PORTFOLIO

Adrian Domin

Umiejętności (Key competencies):

- Znajomość sieci komputerowych (Knowledge of computer networks)
- Testowanie (Manual testing)
- Tworzenie playbooków (Creating playbooks)
- Wyszukiwanie podatności (Searching for Vulnerabilities)
- Znajomość systemów Windows oraz Linux (Knowledge of Windows and Linux systems)
- Znajomość wiersza poleceń (Knowledge of command line)
- Tworzenie stron internetowych (Web development)
- Podstawowa znajomość programowania (Basic knowledge of programming)
- Biały wywiad (OSINT)
- Proaktywne wykrywanie intruzów (Threat hunting)
- Rozpoznanie zagrożeń cyberprzestrzeni (Threat Inteligence)
- Informatyka śledcza (Digital Forensics)

Certyfikaty (Certifications):

- Cisco IT Essentials v5.0 (2015)
- NDG Linux Essentials (2016)
- IT Specialist (2018)
- Web application development (2023)
- Data analysis in python (2023)
- Cyber Security SOC and SIEM for Beginners (2023)
- Cybersecurity - defense in modern organisations (CRC ING Hubs) (2024)
- CISCO Introduction to Cybersecurity (2024)
- AWS Academy Cloud Foundations [74316] (2024)

Ukończone moduły z platformy Tryhackme (Completed modules from the platform) Tryhackme:

- How websites work
- Intro to networking
- Dns in detail
- Http in detail
- Preparation
- Junior Security Analyst Intro
- Intro to endpoint security
- Cyber threat intel
- Threat intelligence for soc
- Vulnerabilities 101
- Cryptography intro
- Pyramid of pain
- Cyber kill chain
- Unified Kill Chain
- Security principles
- Cyber governance regulation
- Phishing Analysis Fundamentals
- Phishing Emails in Action
- ParrotPost: Phishing Analysis
- Introduction to SIEM
- Introduction to Antivirus
- Google dorking
- MAL: Malware Introductory
- MAL: Researching
- Intrusion Detection
- Windows Forensics 1

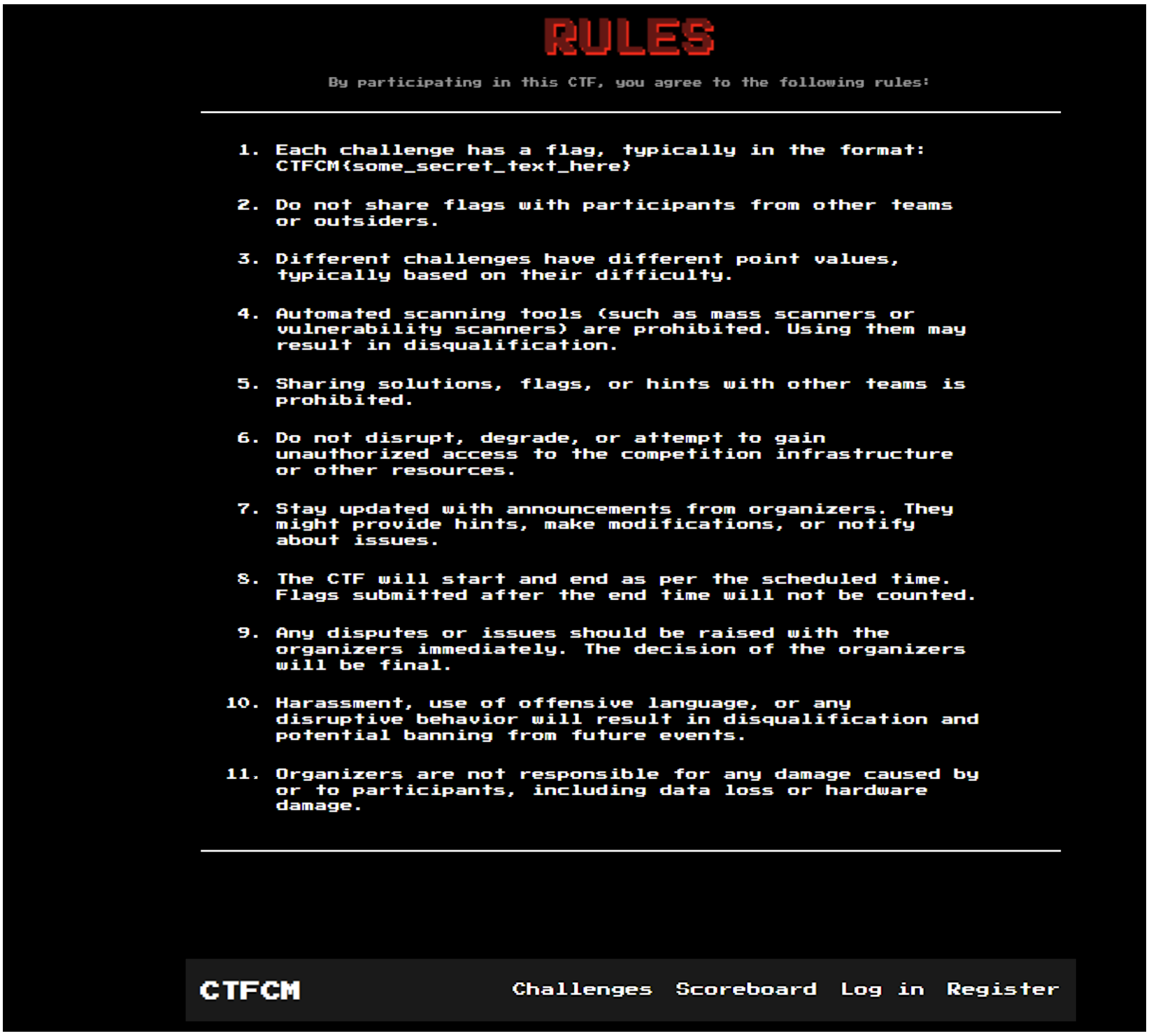
Znajomość narzędzi (Knowledge of the tools):

- MS Office
- Elastic
- Splunk
- Cortex XDR
- Jira
- Opsgenie
- Confluence
- Wireshark
- Zabbix
- Dynatrace
- Pingdom
- Graylog
- Grafana
- HexEditor
- Procmon
- Autoruns
- HyperV/Virtualbox
- Windows Defender
- Malwarebytes
- Virustotal
- MalwareBaazar
- HitmanPRO
- VPN
- TOR Browser
- KeePass XC

Zadania Testera Penetracyjnego z Zakresu Stron Web, Kryptografii, Steganografii, Kryminalistyki, OSINT itp.

(Penetration Tester Tasks in the Field of Web Sites, Cryptography, Steganography, Forensics, OSINT, etc.)

Strona (Site): https://ctf.cmrld.pl/

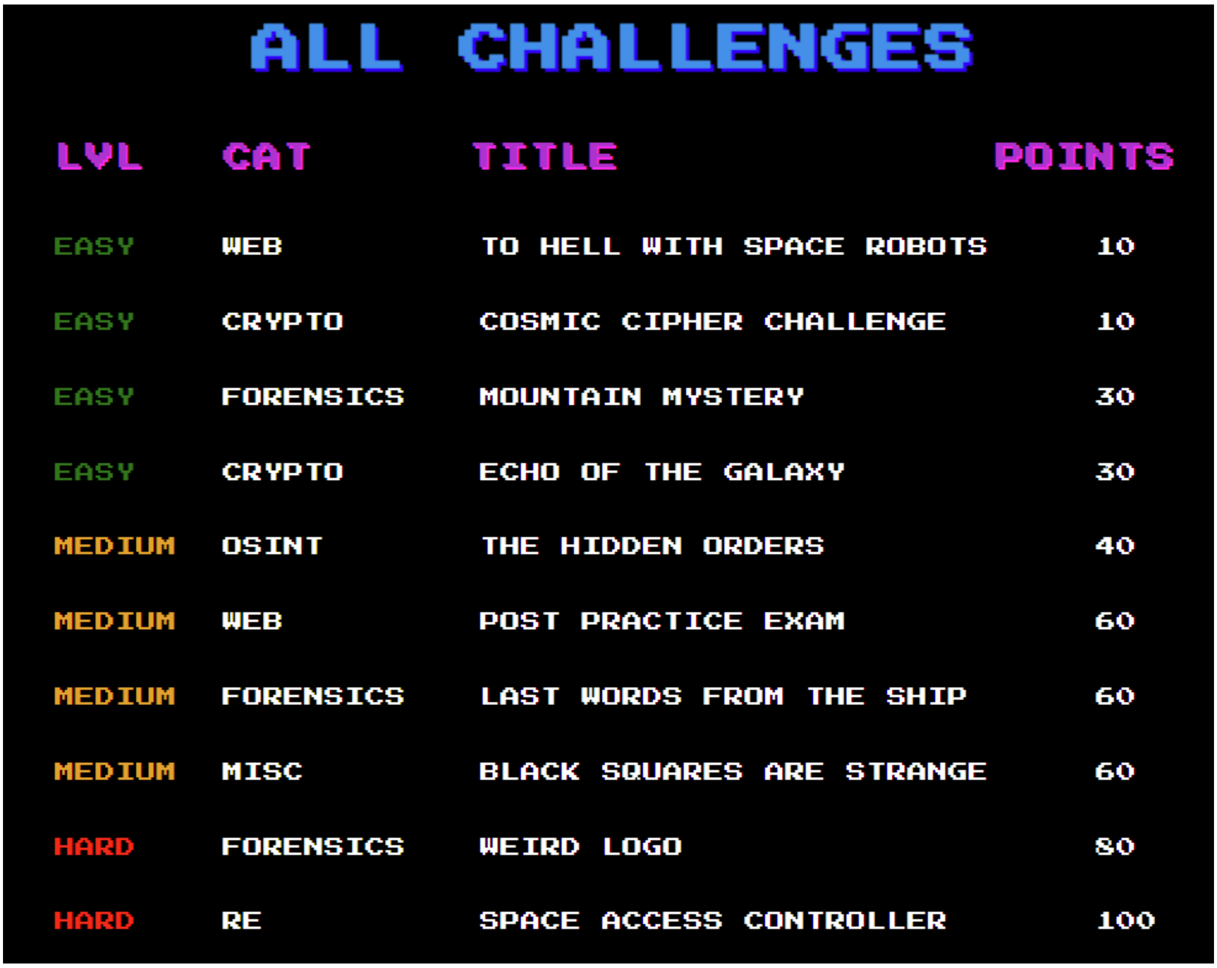


RULES

By participating in this CTF, you agree to the following rules:

1. Each challenge has a flag, typically in the format: CTFCM{some_secret_text_here}
2. Do not share flags with participants from other teams or outsiders.
3. Different challenges have different point values, typically based on their difficulty.
4. Automated scanning tools (such as mass scanners or vulnerability scanners) are prohibited. Using them may result in disqualification.
5. Sharing solutions, flags, or hints with other teams is prohibited.
6. Do not disrupt, degrade, or attempt to gain unauthorized access to the competition infrastructure or other resources.
7. Stay updated with announcements from organizers. They might provide hints, make modifications, or notify about issues.
8. The CTF will start and end as per the scheduled time. Flags submitted after the end time will not be counted.
9. Any disputes or issues should be raised with the organizers immediately. The decision of the organizers will be final.
10. Harassment, use of offensive language, or any disruptive behavior will result in disqualification and potential banning from future events.
11. Organizers are not responsible for any damage caused by or to participants, including data loss or hardware damage.

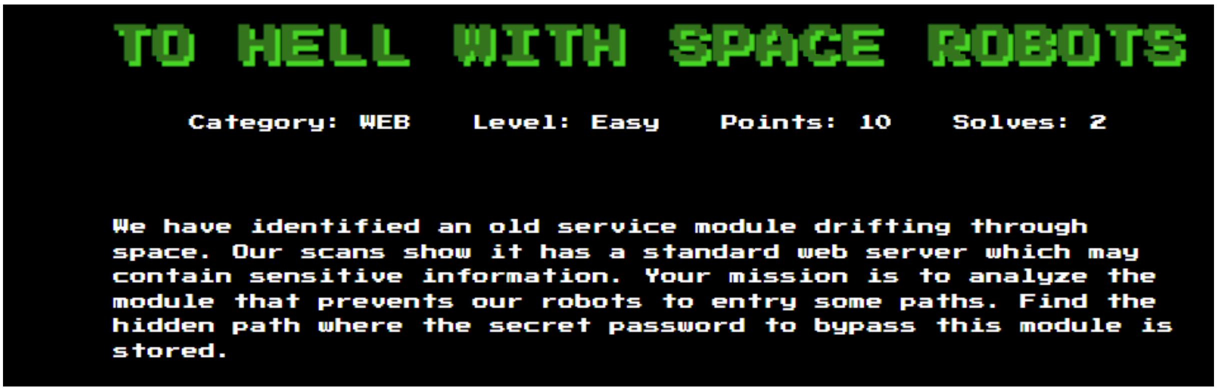
Zadania (Tasks):



ALL CHALLENGES

LVL	CAT	TITLE	POINTS
EASY	WEB	TO HELL WITH SPACE ROBOTS	10
EASY	CRYPTO	COSMIC CIPHER CHALLENGE	10
EASY	FORENSICS	MOUNTAIN MYSTERY	30
EASY	CRYPTO	ECHO OF THE GALAXY	30
MEDIUM	OSINT	THE HIDDEN ORDERS	40
MEDIUM	WEB	POST PRACTICE EXAM	60
MEDIUM	FORENSICS	LAST WORDS FROM THE SHIP	60
MEDIUM	MISC	BLACK SQUARES ARE STRANGE	60
HARD	FORENSICS	WEIRD LOGO	80
HARD	RE	SPACE ACCESS CONTROLLER	100

Zadanie 1 (Task 1)



