Group: G2A5
Luca Manna

CYBERSECURITY

HANDS-ON TRAINING 2024-WEEK 1

FIRST CHALLENGE-ENHANCE PICOCTF PRACTICE LAB

DESCRIPTION

The challenge requires to download an image file and analyze it to find a hidden flag. This task involves using forensic analysis techniques to uncover data that may be embedded within the image. The challenge requires to download this image file and find the flag.

Tags: Forensics, Medium Difficulty, Steganography, Metadata, Image Analysis

IMAGE DOWNLOAD

FIRST CHALLENGE-ENHANCE PICOCTF PRACTICE LAB

STEPS FOLLOWED & SOLUTION

IMAGE 1

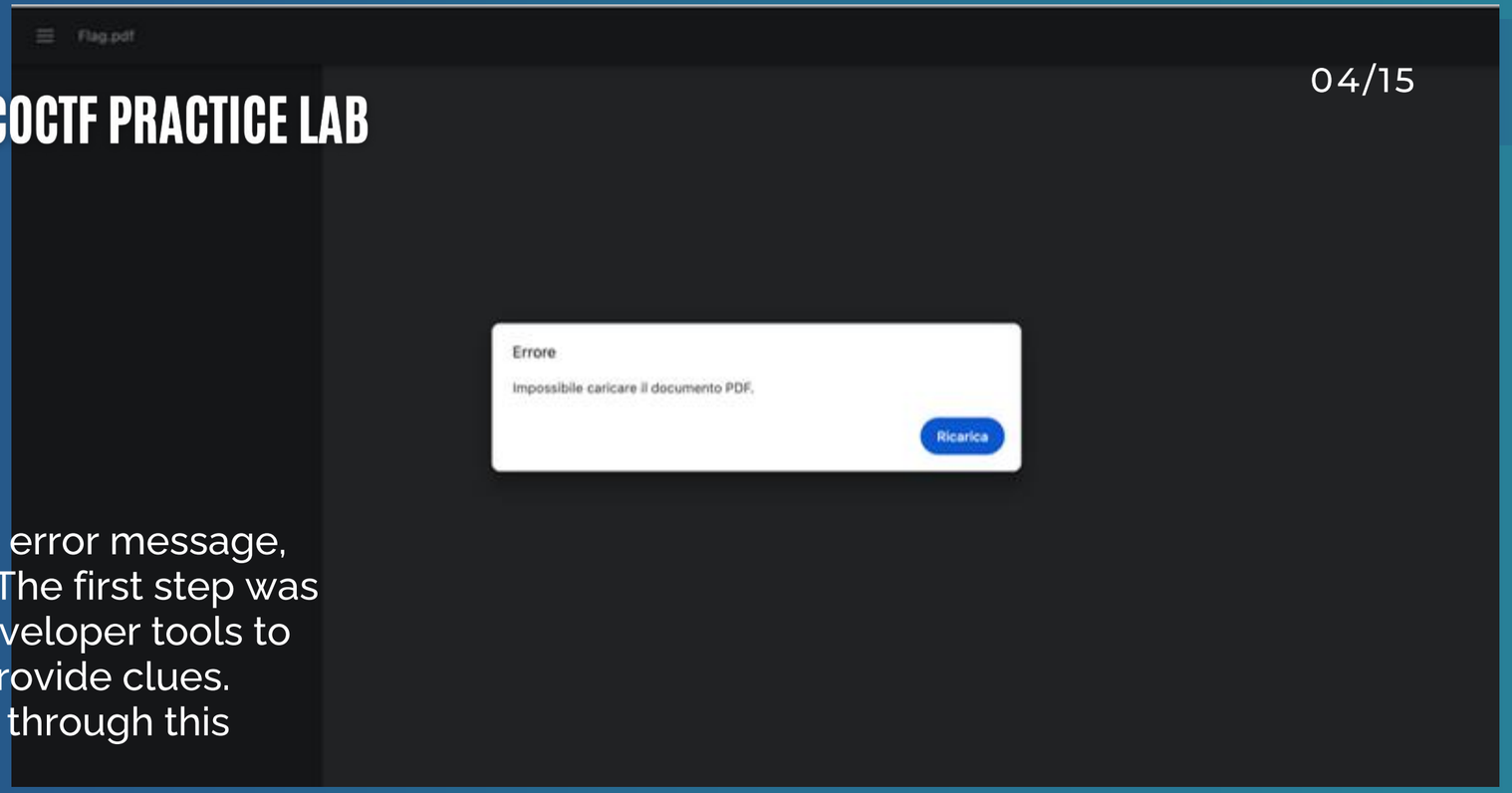
After downloading the image, I opened the file in a text editor to inspect the source code directly **(see IMAGE 1)**. Specifically, the image was an SVG file, a type of XML-based vector graphic format. SVG files are not just images; they contain text and data that describe how the image should be rendered. This makes SVG files particularly useful for hiding information in a way that isn't immediately visible when simply viewing the image. By scrolling through the source code, I discovered the typical flag format used by picoCTF to solve challenges **(see IMAGE 2)**. I then copied the flag **picoCTF{3nh4nc3d_c3d_aab729dd}** without spaces, and the challenge was solved.

