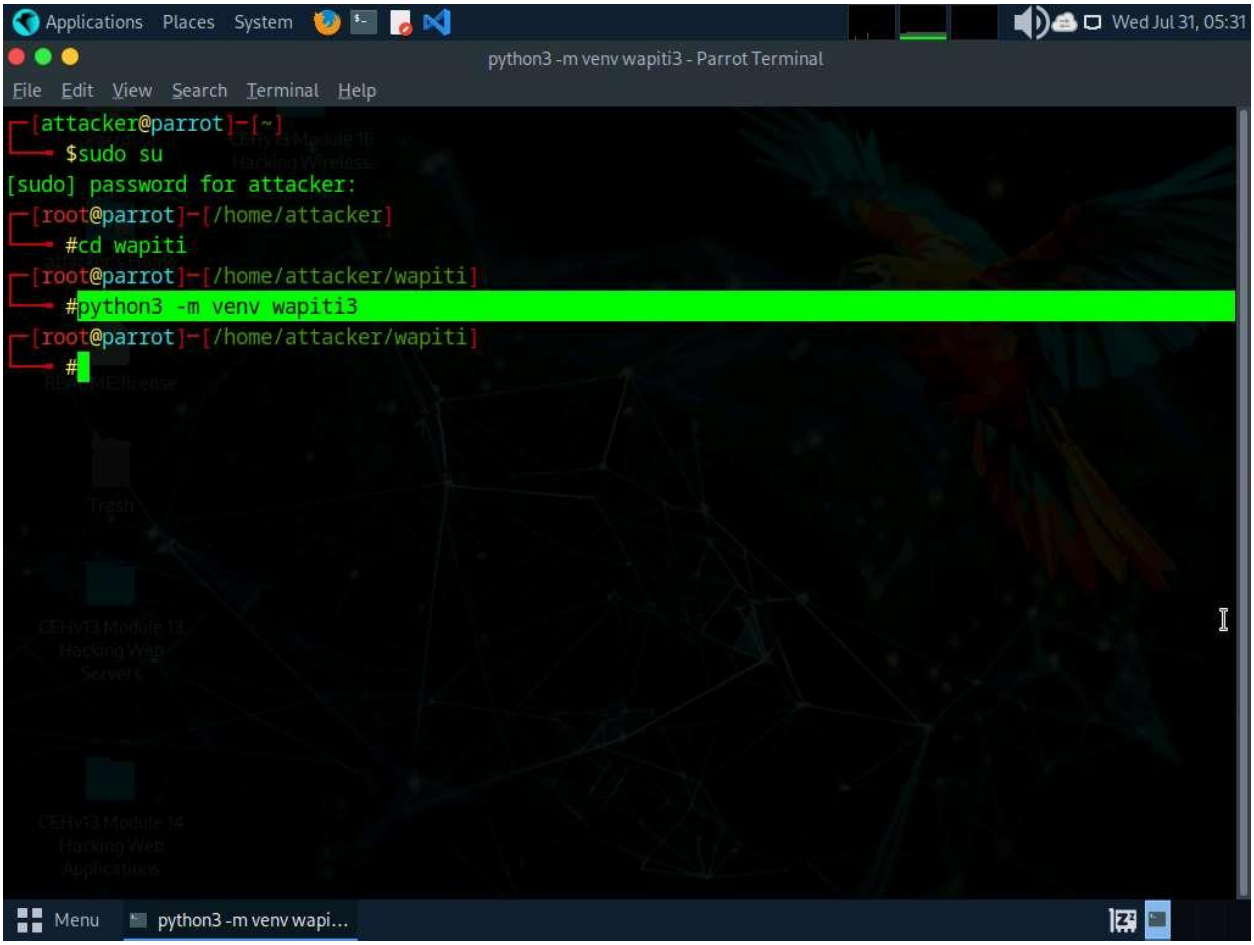
Task 1: Detect Web Application Vulnerabilities using Wapiti Web Application Security Scanner

The Wapiti web-application vulnerability scanner identifies security weaknesses in web applications by crawling websites and performing black-box testing. It detects issues like SQL injections, XSS, and other vulnerabilities.