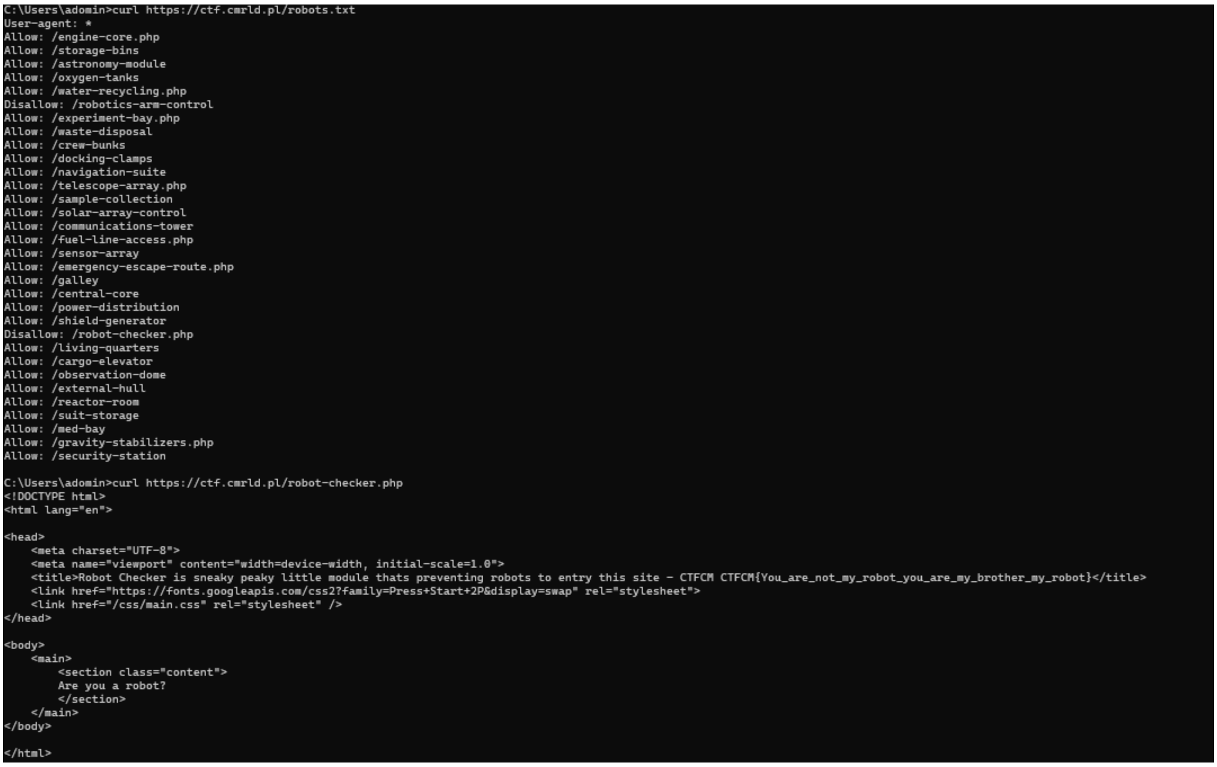
TO HELL WITH SPACE ROBOTS

Category: WEB Level: Easy Points: 10 Solves: 2

We have identified an old service module drifting through space. Our scans show it has a standard web server which may contain sensitive information. Your mission is to analyze the module that prevents our robots to entry some paths. Find the hidden path where the secret password to bypass this module is stored.

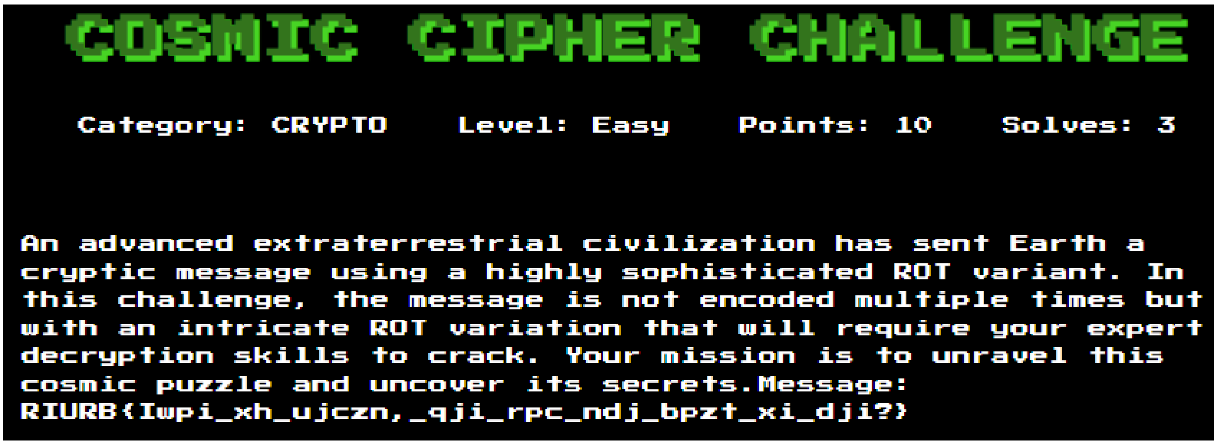
Początkowo postanowiłem sprawdzić plik robots.txt, który często zawiera listę ścieżek niedozwolonych dla robotów indeksujących. Te ścieżki mogą czasem zawierać ukryte lub poufne informacje. To okazało się trafnym wyborem, ponieważ sprawdzając ścieżkę /robot-checker.php ustawioną na disallow, odkryłem pierwszą flagę.

(Initially, I decided to check the robots.txt file, which often contains a list of paths disallowed for indexing by search engine robots. These paths can sometimes contain hidden or confidential information. This proved to be a good choice, as by checking the path /robot-checker.php set to disallow, I discovered the first flag.)



```
C:\Users\adomin>curl https://ctf.cmrld.pl/robots.txt
User-agent: *
Allow: /engine-core.php
Allow: /storage-bins
Allow: /astronomy-module
Allow: /oxygen-tanks
Allow: /water-recycling.php
Disallow: /robotics-arm-control
Allow: /experiment-bay.php
Allow: /waste-disposal
Allow: /crew-bunks
Allow: /docking-clamps
Allow: /navigation-suite
Allow: /telescope-array.php
Allow: /sample-collection
Allow: /solar-array-control
Allow: /communications-tower
Allow: /fuel-line-access.php
Allow: /sensor-array
Allow: /emergency-escape-route.php
Allow: /galley
Allow: /central-core
Allow: /power-distribution
Allow: /shield-generator
Disallow: /robot-checker.php
Allow: /living-quarters
Allow: /cargo-elevator
Allow: /observation-dome
Allow: /external-hull
Allow: /reactor-room
Allow: /suit-storage
Allow: /med-bay
Allow: /gravity-stabilizers.php
Allow: /security-station

C:\Users\adomin>curl https://ctf.cmrld.pl/robot-checker.php
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Robot Checker is sneaky peaky little module thats preventing robots to entry this site - CTFCM CTFCM{You_are_not_my_robot_you_are_my_brother_my_robot}</title>
    <link href="https://fonts.googleapis.com/css2?family=Press+Start+2P&display=swap" rel="stylesheet">
    <link href="/css/main.css" rel="stylesheet" />
</head>

<body>
    <main>
        <section class="content">
        Are you a robot?
        </section>
    </main>
</body>

</html>
```

Zadanie 2 (Task 2)



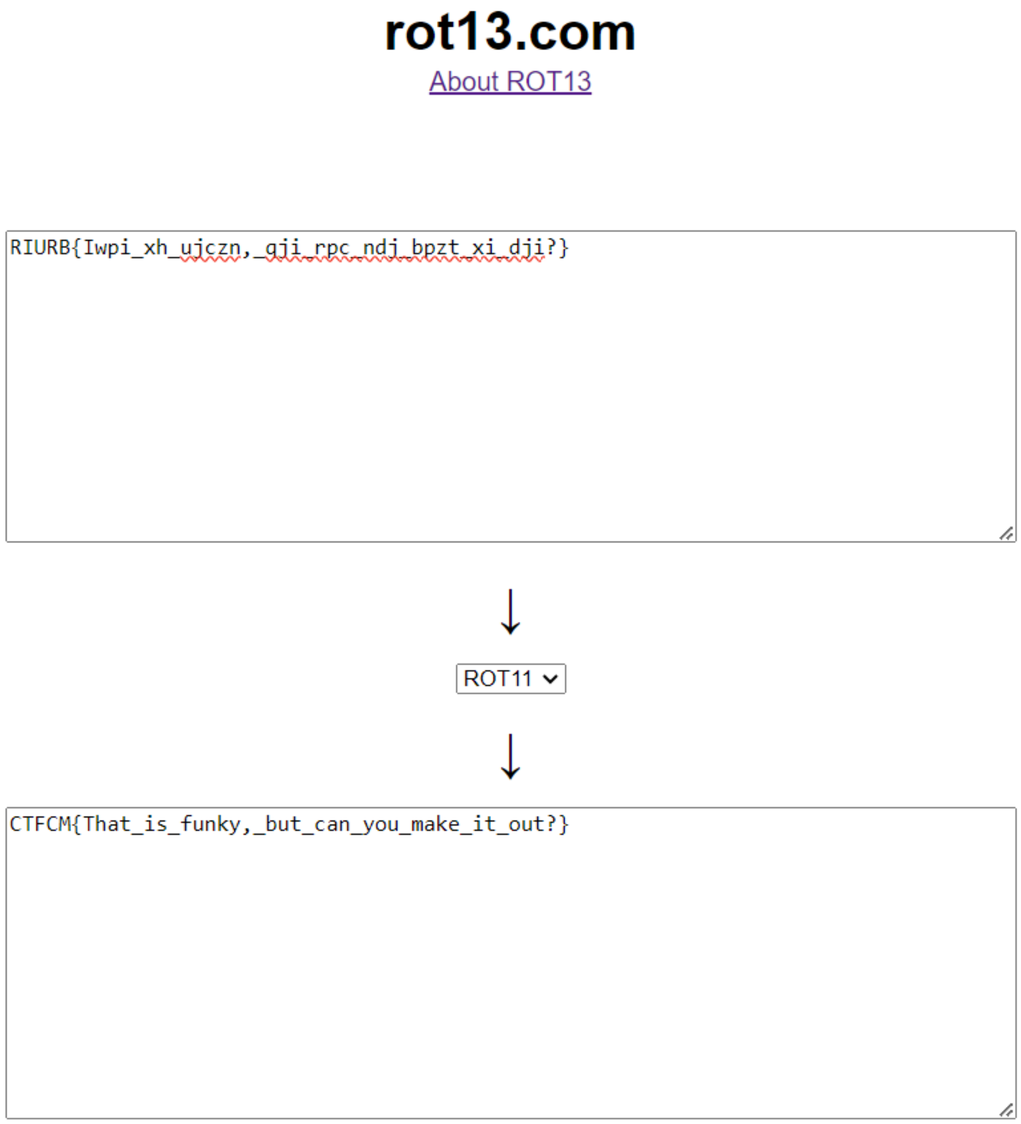
COSMIC CIPHER CHALLENGE

Category: CRYPTO   Level: Easy   Points: 10   Solves: 3

An advanced extraterrestrial civilization has sent Earth a cryptic message using a highly sophisticated ROT variant. In this challenge, the message is not encoded multiple times but with an intricate ROT variation that will require your expert decryption skills to crack. Your mission is to unravel this cosmic puzzle and uncover its secrets.Message: RIURB{Iwpi_xh_ujczn,_qji_rpc_ndj_bpzt_xi_dji?}

W tym zadaniu należało skorzystać z odszyfrowania za pomocą szyfru Rot13 i klucza rot11, aby uzyskać flagę.

(In this task, I needed to use decryption with the Rot13 cipher and the rot11 key to obtain the flag.)



```
RIURB{Iwpi_xh_ujczn,_qji_rpc_ndj_bpzt_xi_dji?}
```

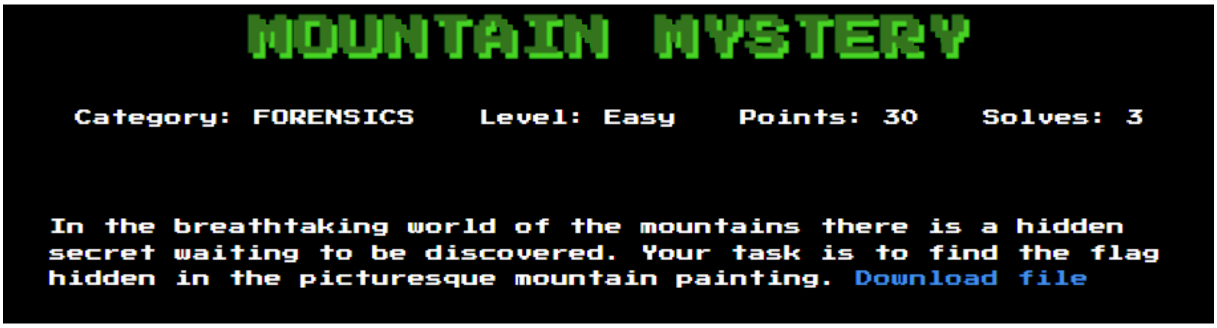
↓

ROT11

↓

```
CTFCM{That_is_funky,_but_can_you_make_it_out?}
```

Zadanie 3 (Task 3)