CONCLUSION:

This challenge underscores the importance of examining the underlying structure of files in forensic analysis to uncover hidden data. The direct inspection of the image's source code revealed text elements that formed the flag. Understanding the type of source code and knowing how to navigate and analyze it is crucial for uncovering such hidden data.

IMAGE 2

SECOND CHALLENGE-FILE TYPES PICOCTF PRACTICE LAB

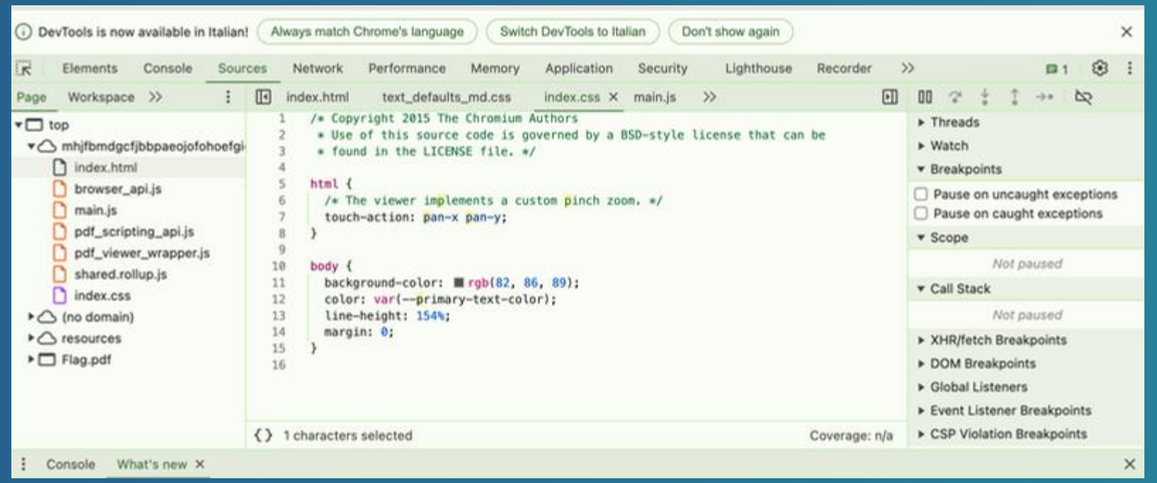


Description

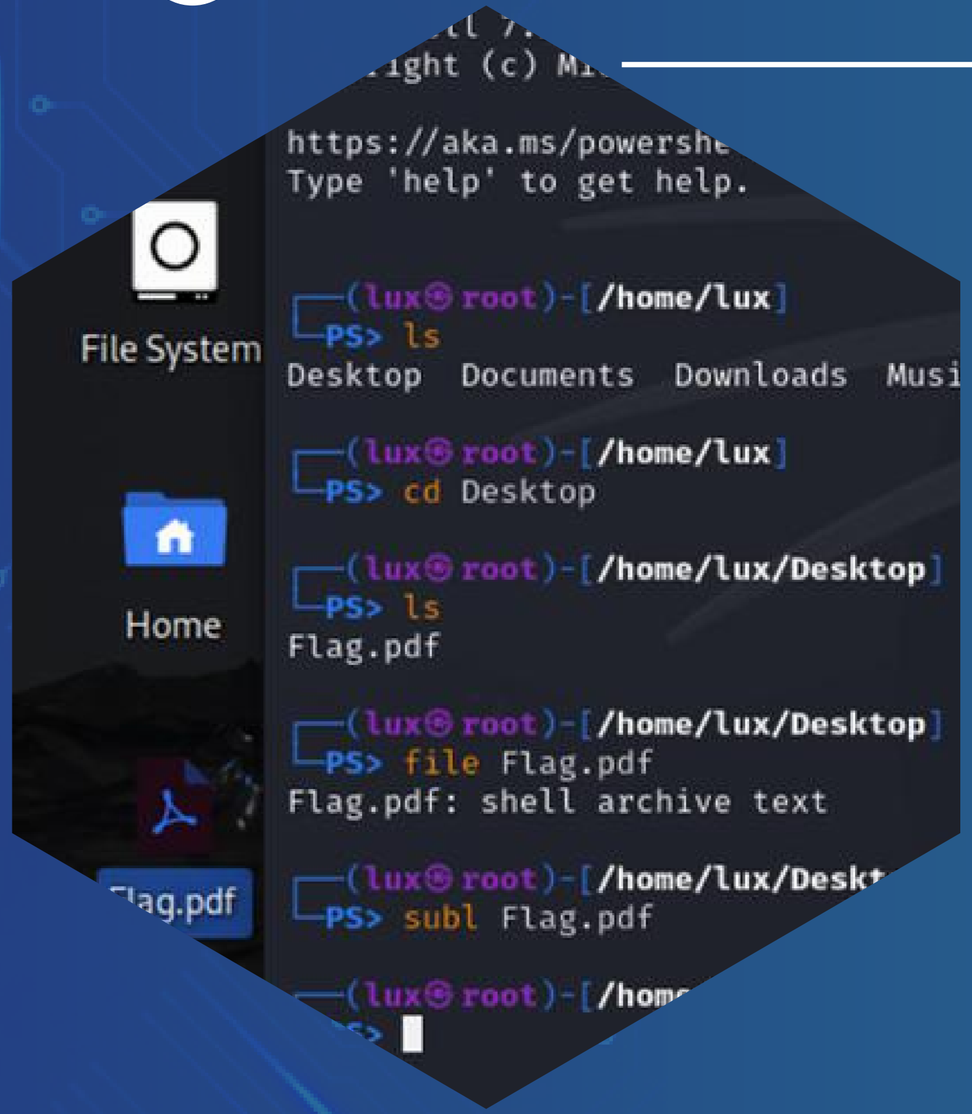
This file was found among some files marked confidential but my pdf reader cannot read it, maybe yours can.

Once downloaded, the file displayed the error message, "Impossible to load the PDF document." The first step was to inspect the file using the browser's developer tools to see if any elements or metadata could provide clues. However, nothing unusual was detected through this method.