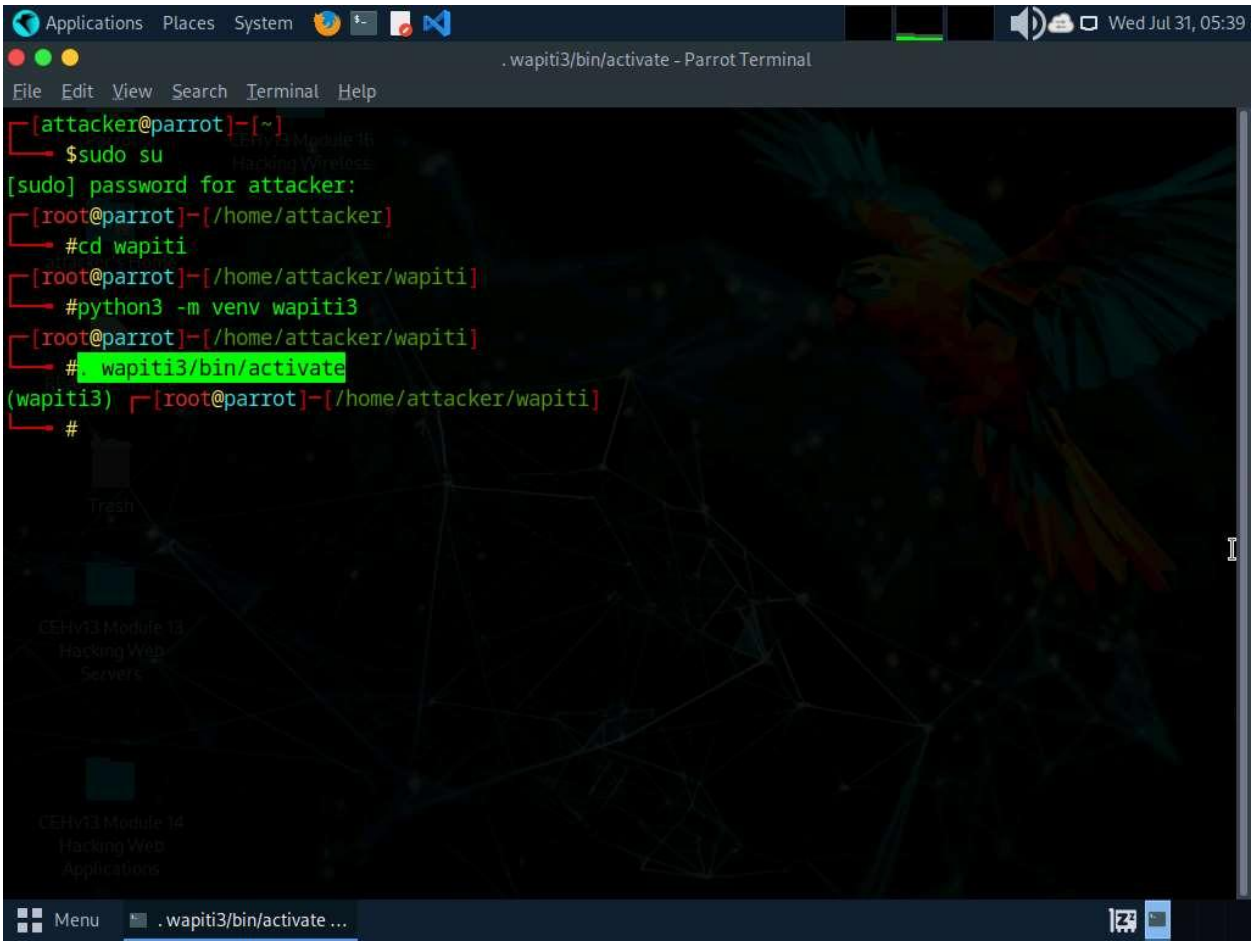
1. Click Parrot Security to switch to the **Parrot Security** machine. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

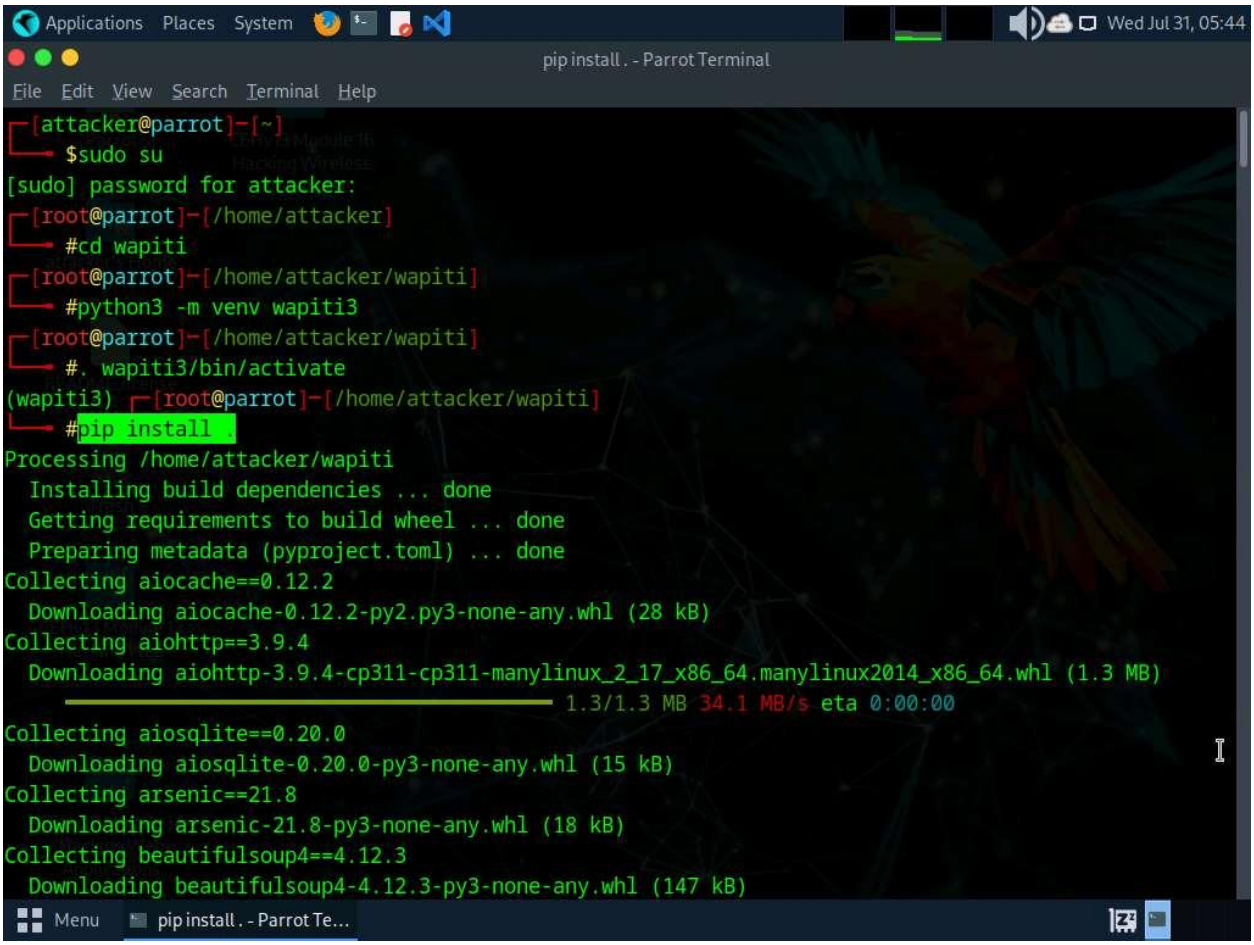
2. In the terminal window run **cd wapiti** command to navigate into wapiti directory and run **python3 -m venv wapiti3** command to create virtual environment in python.