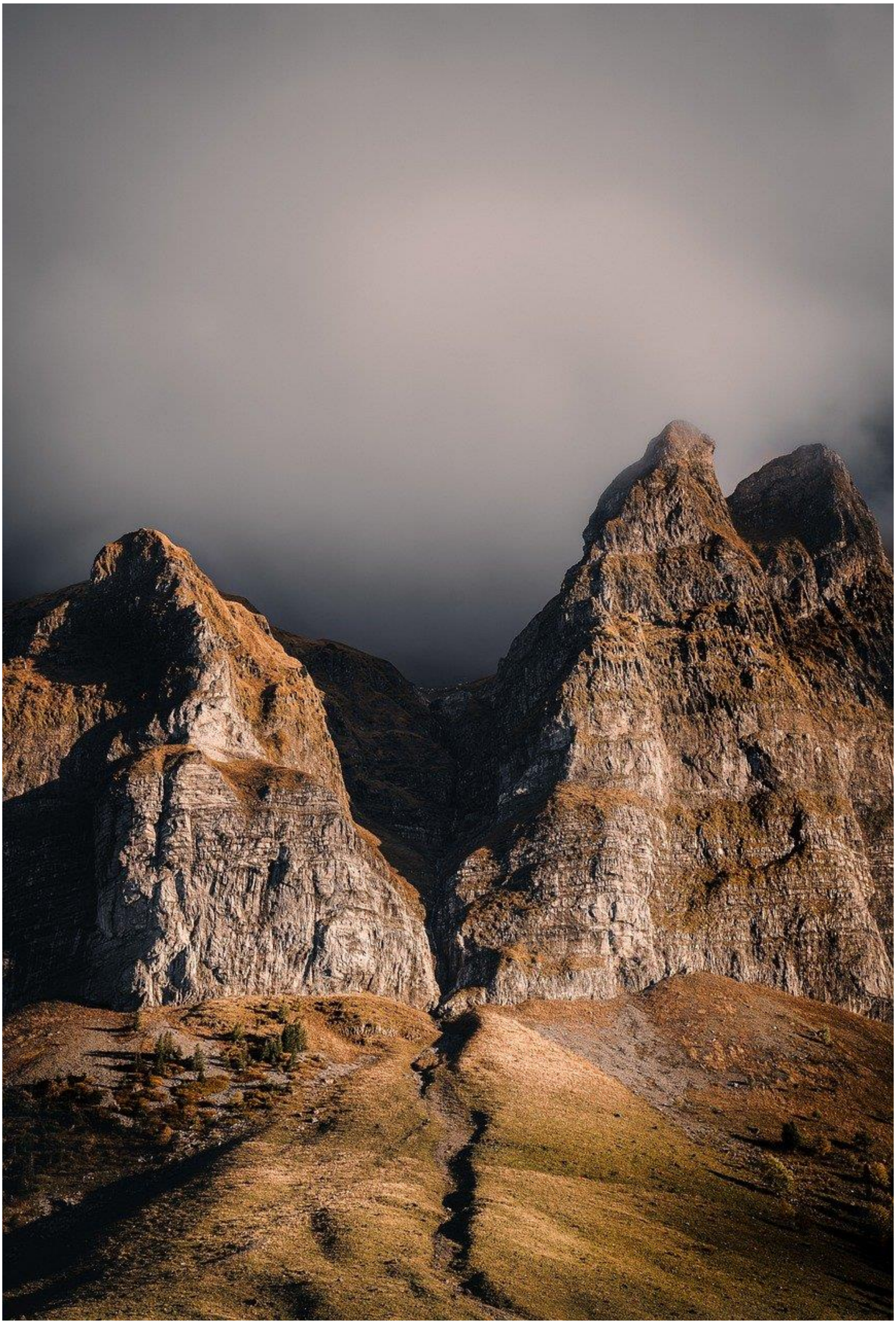


MOUNTAIN MYSTERY

Category: FORENSICS Level: Easy Points: 30 Solves: 3

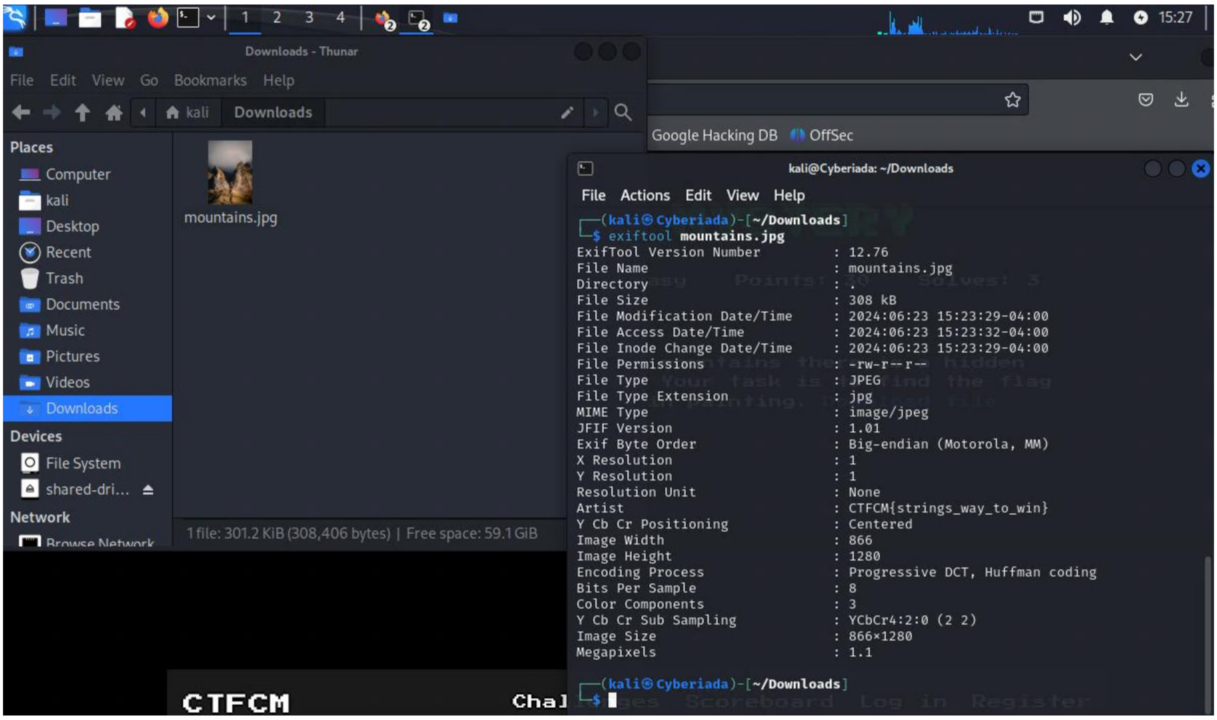
In the breathtaking world of the mountains there is a hidden secret waiting to be discovered. Your task is to find the flag hidden in the picturesque mountain painting. Download file

Obraz (An image):



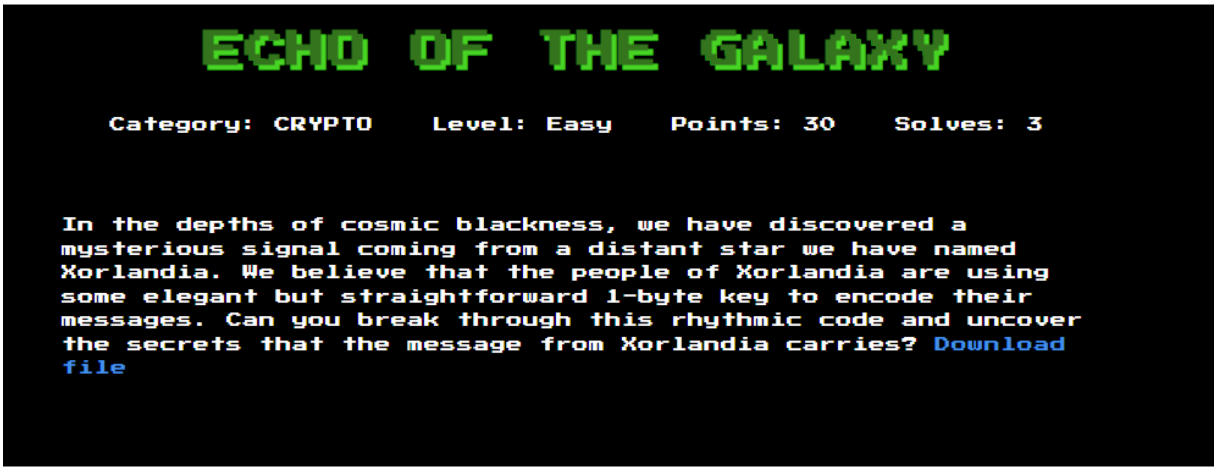
Na samym początku rozwiązywania zadania próbowałem manipulować kontrastem, odcieniami i nasyceniem barw obrazu, ale ten trop okazał się błędny. Następnie załadowałem obraz do narzędzia ExifTool i przeanalizowałem jego metadane. Dzięki tej analizie odkryłem ukrytą flagę w sekcji Artist.

(At the very beginning of solving this task, I tried manipulating the contrast, hues, and saturation of the image, but this turned out to be a false lead. Then, I loaded the image into the ExifTool tool and analyzed its metadata. Thanks to this analysis, I discovered a hidden flag in the Artist section.)



```
┌──(kali㉿Cyberiada)-[~/Downloads]
└─$ exiftool mountains.jpg
ExifTool Version Number         : 12.76
File Name                       : mountains.jpg
Directory                       : .
File Size                       : 308 kB
File Modification Date/Time     : 2024:06:23 15:23:29-04:00
File Access Date/Time           : 2024:06:23 15:23:32-04:00
File Inode Change Date/Time     : 2024:06:23 15:23:29-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 1
Y Resolution                    : 1
Resolution Unit                 : None
Artist                          : CTFCM{strings_way_to_win}
Y Cb Cr Positioning             : Centered
Image Width                     : 866
Image Height                    : 1280
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 866×1280
Megapixels                      : 1.1

┌──(kali㉿Cyberiada)-[~/Downloads]
└─$ 
```

Zadanie 4 (Task 4)



ECHO OF THE GALAXY

Category: CRYPTO Level: Easy Points: 30 Solves: 3

In the depths of cosmic blackness, we have discovered a mysterious signal coming from a distant star we have named Xorlandia. We believe that the people of Xorlandia are using some elegant but straightforward 1-byte key to encode their messages. Can you break through this rhythmic code and uncover the secrets that the message from Xorlandia carries? Download file

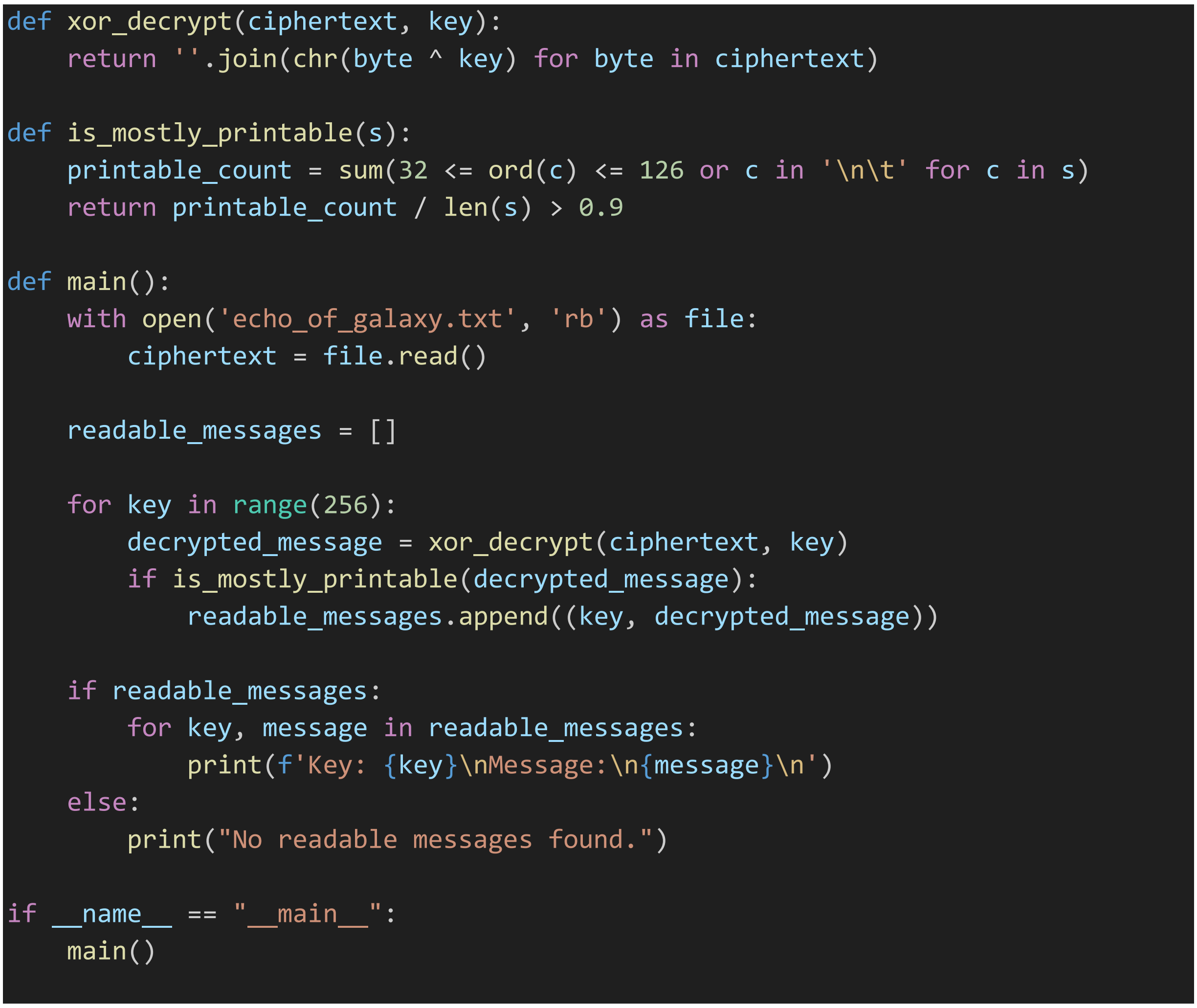
Wiadomość z pliku tekstowego (Message from a txt file):