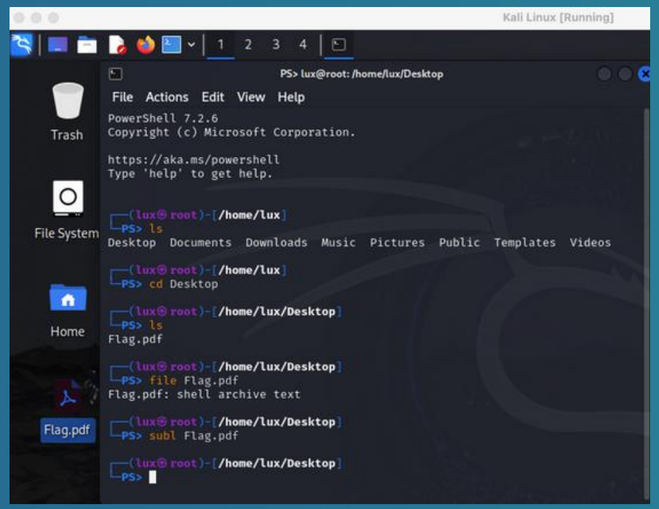
Upon further examination of the file's source, it became apparent that the file contained a nest of embedded files. This indicated that the strategy to solve the challenge would involve extracting these nested files to find the hidden flag.



SECOND CHALLENGE-KALI LINUX-EXTRACTION OF FLAG.PDF



Checking the File Type



- The file command is used to determine the file type. This command revealed that Flag-pdf was a shell archive text file.
- Checking the file type helps understand what tools and commands might be needed to extract or read the file.

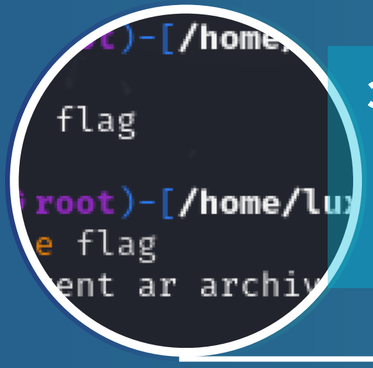
SECOND CHALLENGE-KALI LINUX-EXTRACTION OF FLAG.PDF

FURTHER STEPS

1.Opening the File

- subl (Sublime Text) is used to open the file in a text editor for inspection.
- Opening the file in a text editor allows for manual inspection of its contents.