3. Now, run **. wapiti3/bin/activate** command to activate virtual environment.

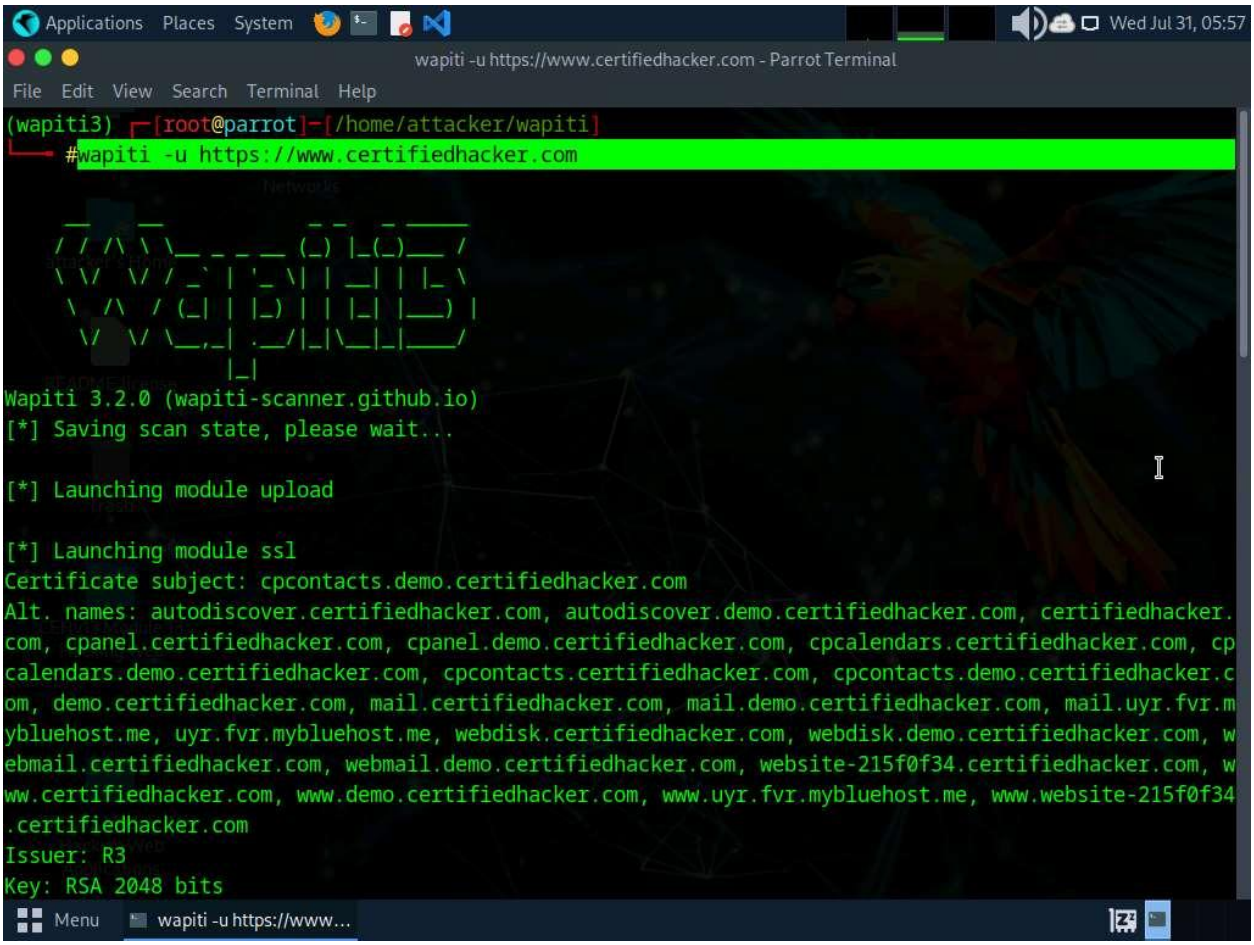


4. Run **pip install .** command to install wapiti web application security scanner.

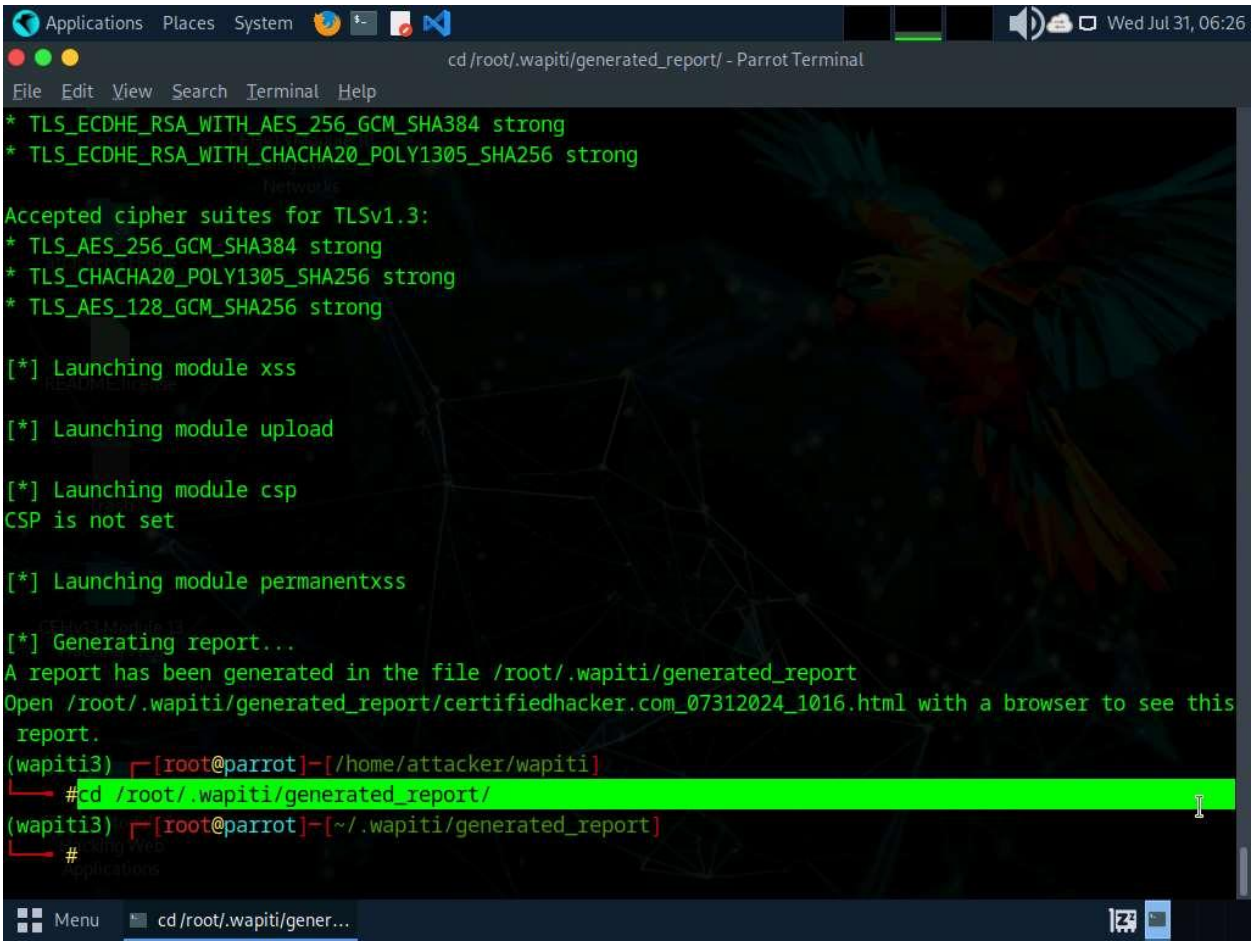


5. After installing the tool run **wapiti -u https://www.certifiedhacker.com** command to perform web application security scanning on certifiedhacker.com website.

It takes approximately 10 minutes for the scan to complete.