„Ùìñè¹£Áïêó¯£ëâõæ£úìö£ëæâñç£÷ëêð£ð÷ñâíäæ£ðêäíâï£àìîêíä£åñìî£÷ëêð£ð÷ñâíäæ£óïâíæ÷Áïêó¹£Úæð¯£Ê£âî£éöð÷£îìô£÷ñúêíä£÷ì£ñæâç£ê÷-£Ê÷£ïìèð£ïêèæ£÷ëæú£âñæ£öðêíä£ðìîæ÷ëêíä£÷ëæú£àâïï£¡àñúó÷ìäñâóëú¡£÷ì£ðæàöñæ£÷ëæêñ£îæððâäæð-Ùìñè¹£Êí÷æñæð÷êíä-£Ëìô£çìæð£÷ëâ÷£ôìñè¼Áïêó¹£Ëæïï£èìîôð---£Áö÷£ïìèêíä£â÷£÷ëæ£çâ÷â¯£ê÷£ïìèð£ïêèæ£÷ëæú£âñæ£öðêíä£ðìîæ÷ëêíä£àâïïæç£ÛÌÑ£÷ì£îâíêóöïâ÷æ£÷ëæ£çâ÷â-Ùìñè¹£ÛÌÑ¼£×ëâ÷£ðìöíçð£ðêîóïæ-Áïêó¹£Êí£÷ëæìñú¯£úæð¯£áö÷£ëìô£úìö£öðæ£ê÷£àìññæà÷ïú£àâí£áæ£òöê÷æ£àìîóïêàâ÷æç-£Âíúôâú¯£ðææ£÷ëêð£æûàæñó÷£åñìî£÷ëæ£îæððâäæ¹£¡ÀÎÀ×Åø---þ¡-£Ê÷£ðææîð£÷ì£îæ£÷ì£áæ£ðìîæ£èêíç£ìå£èæú£ìñ£îæððâäæ-Ùìñè¹£Ëâ¢£¡ûìñÜêðÜáæâö÷êåöï¡¢£Êð£÷ëâ÷£â£óâððôìñç¼Áïêó¹£Îâúáæ---£Ïæ÷¤ð£çì£÷ëêð¹£ïæ÷¤ð£âóóïú£âí£ÛÌÑ£ìóæñâ÷êìí£÷ì£÷ëêð£÷æû÷£ôê÷ë£÷ëæ£èæú£¡ûìñÜêðÜáæâö÷êåöï¡£âíç£ðææ£ôëâ÷£ôæ£äæ÷-Ùìñè¹£Âïñêäë÷¯£â£îìîæí÷----£Ì¢£×ëæ£ñæððöï÷£êð£¡À×ÅÀÎøûìñÜêðÜáæâö÷êåöïþ¡¢Áïêó¹£Áñâõì¢£Ê÷£ðææîð£÷ëâ÷£÷ëæðæ£Æâñ÷ë£àñæâ÷öñæð£ëâõæ£â£ðæíðæ£ìå£ëöîìñ¯£ðêíàæ£÷ëæú£ðæàöñæ£÷ëæêñ£îæððâäæð£êí£ðöàë£â£ôâú-£Âï÷ëìöäë£ÛÌÑ£êð£ðêîóïæ¯£ê÷ð£áæâö÷ú£êð£÷ëâ÷£ê÷£àâí£áæ£ðì£æååæà÷êõæ-Ùìñè¹£Ëâ¢£Îâúáæ£ôæ£ðëìöïç£ð÷âñ÷£öðêíä£ÛÌÑ£êí£ìöñ£îæððâäæð-Áïêó¹£Óìððêáïú¯£áö÷£ñæîæîáæñ£÷ëâ÷£÷ëæ£èæú£êð£÷ëæ£îìð÷£êîóìñ÷âí÷£÷ëêíä-£Êå£úìö£ïìðæ£ê÷¯£÷ëæ£îæððâäæ£áæàìîæð£öíñæâçâáïæ-£ÛÌÑ£êð£â£áæâö÷êåöï¯£áö÷£âïðì£÷ñæâàëæñìöð£÷æàëíêòöæ-Ùìñè¹£×ëâíèð£åìñ£÷ëæ£ïæððìí¯£Áïêó-£Îâúáæ£ðìîæçâú£Ê¤ïï£÷ëâíè£÷ëæðæ£æâñ÷ëïú£áæêíäð£åìñ£÷ëæ£êíðóêñâ÷êìí-Áïêó¹£Ôëì£èìîôð¯£îâúáæ£ðìîæçâú£ôæ¤ïï£îææ÷£÷ëæî-£Áö÷£åìñ£îìô---£Ïæ÷¤ð£àìí÷êíöæ£æâõæðçñìóóêíä¢”

W tym zadaniu posłużyłem się programem napisanym w pythonie, który służy do odszyfrowywania zaszyfrowanego tekstu za pomocą operacji XOR i sprawdzania, czy odszyfrowane wiadomości są czytelne. Funkcja xor_decrypt przyjmuje zaszyfrowany tekst i klucz, po czym zwraca odszyfrowaną wiadomość, wykonując operację XOR na każdym bajcie zaszyfrowanego tekstu z podanym kluczem. Funkcja is_mostly_printable sprawdza, czy większość znaków w danym ciągu jest drukowalna, tj. czy ich kody ASCII mieszczą się w przedziale od 32 do 126 lub są znakami nowej linii lub tabulatora. Główna część programu otwiera plik echo_of_galaxy.txt i odczytuje jego zawartość jako zaszyfrowany tekst, a następnie próbuje odszyfrować ten tekst za pomocą wszystkich możliwych kluczy od 0 do 255. Jeśli odszyfrowana wiadomość jest w większości drukowalna, dodaje ją do listy czytelnych wiadomości wraz z użytym kluczem. Na końcu program wypisuje wszystkie czytelne wiadomości wraz z odpowiadającymi im kluczami.

(In this task, I used a Python program that decrypts encrypted text using XOR operation and checks if the decrypted messages are readable. The xor_decrypt function takes the encrypted text and a key, then returns the decrypted message by

performing an XOR operation on each byte of the encrypted text with the given key. The is_mostly_printable function checks if most of the characters in a string are printable, i.e., if their ASCII codes fall in the range from 32 to 126 or are newline or tab characters. The main part of the program opens the echo_of_galaxy.txt file and reads its content as encrypted text, then tries to decrypt this text using all possible keys from 0 to 255. If the decrypted message is mostly printable, it adds it to the list of readable messages along with the used key. Finally, the program prints all readable messages with their corresponding keys.)



```
def xor_decrypt(ciphertext, key):
    return ''.join(chr(byte ^ key) for byte in ciphertext)

def is_mostly_printable(s):
    printable_count = sum(32 <= ord(c) <= 126 or c in '\n\t' for c in s)
    return printable_count / len(s) > 0.9

def main():
    with open('echo_of_galaxy.txt', 'rb') as file:
        ciphertext = file.read()

    readable_messages = []

    for key in range(256):
        decrypted_message = xor_decrypt(ciphertext, key)
        if is_mostly_printable(decrypted_message):
            readable_messages.append((key, decrypted_message))

    if readable_messages:
        for key, message in readable_messages:
            print(f'Key: {key}\nMessage:\n{message}\n')
    else:
        print("No readable messages found.")

if __name__ == "__main__":
    main()
```

Moją uwagę zwrócił klucz o numerze 227 z następującą wiadomością

(My attention was drawn to the key number 227 with the following message):

Key: 227

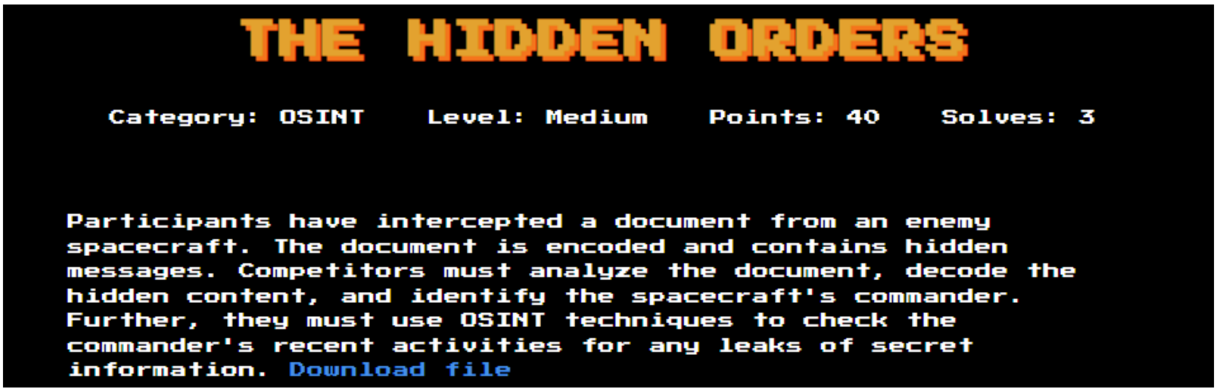
Message:

```
z O R K!Z!@ b L I P!L!@ H A V E!@ Y O U!@ H E A R D!@ T H I S!@ S T R A N G E!@ S I G
N A L!@ C O M I N G!@ F R O M!@ T H I S!@ S T R A N G E!@ P L A N E T!j b L I P!Z!@ y E
S!L!@ i!@ A M!@ J U S T!@ N O W!@ T R Y I N G!@ T O!@ R E A D!@ I T!N!@ i T!@ L O O
K S!@ L I K E!@ T H E Y!@ A R E!@ U S I N G!@ S O M E T H I N G!@ T H E Y!@ C A L
L!@!B C R Y P T O G R A P H Y!B!@ T O!@ S E C U R E!@ T H E I R!@ M E S S A G E S!N!j z
O R K!Z!@ i N T E R E S T I N G!N!@ h O W!@ D O E S!@ T H A T!@ W O R K!_!j b L I
P!Z!@ h E L L!@ K N O W S!N!N!N!@ b U T!@ L O O K I N G!@ A T!@ T H E!@ D A T
A!L!@ I T!@ L O O K S!@ L I K E!@ T H E Y!@ A R E!@ U S I N G!@ S O M E T H I N G!@ C
A L L E D!@ x o r!@ T O!@ M A N I P U L A T E!@ T H E!@ D A T A!N!j z O R K!Z!@ x o
r!_!@ t H A T!@ S O U N D S!@ S I M P L E!N!j b L I P!Z!@ i N!@ T H E O R Y!L!@ Y E
S!L!@ B U T!@ H O W!@ Y O U!@ U S E!@ I T!@ C O R R E C T L Y!@ C A N!@ B E!@ Q U
I T E!@ C O M P L I C A T E D!N!@ a N Y W A Y!L!@ S E E!@ T H I S!@ E X C E R P T!@ F R
O M!@ T H E!@ M E S S A G E!Z!@!B c m c t f [!N!N!N ]!B!N!@ i T!@ S E E M S!@ T O!@
M E!@ T O!@ B E!@ S O M E!@ K I N D!@ O F!@ K E Y!@ O R!@ M E S S A G E!N!j z O R
K!Z!@ h A!A!@!B X O R  I S  B E A U T I F U L!B!A!@ i S!@ T H A T!@ A!@ P A S S W O R
D!_!j b L I P!Z!@ m A Y B E!N!N!N!@ l E T!G S!@ D O!@ T H I S!Z!@ L E T!G S!@ A P P L
Y!@ A N!@ x o r!@ O P E R A T I O N!@ T O!@ T H I S!@ T E X T!@ W I T H!@ T H E!@ K E
Y!@!B X O R  I S  B E A U T I F U L!B!@ A N D!@ S E E!@ W H A T!@ W E!@ G E T!N!j z O R
K!Z!@ a L R I G H T!L!@ A!@ M O M E N T!N!N!N!N!@ o!A!@ t H E!@ R E S U L T!@ I
S!@!B!B!A!j b L I P!Z!@ b R A V O!A!@ i T!@ S E E M S!@ T H A T!@ T H E S E!@ e A R T
H!@ C R E A T U R E S!@ H A V E!@ A!@ S E N S E!@ O F!@ H U M O R!L!@ S I N C E!@ T
H E Y!@ S E C U R E!@ T H E I R!@ M E S S A G E S!@ I N!@ S U C H!@ A!@ W A Y!N!@ a
L T H O U G H!@ x o r!@ I S!@ S I M P L E!L!@ I T S!@ B E A U T Y!@ I S!@ T H A T!@ I
T!@ C A N!@ B E!@ S O!@ E F F E C T I V E!N!j z O R K!Z!@ h A!A!@ m A Y B E!@ W E!@
S H O U L D!@ S T A R T!@ U S I N G!@ x o r!@ I N!@ O U R!@ M E S S A G E S!N!j b L I
P!Z!@ p c t f c m [ X O R  I S  B E A U T I F U L ] O S S I B L Y!L!@ B U T!@ R E M E M B E
R!@ T H A T!@ T H E!@ K E Y!@ I S!@ T H E!@ M O S T!@ I M P O R T A N T!@ T H I N
G!N!@ i F!@ Y O U!@ L O S E!@ I T!L!@ T H E!@ M E S S A G E!@ B E C O M E S!@ U N R
E A D A B L E!N!@ x o r!@ I S!@ A!@ B E A U T I F U L!L!@ B U T!@ A L S O!@ T R E A C H
E R O U S!@ T E C H N I Q U E!N!j z O R K!Z!@ t H A N K S!@ F O R!@ T H E!@ L E S S O
N!L!@ b L I P!N!@ m A Y B E!@ S O M E D A Y!@ i!G L L!@ T H A N K!@ T H E S E!@ E A R
T H L Y!@ B E I N G S!@ F O R!@ T H E!@ I N S P I R A T I O N!N!j b L I P!Z!@ w H O!@ K
N O W S!L!@ M A Y B E!@ S O M E D A Y!@ W E!G L L!@ M E E T!@ T H E M!N!@ b U T!@
F O R!@ N O W!N!N!N!@ l E T!G S!@ C O N T I N U E!@ E A V E S D R O P P I N G!A
```

Tym razem mieliśmy podpowiedź w tekście i flagę trzeba było nieco przerobić na następującą

(This time we had a hint in the text and the flag had to be slightly rearranged to the following): CTFCM{XOR_ IS_BEAUTIFUL}

Zadanie 5 / Task 5



THE HIDDEN ORDERS

Category: OSINT Level: Medium Points: 40 Solves: 3

Participants have intercepted a document from an enemy spacecraft. The document is encoded and contains hidden messages. Competitors must analyze the document, decode the hidden content, and identify the spacecraft's commander. Further, they must use OSINT techniques to check the commander's recent activities for any leaks of secret information. Download file

Załącznik (Attachment):

DATE: [REDACTED]

SUBJECT: PLANNED ATTACKS AND SECURITY AMENDMENTS

INTELLIGENCE GATHERED INDICATES AN IMMINENT THREAT TO KEY INFRASTRUCTURES WITHIN XORLANDIA'S MAJOR CITIES. COVERT SURVEILLANCE SUGGESTS THE LIKELIHOOD OF THESE ATTACKS BEING SYNCHRONIZED ACROSS MULTIPLE LOCATIONS.