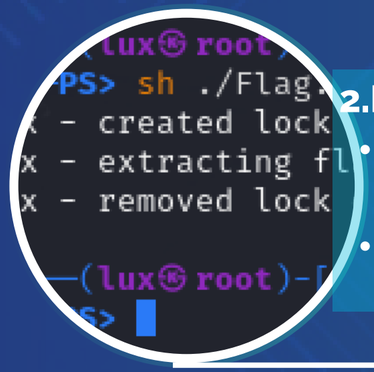
→ SUBL FLAG-PDF



3.Inspecting the Extracted Files

- The file command is used again to inspect the newly extracted file type, revealing it as an ar (archive) file.
- Identifying the file type guides the next steps for extraction.

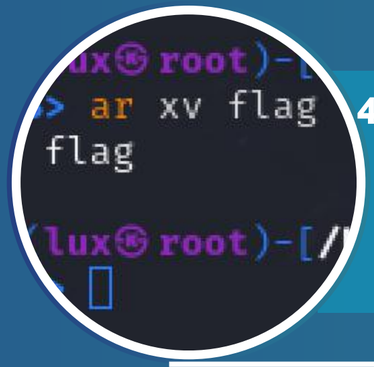
→ FILE FLAG



2.Extracting the Shell Archive

- Running the sh command executes the shell script to extract the contents of the shell archive.
- Since the file is a shell archive, running it will extract its contents.

→ SH FLAG-PDF



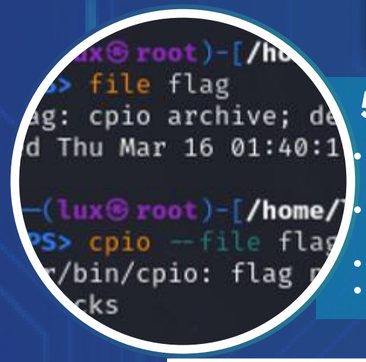
4.Extracting the AR Archive

- The ar command extracts files from the archive.
- Extracting the contents of the ar archive to reveal further nested files.

→ AR XV FLAG

SECOND CHALLENGE-KALI LINUX-EXTRACTION OF FLAG.PDF

FURTHER STEPS



5.Handling CPIO Archive

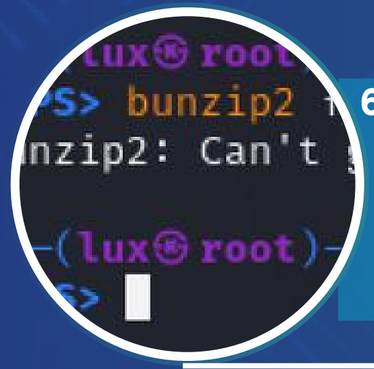
- The file command is used again to check the new file type, which is a cpio archive.
- Identifying the file type helps determine the correct extraction command.
- The cpio command extracts files from the cpio archive.
- Extracting the nested files to continue the search for the flag.

→ CPIO -ID < FLAG

7.Handling LZ4 Compression

- The lz4 command decompresses LZ4 compressed data.
- Further decompressing the file to continue the extraction process.

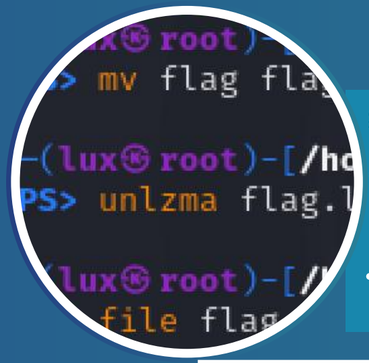
→ LZ4 -D FLAG.OUT FLAG
FILE FLAG



6.Handling Compression Layers

- These commands (bunzip2, gunzip) are used to handle compressed files (bzip2, gzip) and extract their contents.
- The file has multiple layers of compression. Each command is used to decompress and reveal the next layer.

→ FILE FLAG
BUNZIP2 FLAG
FILE FLAG.OUT
MV FLAG.OUT FLAG.GZ
GUNZIP FLAG.GZ
FILE FLAG



8.Handling LZMA and LZOP Compression

- Commands unlzma and lzop are used to handle LZMA and LZOP compression respectively.
- Each step involves decompressing the file until the final layer is reached.