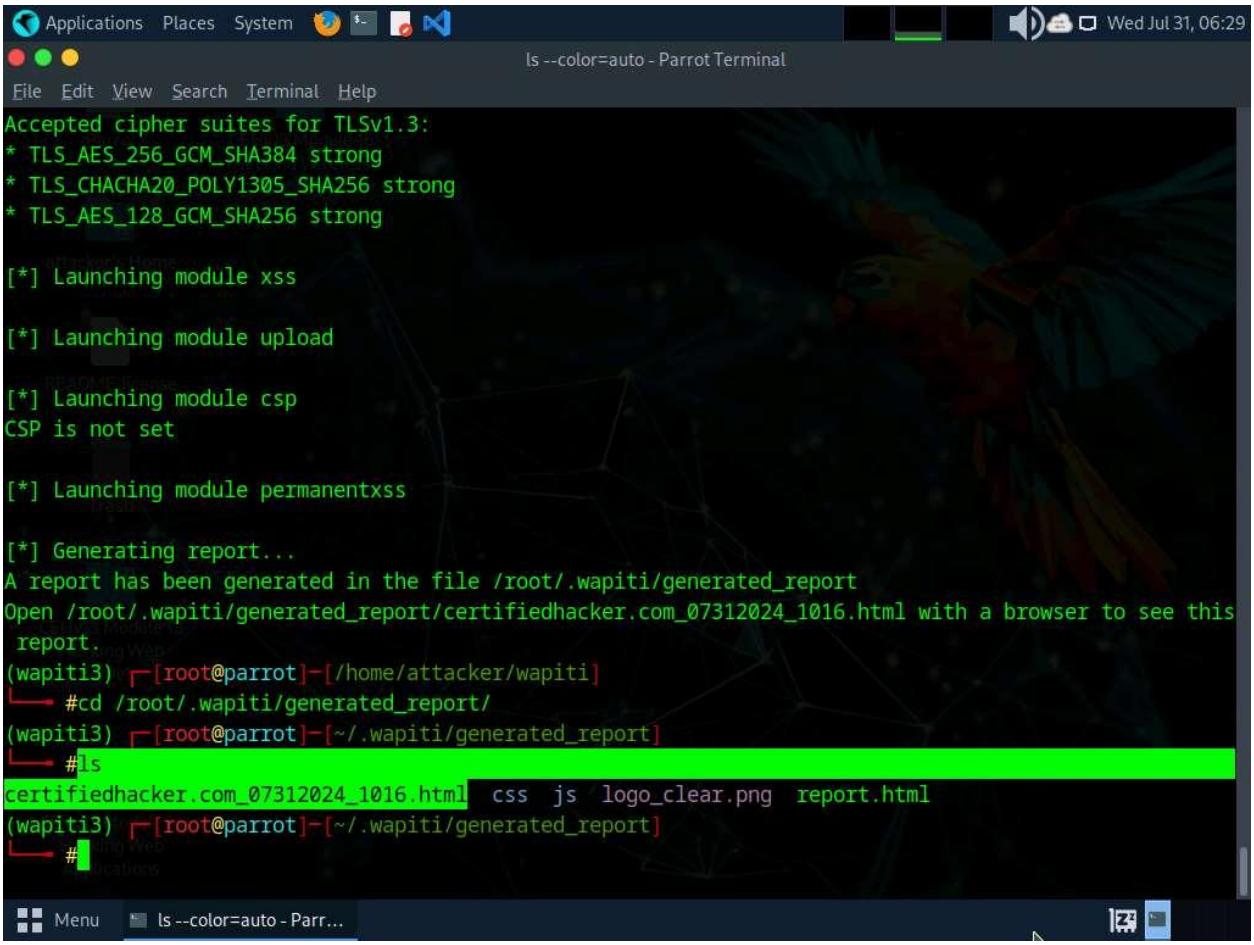


6. Now, in the terminal run **cd /root/.wapiti/generated_report/** to navigate to generated_report directory.

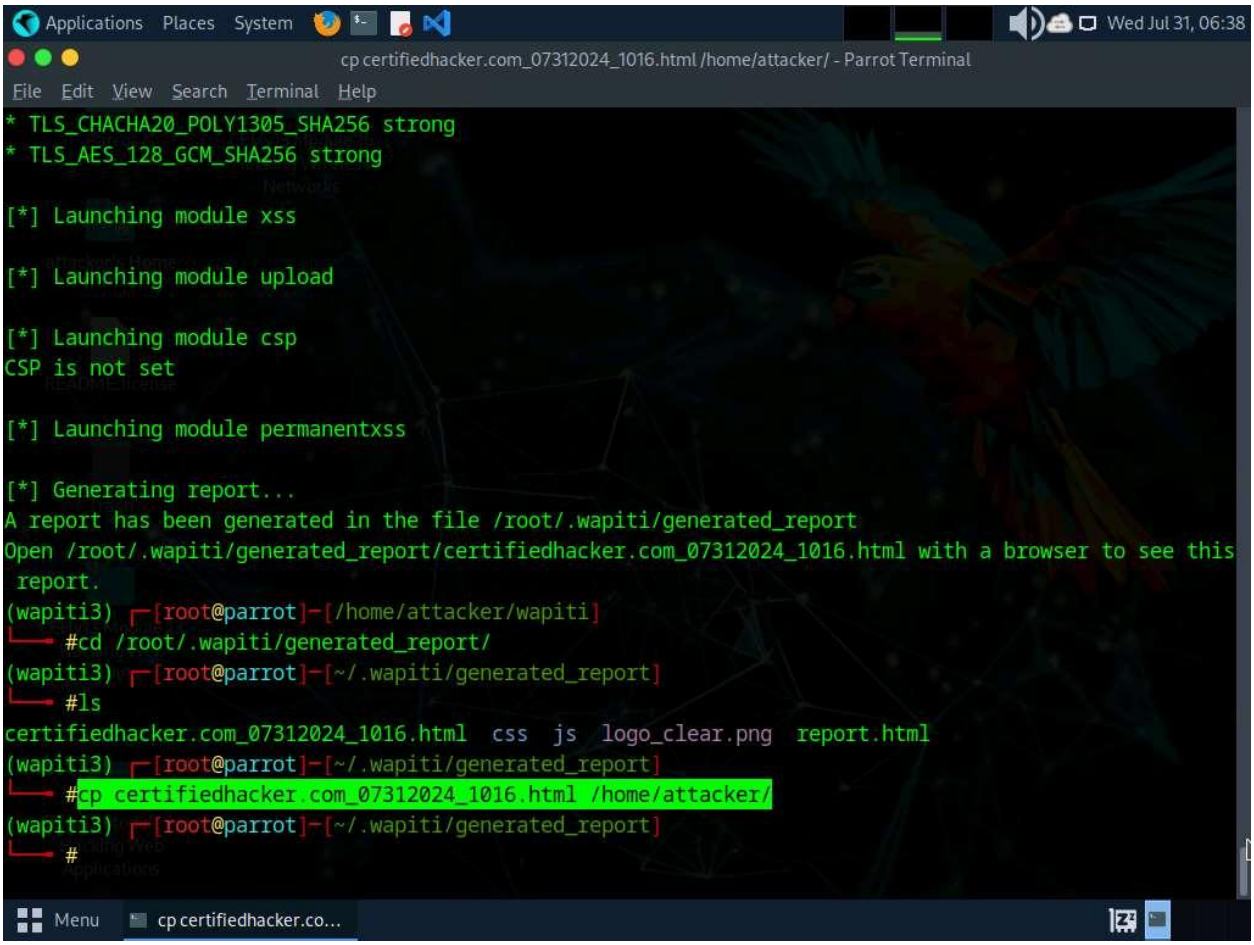