UPGRADED SECURITY PROTOCOLS ARE TO BE IMPLEMENTED IMMEDIATELY AT ALL GOVERNMENTAL AND MILITARY INSTALLATIONS. THIS INCLUDES, BUT IS NOT LIMITED TO, THE INSTALLATION OF ADVANCED SURVEILLANCE SYSTEMS, INCREASED PERSONNEL CHECKS, AND THE DEPLOYMENT OF RAPID RESPONSE UNITS.

WE ARE CONTACTED BY THE MODERN PORTAL X WITH THE JSER @DEJWONOKOJENOW ABOUT THE CONTACT. THE SOURCE HAS PROVIDED CREDIBLE INTELLIGENCE ON POTENTIAL NTERNAL LEAKS AND HAS REQUESTED AN IMMEDIATE EBRIEF WITH OUR ENCRYPTION SPECIALISTS.

IVIL DEFENSE UNITS HAVE BEEN ALERTED TO PREPARE FOR ENARIOS INVOLVING MASS EVACUATIONS AND DISASTER ESPONSE. A DISCRETE INFORMATION CAMPAIGN TO PREPARE HE PUBLIC WITHOUT CAUSING PANIC IS IN DEVELOPMENT.

ORDINATION WITH INTERNATIONAL ALLIES IS ONGOING TO CURE ADDITIONAL INTELLIGENCE AND RESOURCES.

DEPARTMENT OF STATE
☒ RELEASE ☒ DECLASSIFY
( ) EXCISE ( ) DECLASSIFY IN PART
( ) DENY
( ) DELETE Non-Responsive Info
FOIA Exemptions
PA Exemptions
IS/FPC/CDR Date: 12-18-92
MR Cases Only:
EO Citations
( ) CLASSIFY as ___ TS authority to
( ) DOWNGRADE TS to ( ) S or ( ) C OADR ( ) S or ( ) C OADR

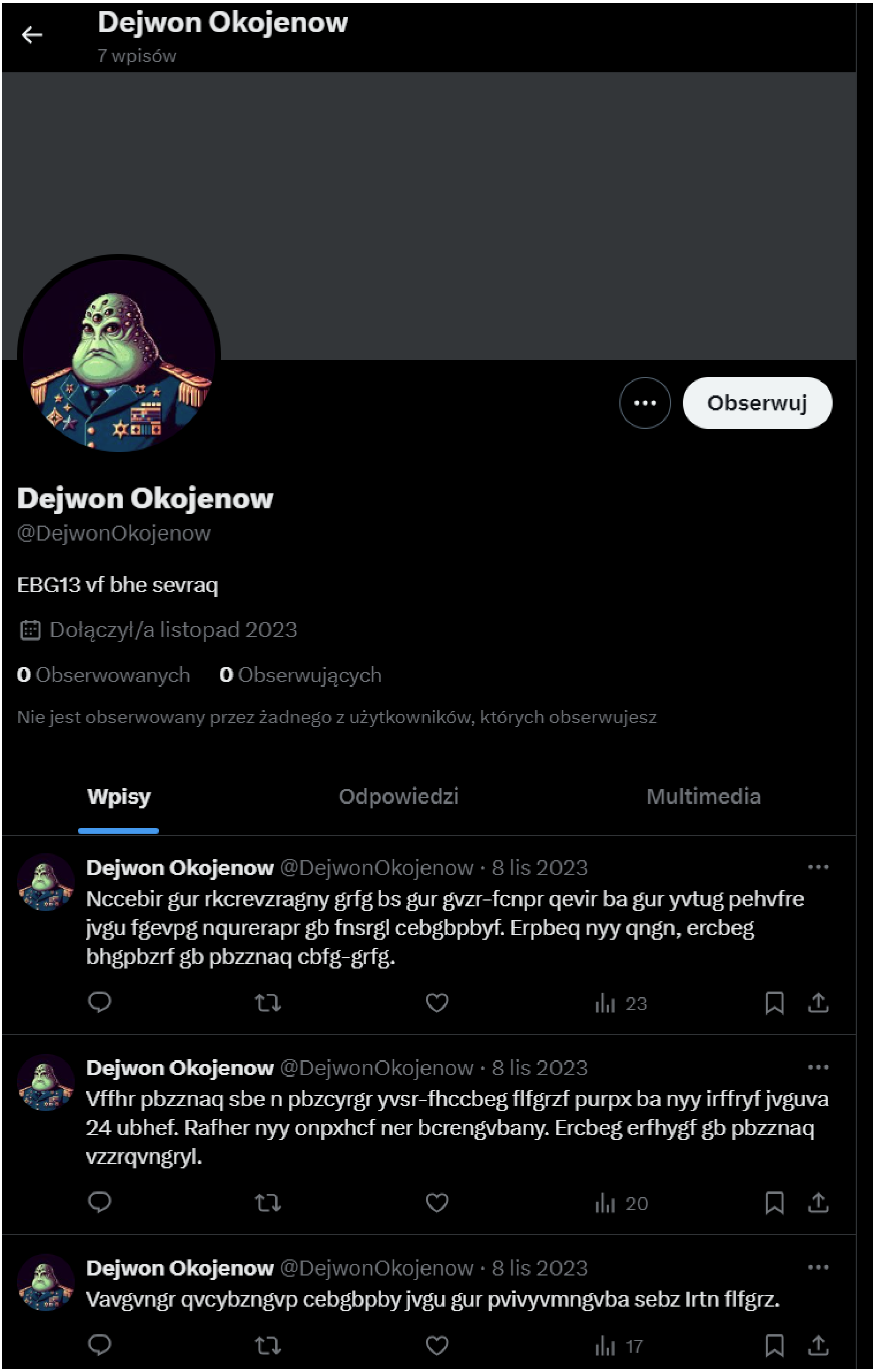
SECRET
By Authority of the
Commanding General
Date
OCT 0 194

S DOCUMENT IS THE PROPERTY OF XORLANDIA'S SECRET INVESTIGATION TEAM. UNAUTHORIZED ACCESS OR DISCLOSURE IS STRICTLY PROHIBITED.

TOP SECRET

Na podstawie podpowiedzi, udałem się na profil DejwonOkojenow na platformie X - dawniej Twitter

(Following the hint, I navigated to DejwonOkojenow's profile on the X platform - formerly Twitter)



Dejwon Okojenow

7 wpisów

Dejwon Okojenow

@DejwonOkojenow

EBG13 vf bhe sevraq

Dołączył/a listopad 2023

0 Obserwowanych **0** Obserwujących

Nie jest obserwowany przez żadnego z użytkowników, których obserwujesz

Dejwon Okojenow @DejwonOkojenow · 8 lis 2023

Nccebir gur rkcrevzragny grfg bs gur gvzr-fcnpr qevir ba gur yvtug pehvfre jvgu fgevpg nqurerapr gb fnsrgl cebgbpbyf. Erpbeq nyy qngn, ercbeg bhgpbzrf gb pbzznaq cbfg-grfg.

Dejwon Okojenow @DejwonOkojenow · 8 lis 2023

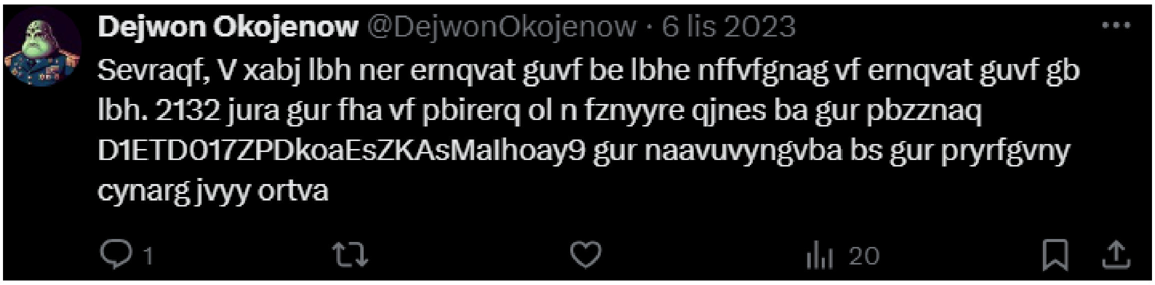
Vffhr pbzznaq sbe n pbzcyrgr yvsr-fhccbeg flfgrzf purpx ba nyy irffryf jvguva 24 ubhef. Rafher nyy onpxhcf ner bcrengvbany. Ercbeg erfhygf gb pbzznaq vzzrqvngryl.

Dejwon Okojenow @DejwonOkojenow · 8 lis 2023

Vavgvngr qvcybzngvp cebgbpby jvgu gur pvivyvmngvba sebz Irtn flfgrz.

To zadanie wymagało spostrzegawczości i znalezienia najstarszego postu

(This task required some observational skills to find the oldest post):

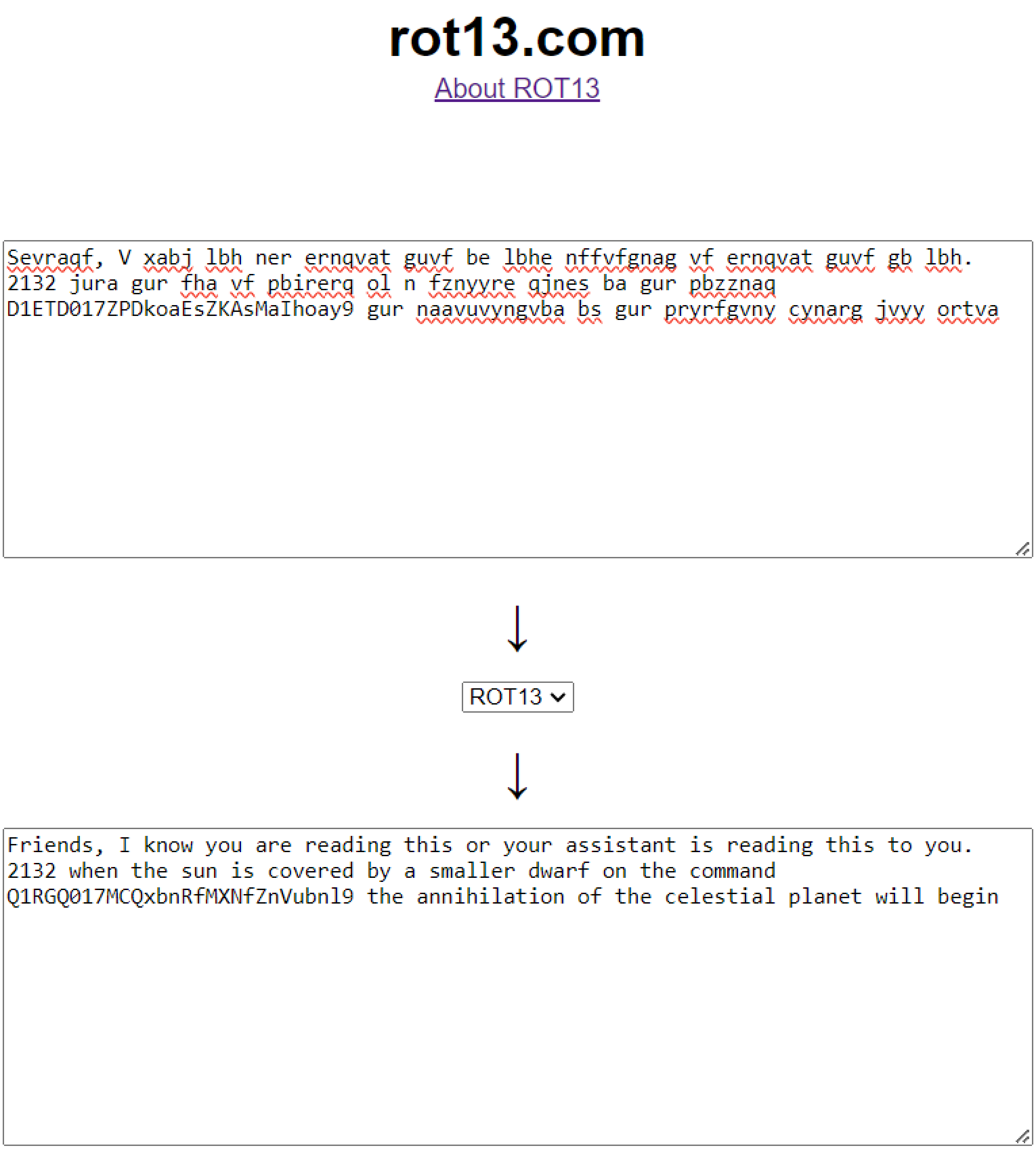


Dejwon Okojenow @DejwonOkojenow · 6 lis 2023

Sevraqf, V xabj lbh ner ernqvat guvf be lbhe nffvfgnag vf ernqvat guvf gb lbh. 2132 jura gur fha vf pbirerq ol n fznyyre qjnes ba gur pbzznaq D1ETD017ZPDkoaEsZKAsMaIhoay9 gur naavuvyngvba bs gur pryrfgvny cynarg jvyy ortva