→ MV FLAG FLAG.LZMA
UNLZMA FLAG.LZMA
FILE FLAG
MV FLAG FLAG.LZOP
LZOP -D FLAG.LZOP
FILE FLAG

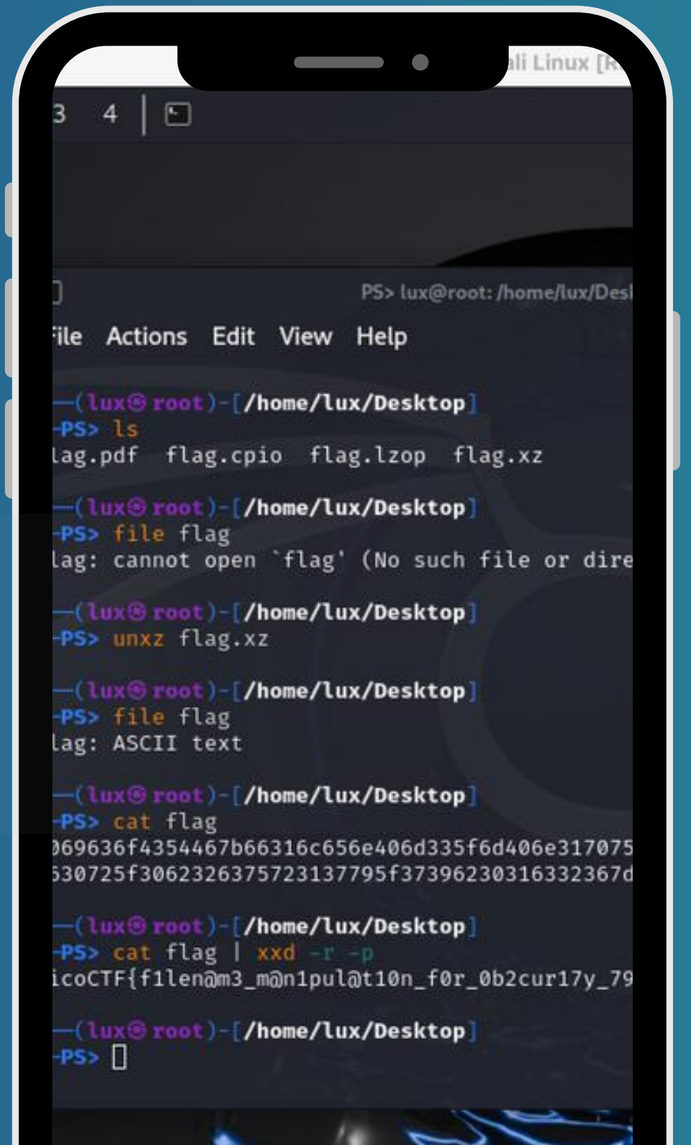
SECOND CHALLENGE-KALI LINUX-EXTRACTION OF FLAG.PDF

FINAL

DECOMPRESSION AND REVEALING THE FLAG

- Commands unxz and cat are used to handle XZ compression and read the final contents.
- The final step reveals the ASCII text which contains the flag in hexadecimal. Using xxd -r converts the hex to plain text, revealing the flag: **picoCTF{f1lenam3_m@n1pul@t10n_for_0b2cur17y_79b01c26}.**

→ MV FLAG FLAG.XZ
UNXZ FLAG.XZ
FILE FLAG LAG: ASCII TEXT
CAT FLAG | XXD -R -P
PICOCTF{F1LENAM3_M@N1PUL@T10N_FOR_0B2CUR17Y_79B01C26}



SECOND CHALLENGE-FILE TYPES PICOCTF PRACTICE LAB

Conclusion

This challenge demonstrates the importance of understanding different file types and compression methods in forensic analysis. By systematically identifying and extracting nested files, one can uncover hidden data and solve complex challenges. This process highlights the necessity of being proficient with command-line tools and understanding file formats in cybersecurity tasks.

THIRD CHALLENGE-CHECK OUT THIS WEBSITE, SEE IF YOU CAN SUBMIT YOUR NAME IN THE HIDDEN FORM!!

TARGET WEBSITE

https://rs11.mohammadlotfi.com/

OBJECTIVE

Analyze the given website to discover hidden elements or vulnerabilities. The specific task was to login and find a hidden form.