7. Run **ls** command to view the contents of the directory. we can see that the **certifiedhacker.com_xxxxxxxx_xxxx.html** file is created.

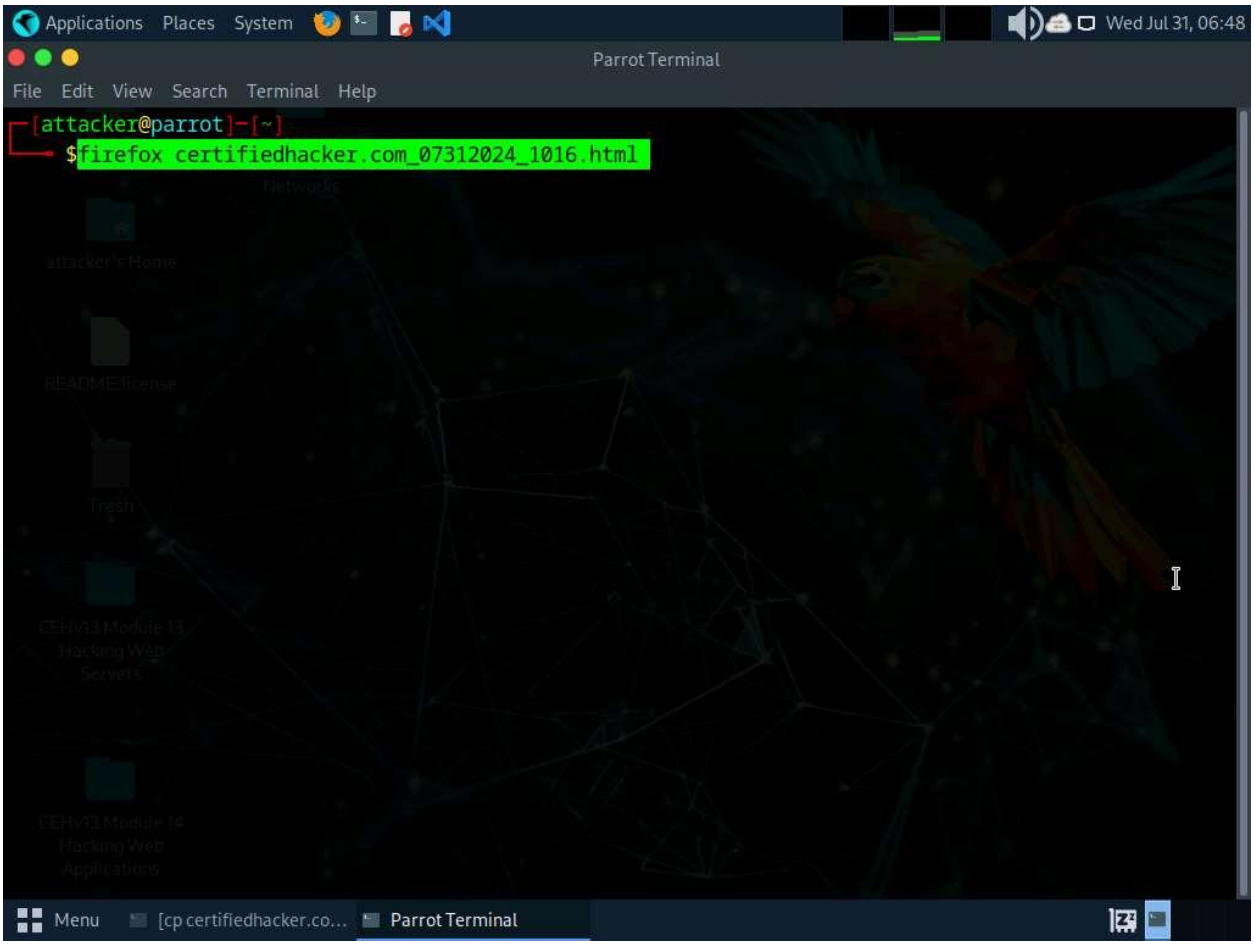
The name of the .html file varies when you perform this lab.