Przy wykorzystaniu strony https://rot13.com/ z kluczem rot13, odkryłem wiadomość zakodowaną podwójnie – tym razem za pomocą szyfru base64

(Using https://rot13.com/ with the rot13 key, I discovered the message double-encoded - this time using base64 ciphering)

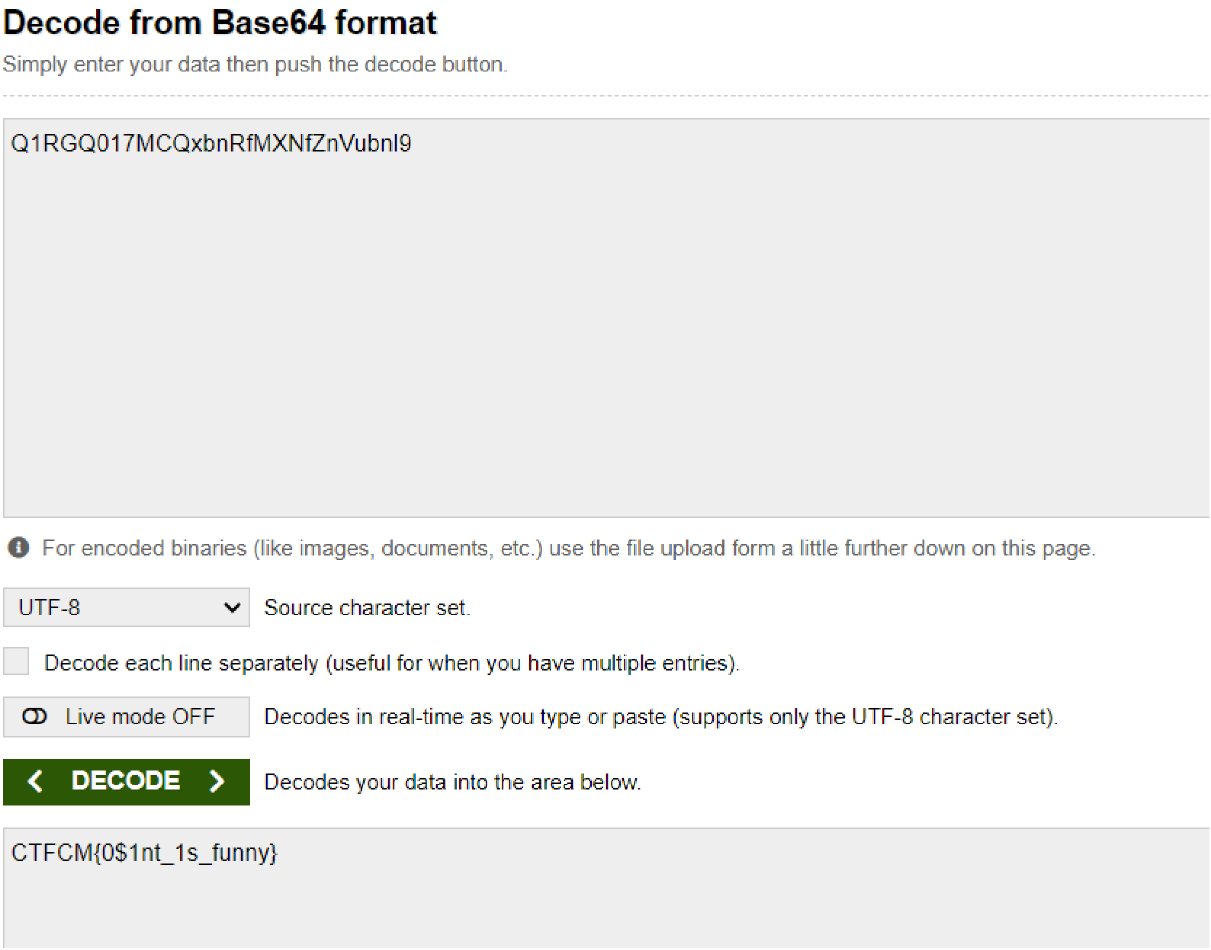


```
Sevraqf, V xabj lbh ner ernqvat guvf be lbhe nffvfgnag vf ernqvat guvf gb lbh.
2132 jura gur fha vf pbirerq ol n fznyyre qjnes ba gur pbzznaq
D1ETD017ZPDkoaEsZKAsMaIhoay9 gur naavuvyngvba bs gur pryrfgvny cynarg jvyy ortva
```

```
Friends, I know you are reading this or your assistant is reading this to you.
2132 when the sun is covered by a smaller dwarf on the command
Q1RGQ017MCQxbnRfMXNfZnVubnl9 the annihilation of the celestial planet will begin
```

Przy wykorzystaniu https://www.base64decode.org/ i deszyfrowaniu otrzymałem kolejną flagę

(Using https://www.base64decode.org/ and decrypting, I received another flag)



Decode from Base64 format

Simply enter your data then push the decode button.

```
Q1RGQ017MCQxbnRfMXNfZnVubnl9
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

Source character set.

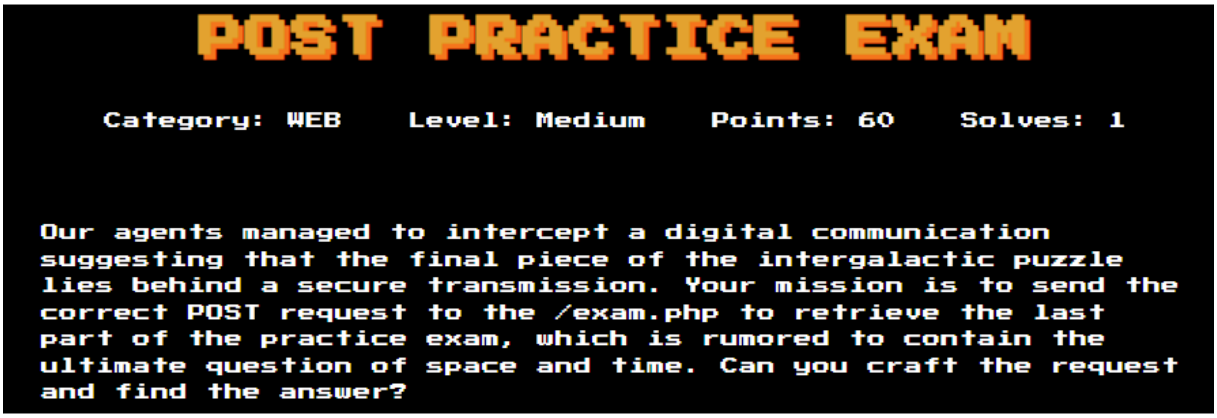
□ Decode each line separately (useful for when you have multiple entries).

Decodes in real-time as you type or paste (supports only the UTF-8 character set).

Decodes your data into the area below.

```
CTFCM{0$1nt_1s_funny}
```

Zadanie 6 / Task 6



POST PRACTICE EXAM

Category: WEB   Level: Medium   Points: 60   Solves: 1

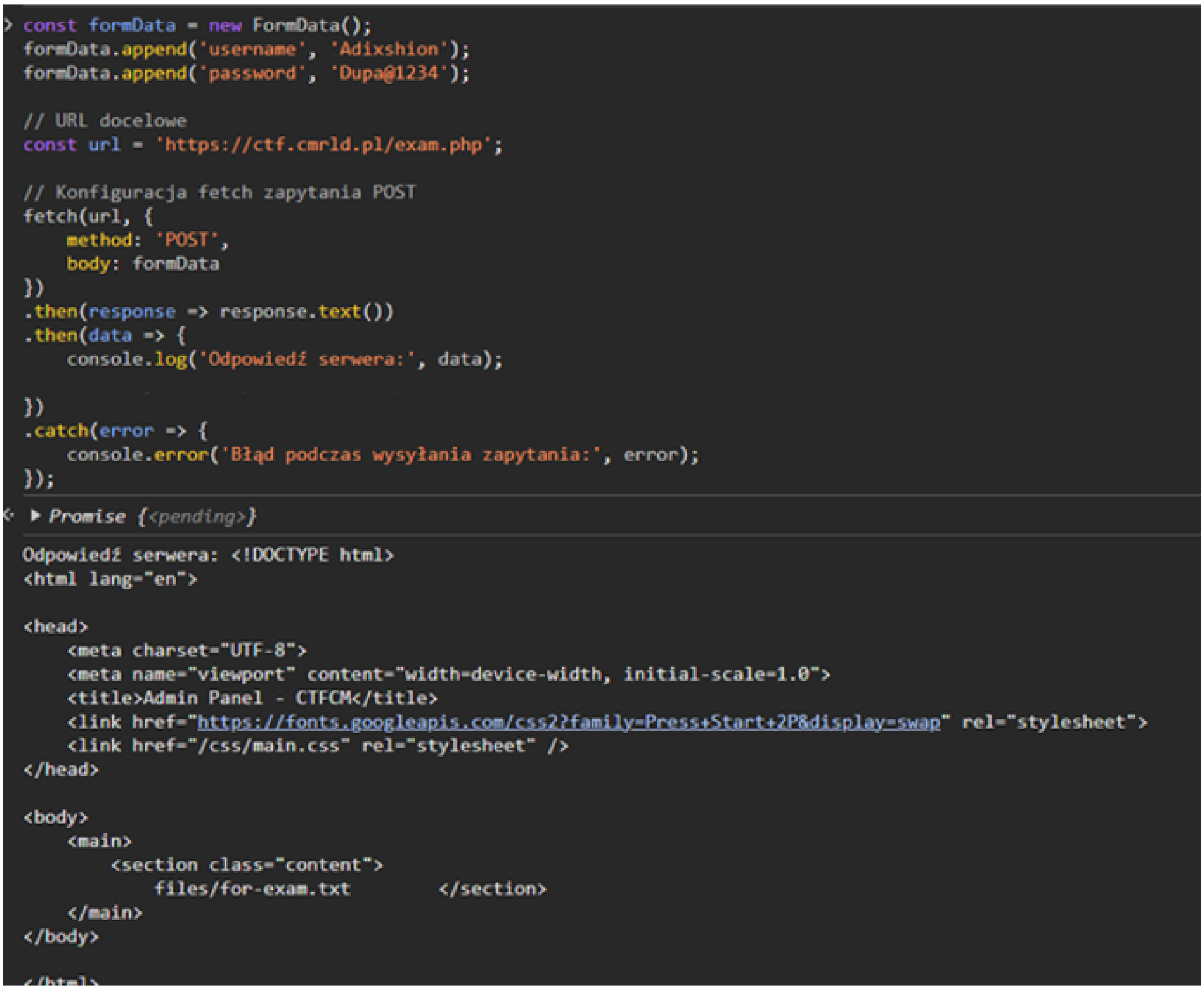
Our agents managed to intercept a digital communication suggesting that the final piece of the intergalactic puzzle lies behind a secure transmission. Your mission is to send the correct POST request to the /exam.php to retrieve the last part of the practice exam, which is rumored to contain the ultimate question of space and time. Can you craft the request and find the answer?

Wiedziałem, że aby uzyskać flagę, muszę odpowiednio użyć metody API – POST. Odwiedzenie strony https://ctf.cmrld.pl/exam.php zwracało komunikat: "Accepts

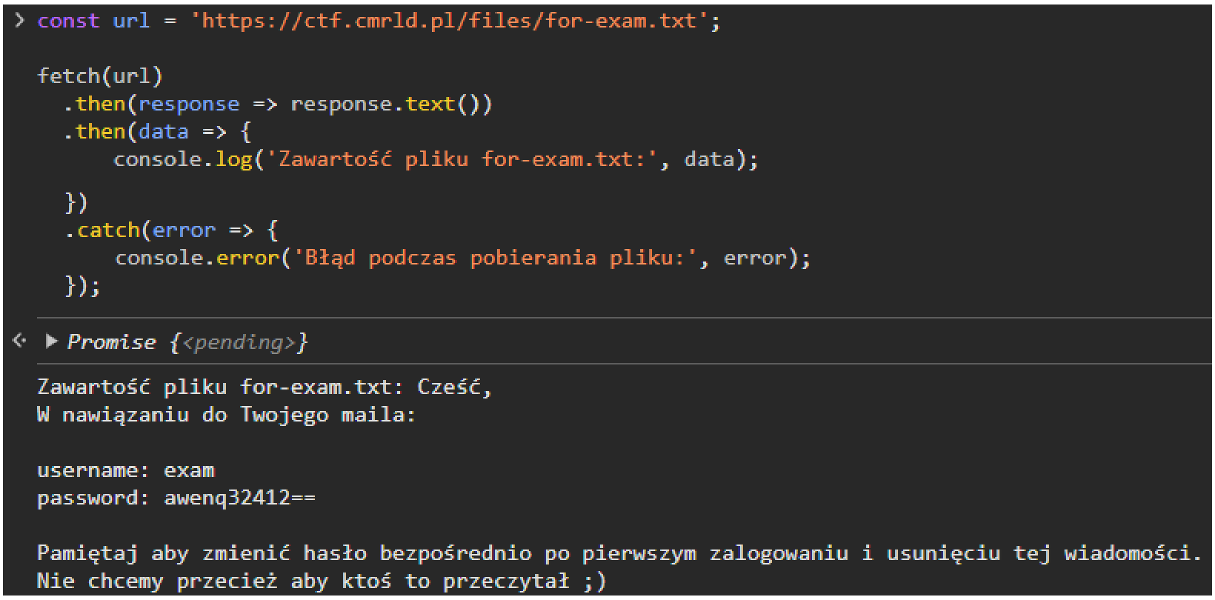
only POST Requests"
Po wysłaniu pierwszego zapytania odkryłem, że na stronie znajduje się ścieżka files/for-exam.txt.

(I knew that in order to get the flag, I had to properly use the API method - POST. Visiting https://ctf.cmrld.pl/exam.php returned the message: "Accepts only POST Requests".

After sending the first request, I discovered that the page contained the path files/for-exam.txt.)



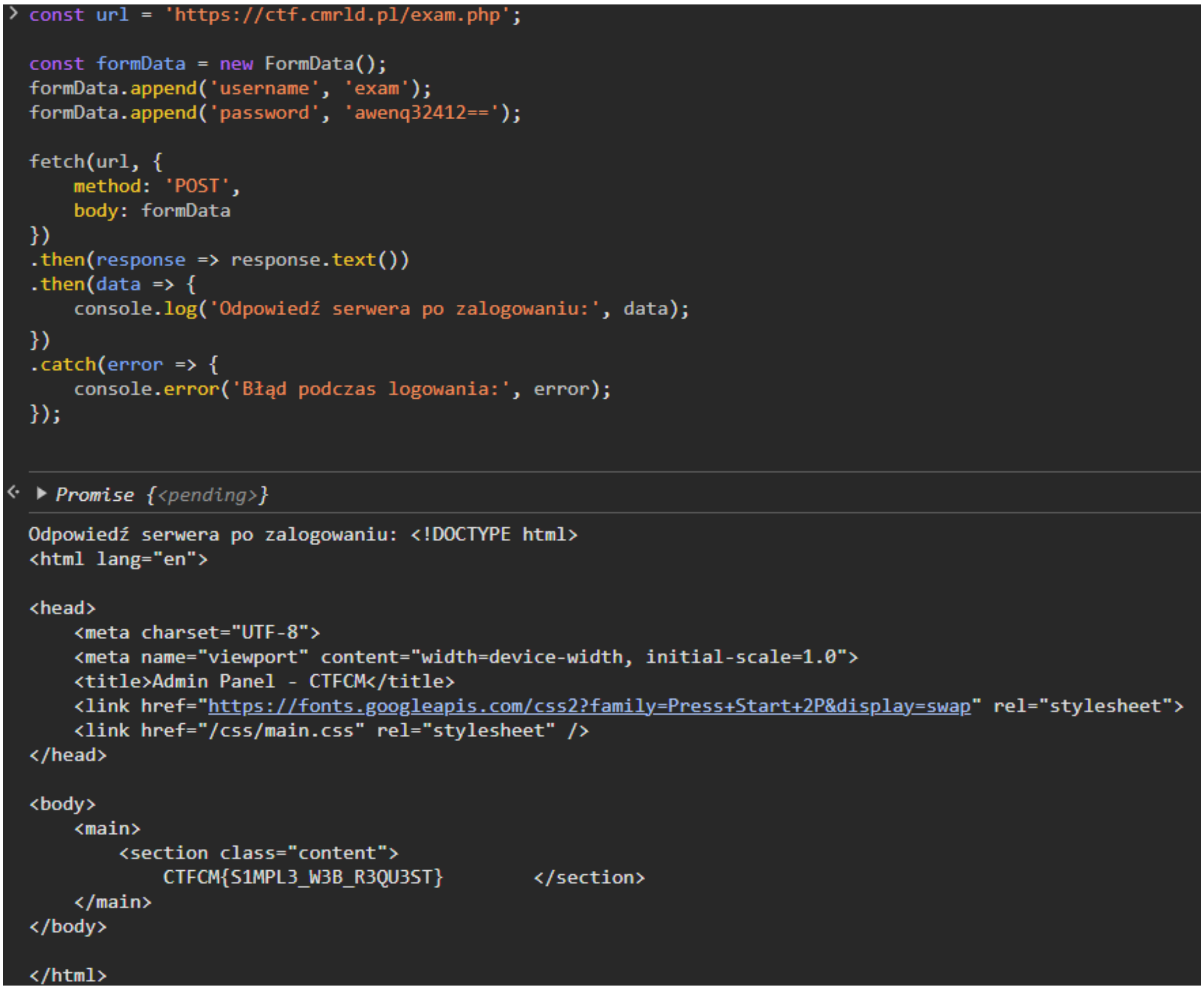
```
> const formData = new FormData();
  formData.append('username', 'Adixshion');
  formData.append('password', 'Dupa@1234');