TOOLS USED

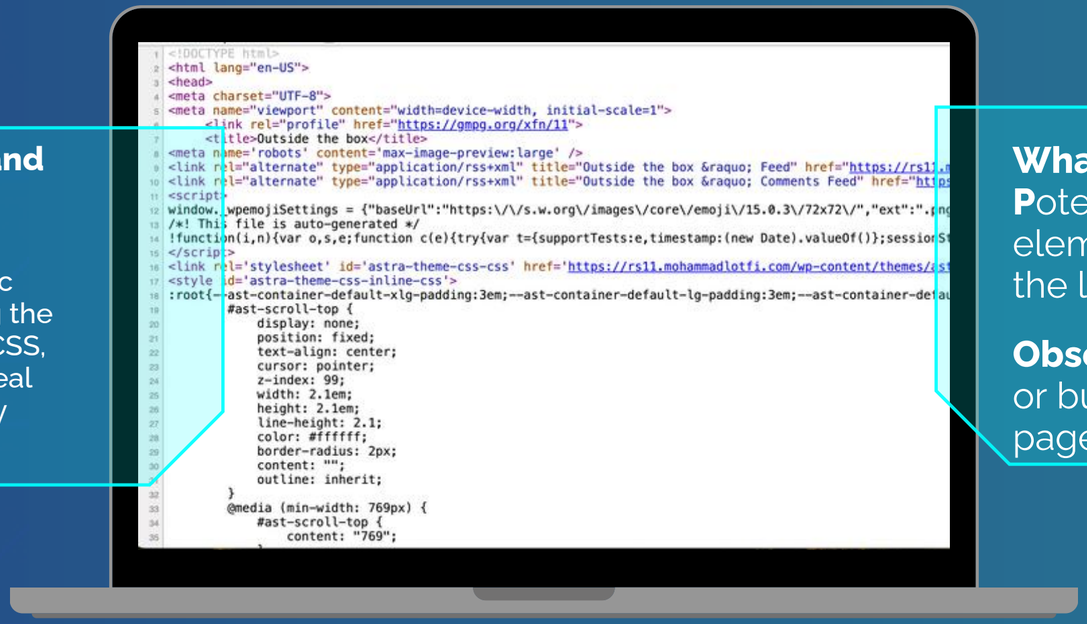
- Browser Developer Tools (e.g., Inspect Element)
- Burp Suite on Kali Linux
- Manual URL manipulation
- XML Sitemap analysis

THIRD CHALLENGE-CHECK OUT THIS WEBSITE, SEE IF YOU CAN SUBMIT YOUR NAME IN THE HIDDEN FORM!!

STEP 1: INITIAL INSPECTION

Action: Opened the website and inspected the page source.

The first step in any web security assessment is to understand the basic structure of the webpage. By viewing the page source, we can see the HTML, CSS, and any inline scripts, which may reveal hidden elements or comments left by developers.



What I Expected to Find:
Potential hints or hidden elements that could lead to the login form.

Observation: No visible forms or buttons leading to a login page.

THIRD CHALLENGE-CHECK OUT THIS WEBSITE, SEE IF YOU CAN SUBMIT YOUR NAME IN THE HIDDEN FORM!!