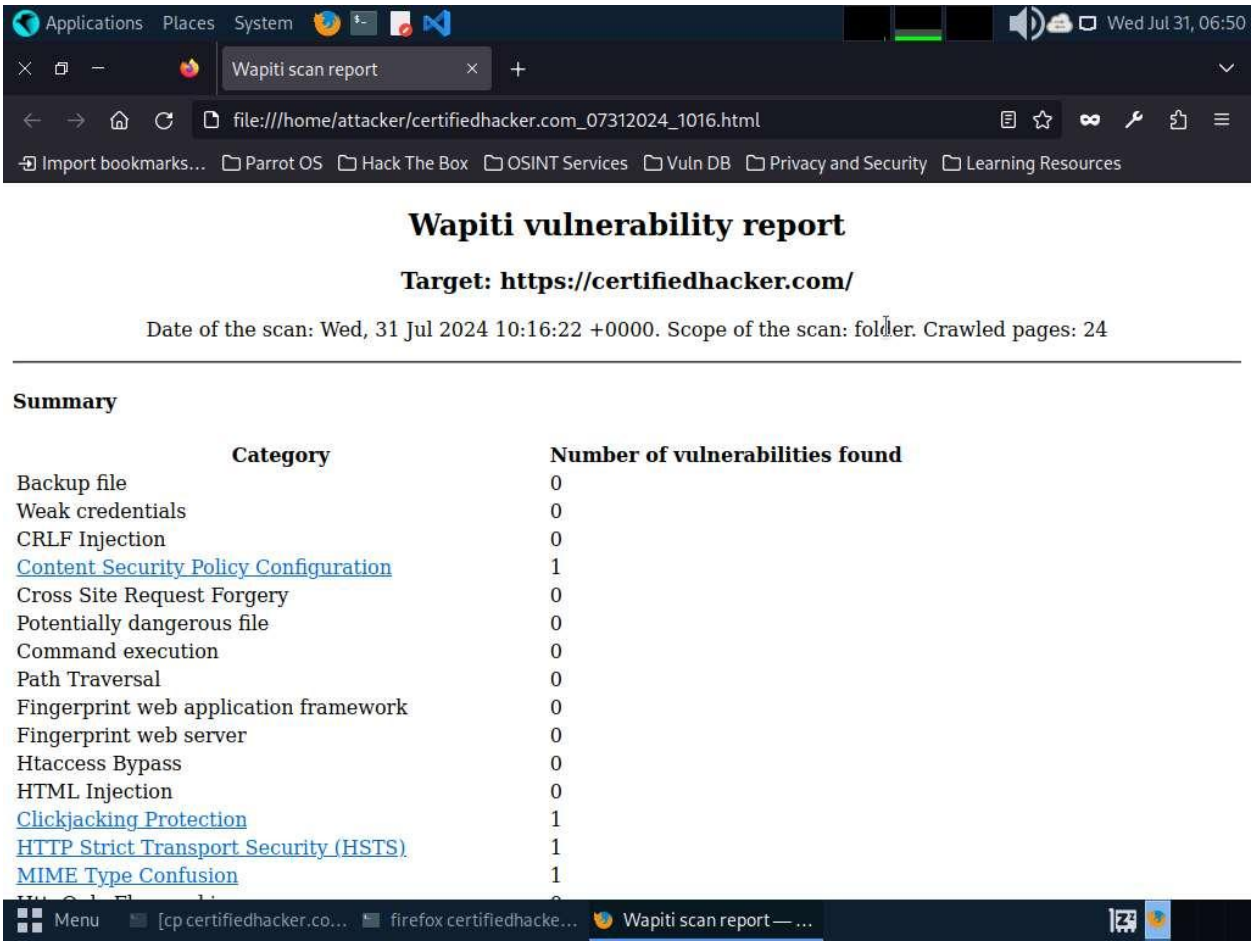
8. Run **cp certifiedhacker.com_xxxxxxxx_xxxx.html /home/attacker/** command to copy the .html file to **/home/attacker** location.