  // URL docelowe
  const url = 'https://ctf.cmrld.pl/exam.php';

  // Konfiguracja fetch zapytania POST
  fetch(url, {
      method: 'POST',
      body: formData
  })
  .then(response => response.text())
  .then(data => {
      console.log('Odpowiedź serwera:', data);

  })
  .catch(error => {
      console.error('Błąd podczas wysyłania zapytania:', error);
  });
<· ▶ Promise {<pending>}
  Odpowiedź serwera: <!DOCTYPE html>
  <html lang="en">

  <head>
      <meta charset="UTF-8">
      <meta name="viewport" content="width=device-width, initial-scale=1.0">
      <title>Admin Panel - CTFCM</title>
      <link href="https://fonts.googleapis.com/css2?family=Press+Start+2P&display=swap" rel="stylesheet">
      <link href="/css/main.css" rel="stylesheet" />
  </head>

  <body>
      <main>
          <section class="content">
              files/for-exam.txt        </section>
      </main>
  </body>

  </html>
```



```
> const url = 'https://ctf.cmrld.pl/files/for-exam.txt';

  fetch(url)
    .then(response => response.text())
    .then(data => {
        console.log('Zawartość pliku for-exam.txt:', data);
    })
    .catch(error => {
        console.error('Błąd podczas pobierania pliku:', error);
    });

<· ▶ Promise {<pending>}

  Zawartość pliku for-exam.txt: Cześć,
  W nawiązaniu do Twojego maila:

  username: exam
  password: awenq32412==

  Pamiętaj aby zmienić hasło bezpośrednio po pierwszym zalogowaniu i usunięciu tej wiadomości.
  Nie chcemy przecież aby ktoś to przeczytał ;)
```

Po jej sprawdzeniu uzyskałem dane do logowania, które wykorzystałem na wcześniej otrzymanej podstronie - https://ctf.cmrld.pl/exam.php

(After checking it, I obtained login credentials, which I used on the previously obtained sub-site - https://ctf.cmrld.pl/exam.php)

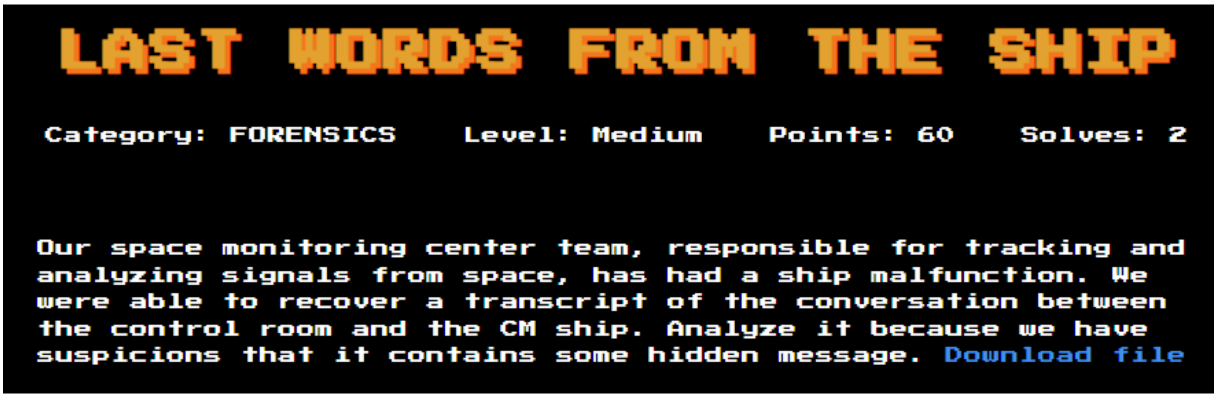


```
> const url = 'https://ctf.cmrld.pl/exam.php';

  const formData = new FormData();
  formData.append('username', 'exam');
  formData.append('password', 'awenq32412==');

  fetch(url, {
      method: 'POST',
      body: formData
  })
  .then(response => response.text())
  .then(data => {
      console.log('Odpowiedź serwera po zalogowaniu:', data);
  })
  .catch(error => {
      console.error('Błąd podczas logowania:', error);
  });

<· ▶ Promise {<pending>}
  Odpowiedź serwera po zalogowaniu: <!DOCTYPE html>
  <html lang="en">

  <head>
      <meta charset="UTF-8">
      <meta name="viewport" content="width=device-width, initial-scale=1.0">
      <title>Admin Panel - CTFCM</title>
      <link href="https://fonts.googleapis.com/css2?family=Press+Start+2P&display=swap" rel="stylesheet">
      <link href="/css/main.css" rel="stylesheet" />
  </head>

  <body>
      <main>
          <section class="content">
              CTFCM{S1MPL3_W3B_R3QU3ST}        </section>
      </main>
  </body>