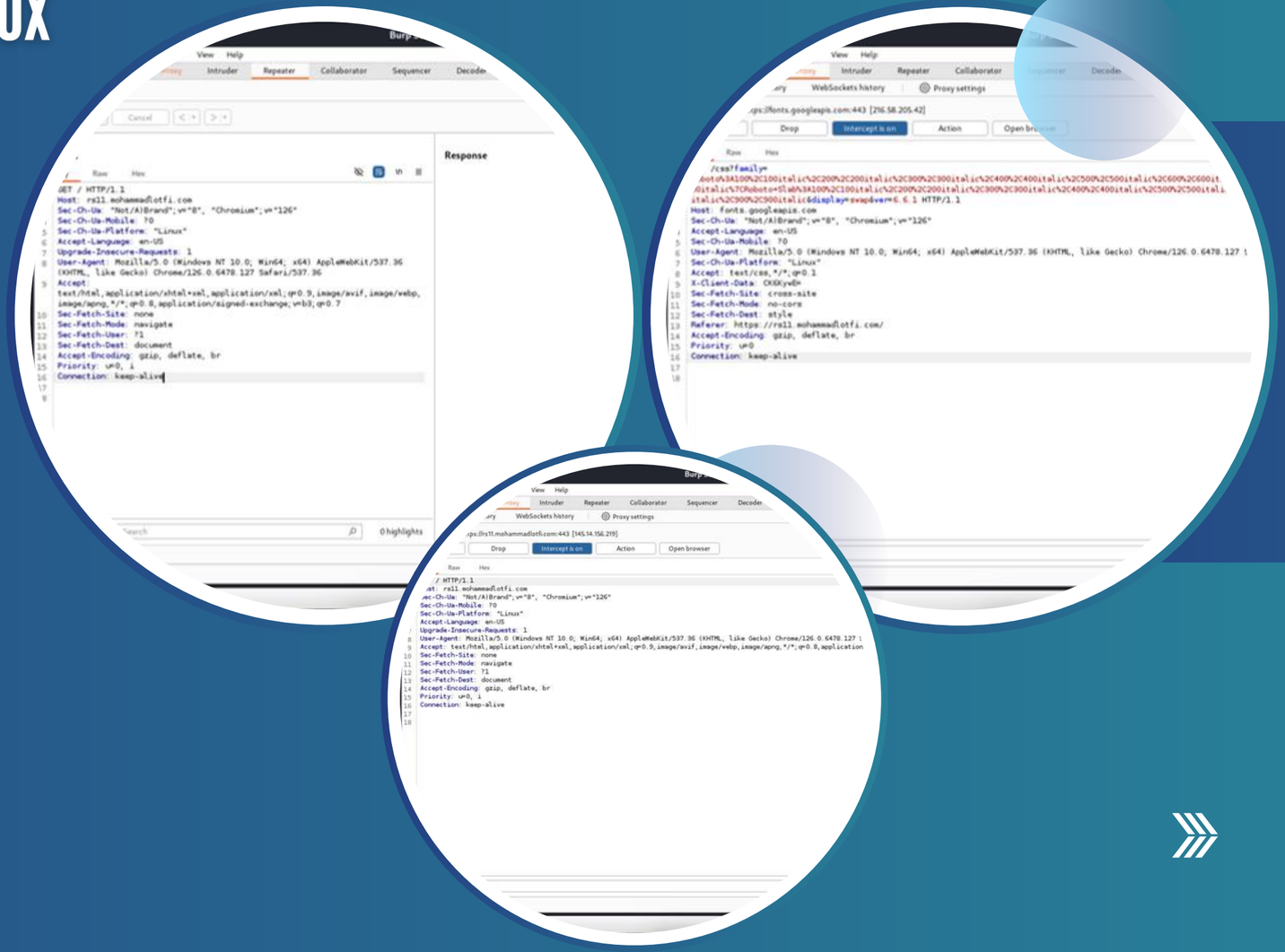
STEP 2: USING BURP SUITE ON KALI LINUX

Burp Suite is a powerful tool for intercepting and modifying web traffic. By capturing requests and responses, I could potentially uncover hidden interactions or data being exchanged with the server.

Action: Configured Burp Suite to intercept and analyze traffic.

What I Expected to Find: Hidden POST requests, parameters, or redirect paths that might indicate a login form submission.

Observation: Only GET requests were observed, indicating no form submissions or login actions.



THIRD CHALLENGE-CHECK OUT THIS WEBSITE, SEE IF YOU CAN SUBMIT YOUR NAME IN THE HIDDEN FORM!!

STEP 3: URL MANIPULATION

Manually altering URLs is a common technique to discover hidden admin pages or login forms. Many web applications have predictable URL patterns for these functionalities.

Action

Tried various common URL paths (e.g., /admin, /login, /php)

What I Expected to Find

A direct link to the login page or a page that provides more information.

Observation

Redirected to other pages or the WordPress login page.

THIRD CHALLENGE-CHECK OUT THIS WEBSITE, SEE IF YOU CAN SUBMIT YOUR NAME IN THE HIDDEN FORM!!

STEP 4: XML SITEMAP ANALYSIS

01

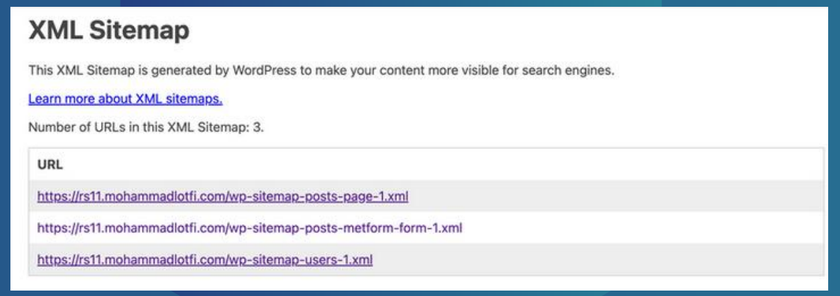
Action

Navigated to the XML Sitemap at **https://rs11.mohammadlotfi.com/wp-sitemap.xml**.