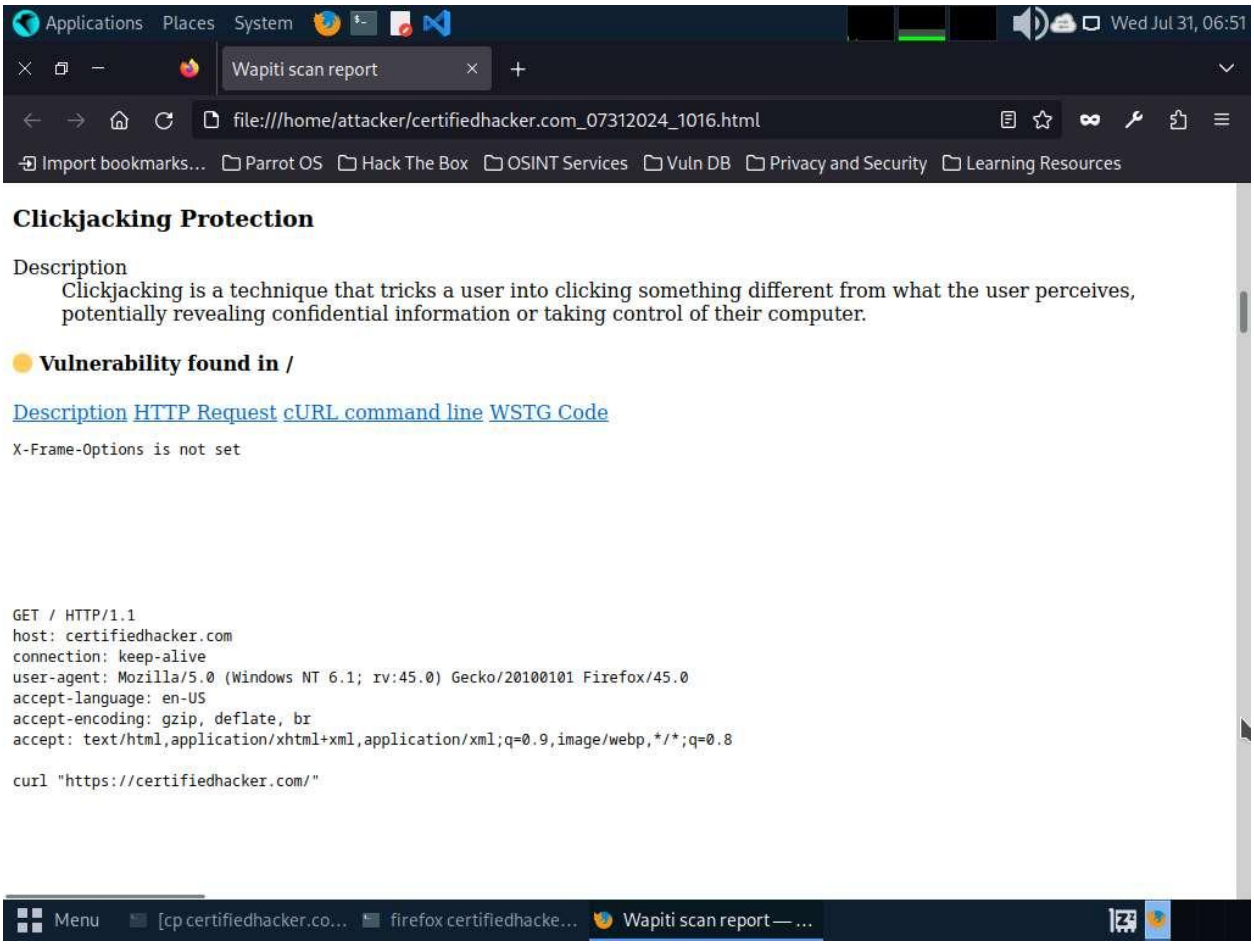
9. Open a new terminal and run **firefox certifiedhacker.com_xxxxxxxx_xxxx.html** command to open the .html file in Firefox browser.



10. Wapiti scan report opens upp in Firefox browser, you can analyze the scan result with the discovered vulnerabilities.



11. Scroll down to view the detailed information regarding each discovered vulnerability.



12. This concludes the demonstration of discovering vulnerabilities in a target website scanning using wapiti.
13. Close all open windows and document all acquired information.

Question 14.3.1.1

In Parrot Security machine use wapiti web application security scanner to detect web application vulnerabilities of https://www.certifiedhacker.com web application and generate a .html report. Enter the WSTG code of the Clickjacking Protection vulnerability. (Answer Format: XXXX-X-Xxxxx-Xxxxxxx)