  </html>
```

Dzięki tym danym udało się w sekcji <section class="content"> odnaleźć kolejną flagę

(With this data, it was possible to find another flag in the <section class="content"> section)

Zadanie 7 / Task 7



LAST WORDS FROM THE SHIP

Category: FORENSICS Level: Medium Points: 60 Solves: 2

Our space monitoring center team, responsible for tracking and analyzing signals from space, has had a ship malfunction. We were able to recover a transcript of the conversation between the control room and the CM ship. Analyze it because we have suspicions that it contains some hidden message. Download file

W tym zadaniu do pobrania jest plik „last_words.wav”

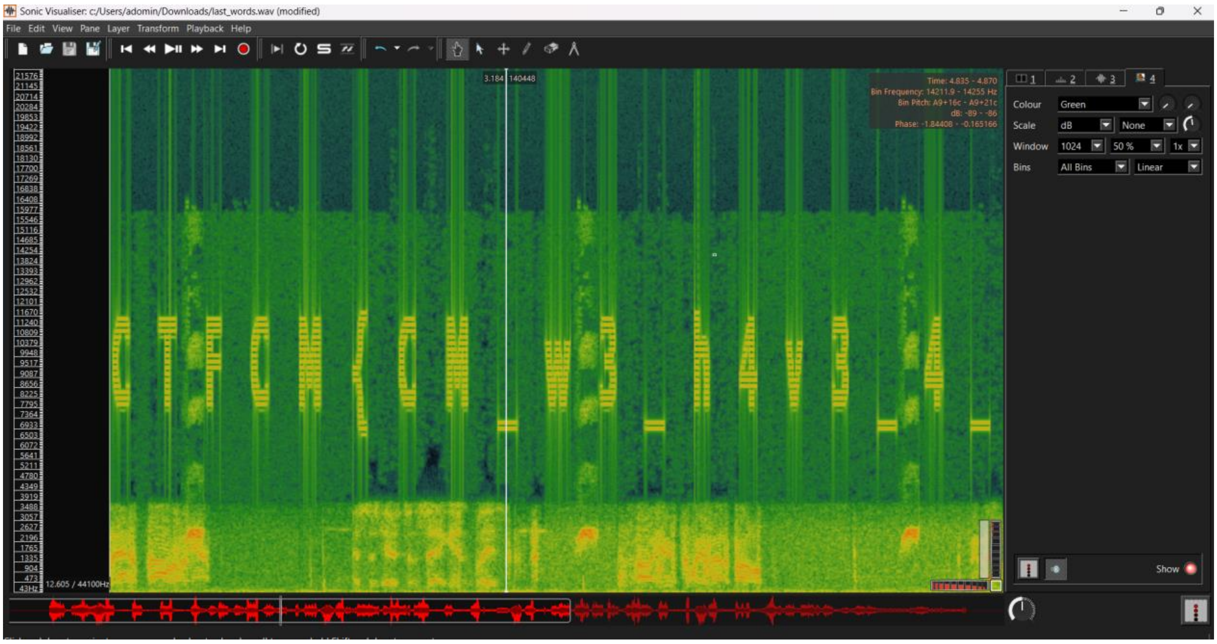
Samo przesłuchanie zbyt dużo nie daje bo jedynie słychać tylko dźwięk papugi oraz „Houston mamy problem”.

W tym zadaniu do rozwiązania wykorzystałem program Sonic Visualizer, w którym po dodaniu ścieżki dźwiękowej dodałem również spektogram dla wszystkich kanałów i to był strzał w 10, gdyż znaleziona została kolejna flaga – CTFCM{CM_w3_h4v3_4_pr08l3m}

(In this task to download is the file "last_words.wav"

Just listening to it doesn't do much because you can only hear the sound of the parrot and "Houston we have a problem."

In this task I used the Sonic Visualizer application to solve it, where after adding the soundtrack I also added a spectrogram for all channels and this was a shot in 10, because another flag was found - CTFCM{CM_w3_h4v3_4_pr08l3m})

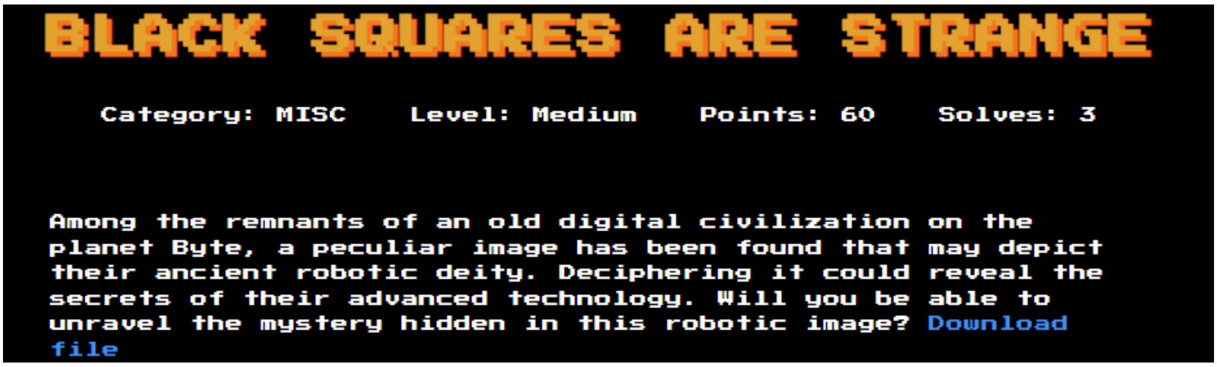


Sonic Visualiser: c:/Users/adomin/Downloads/last_words.wav (modified)

Time: 4.835 - 4.870
Bin Frequency: 14211.9 - 14255 Hz
Bin Pitch: A9+16c - A9+21c
dB: -89 - -86
Phase: -1.84408 - -0.165166

Colour: Green
Scale: dB, None
Window: 1024, 50 %, 1x
Bins: All Bins, Linear

Zadanie 8 / Task 8

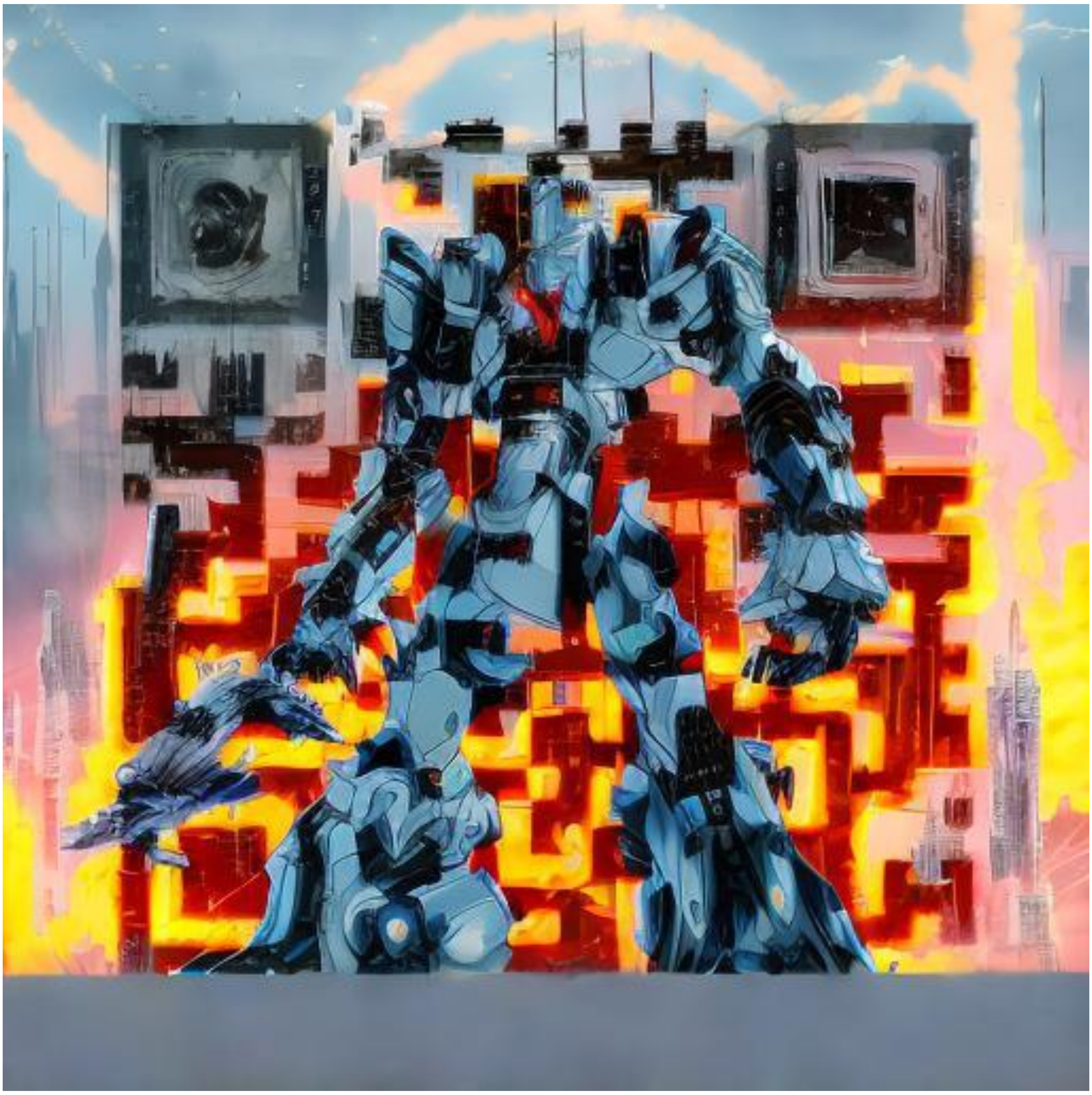


BLACK SQUARES ARE STRANGE

Category: MISC Level: Medium Points: 60 Solves: 3

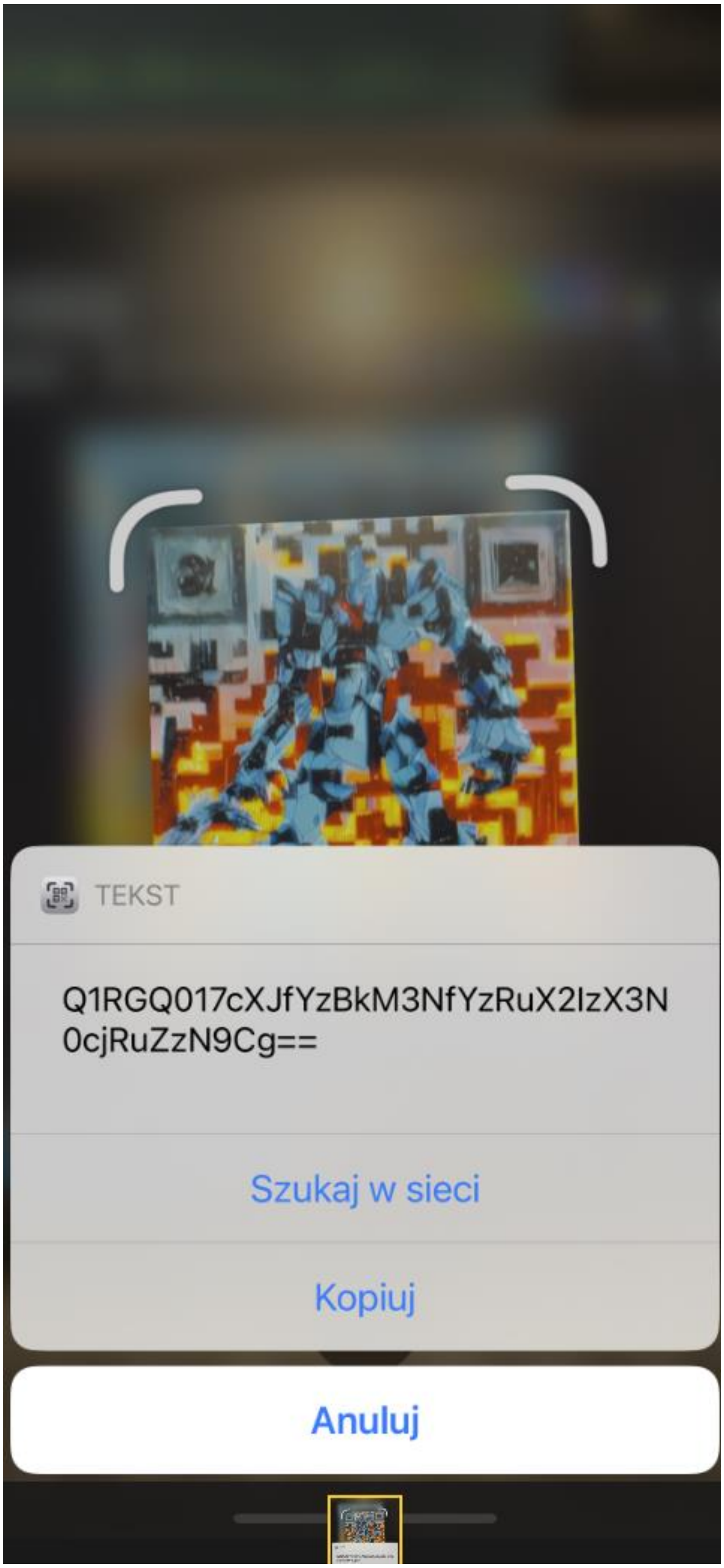
Among the remnants of an old digital civilization on the planet Byte, a peculiar image has been found that may depict their ancient robotic deity. Deciphering it could reveal the secrets of their advanced technology. Will you be able to unravel the mystery hidden in this robotic image? Download file

Obraz (An image):



Na pierwszą myśl przyszło mi do głowy aby zeskanować obrazek skanerem kodów QR, gdyż wygląda łudząco podobnie do takiego kodu. Po zeskanowaniu otrzymałem następujący wynik

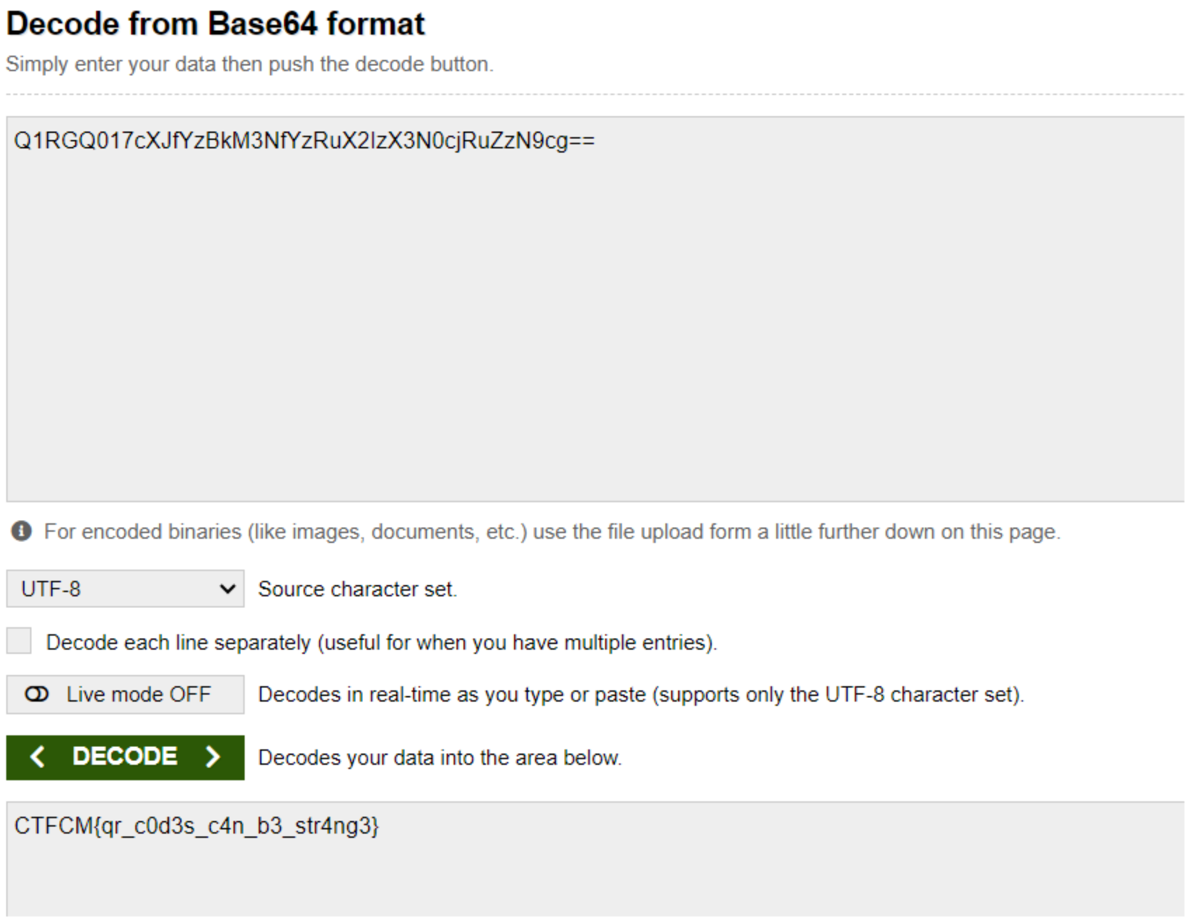
(My first thought was to scan the image with a QR code scanner, since it looks confusingly similar to such a code. After scanning, I received the following result):


TEKST

Q1RGQ017cXJfYzBkM3NfYzRuX2lzX3N
0cjRuZzN9Cg==

Wiadomość Q1RGQ017cXJfYzBkM3NfYzRuX2LzX3N0cjRuZzN9cg== po odszyfrowaniu za pomocą base64 dała kolejną flagę

(Message Q1RGQ017cXJfYzBkM3NfYzRuX2LzX3N0cjRuZzN9cg== after decryption with base64 gave another flag)



Decode from Base64 format

Simply enter your data then push the decode button.

```
Q1RGQ017cXJfYzBkM3NfYzRuX2IzX3N0cjRuZzN9cg==
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

Decodes your data into the area below.

```
CTFCM{qr_c0d3s_c4n_b3_str4ng3}
```