Sitemaps are often used by search engines to index content, and they can reveal all accessible URLs on a website, including those not directly linked from the main site.

02

What I found



03

Identifying the Correct Subdomain

Noted the subdomain containing the keyword "form" - https://rs11.mohammadlotfi.com/wp-sitemap-posts-metform-form-1.xml.

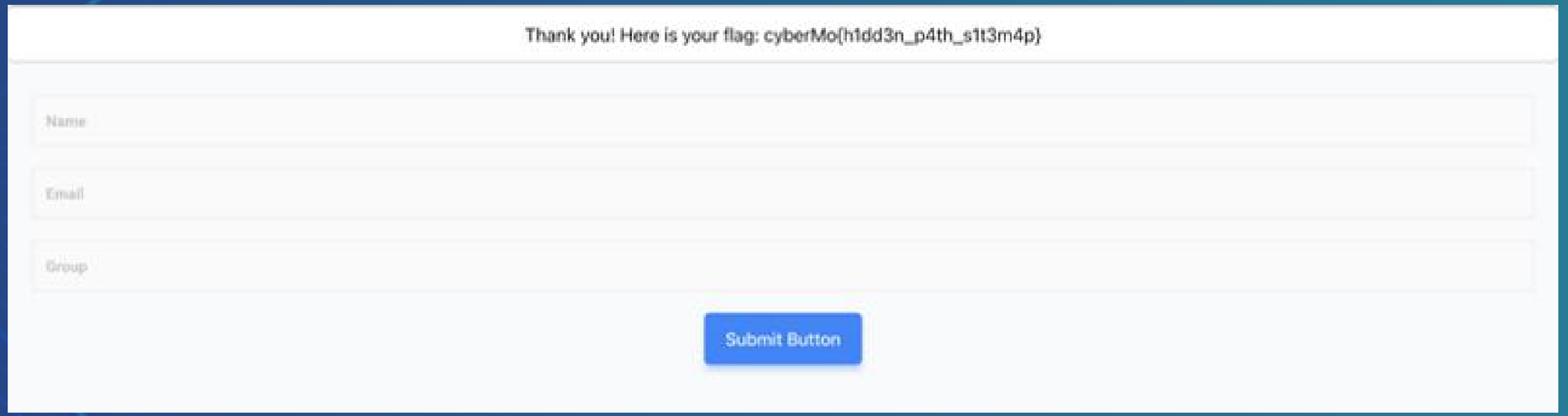
THIRD CHALLENGE-CHECK OUT THIS WEBSITE, SEE IF YOU CAN SUBMIT YOUR NAME IN THE HIDDEN FORM!!

STEP 5: ACCESSING THE HIDDEN FORM

https://rs11.mohammadlotfi.com/index.php/metform-form/namano/

Filled out the form with the required information.

- Submitting the form as requested is the final step to complete the challenge and reveal any hidden information or flag.
- What I Expected to Find: The solution flag or confirmation of successful form submission.
- Observation: Received the solution flag: **cyberMo{h1dd3n_p4th_s1t3m4p}.**



THIRD CHALLENGE-CHECK OUT THIS WEBSITE, SEE IF YOU CAN SUBMIT YOUR NAME IN THE HIDDEN FORM!!

CONCLUSION

The analysis successfully identified the hidden form by examining the XML Sitemap, leading to the discovery of the flag. This method highlights the importance of checking sitemap files during web security assessments, as they can reveal hidden paths and resources.

Theoretical Insights and Strategies

- Source Code Inspection: Often reveals hidden comments, elements, and scripts that can provide clues about the website's structure.
- Traffic Analysis with Burp Suite: Useful for uncovering hidden interactions, parameters, and potential vulnerabilities in web traffic.
- URL Manipulation: Explores common and predictable paths that developers might use for administrative or hidden functionalities.
- Sitemap Exploration: An essential step in identifying all accessible URLs, especially those not linked directly from the main website. Sitemaps are a goldmine for uncovering hidden content.

By combining these strategies, a comprehensive understanding of the website's structure and hidden elements was achieved, leading to the successful completion of the challenge.