

CTF Report

Full Name:Ilyas Bajji

Program: HCS - Penetration Testing 1-Month Internship

Date:20/02/2024

Category: Cryptography

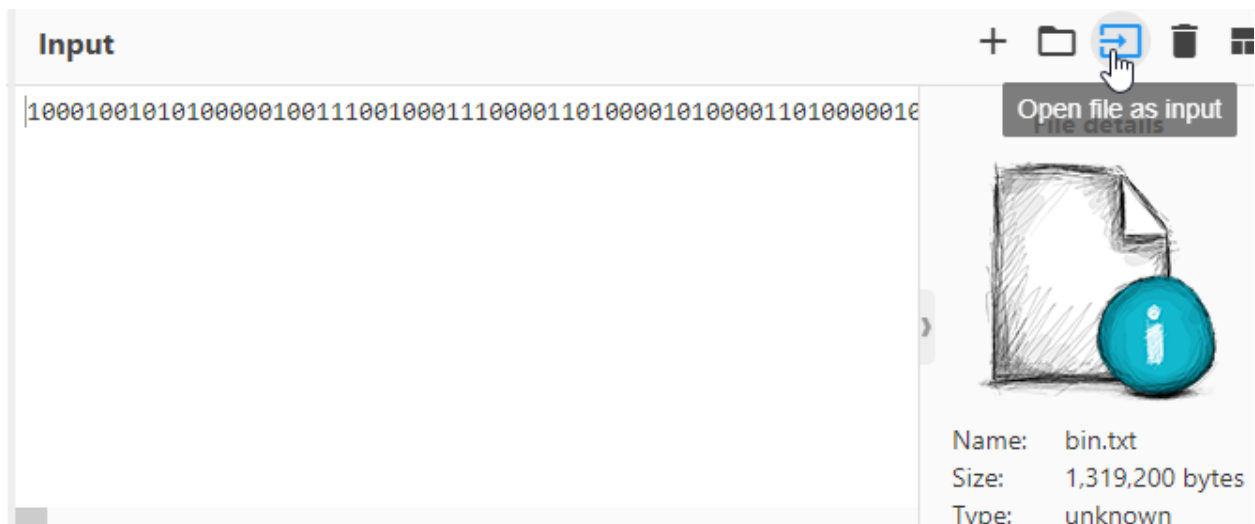
Description:

Cryptography challenges turn the learning process into a secret code-breaking adventure. Participants decipher hidden messages, honing the basics of cryptography, and understanding how to safeguard information from prying eyes.

Challenge Overview: Cipher quest : decipher a binary file to a picture

Steps for Finding the Flag:

1. Import file to cyberchef.com



2. In recipe add :

Recipe [Icons]

From Binary [Icons]

Delimiter: Space Byte Length: 8


Render Image [Icons]

Input format: Raw


Input [Icons]

10001001010100000100111001000111000011010000101000011010000010

File details

 Name: bin.txt
Size: 1,319,200 bytes
Type: unknown
Tr Raw Bytes [Icon]

REC 1319200 1



Baking input 1...

3. Download the image



4. Zoom in :

Flag: flag{crypt1c_1mp0st3r}

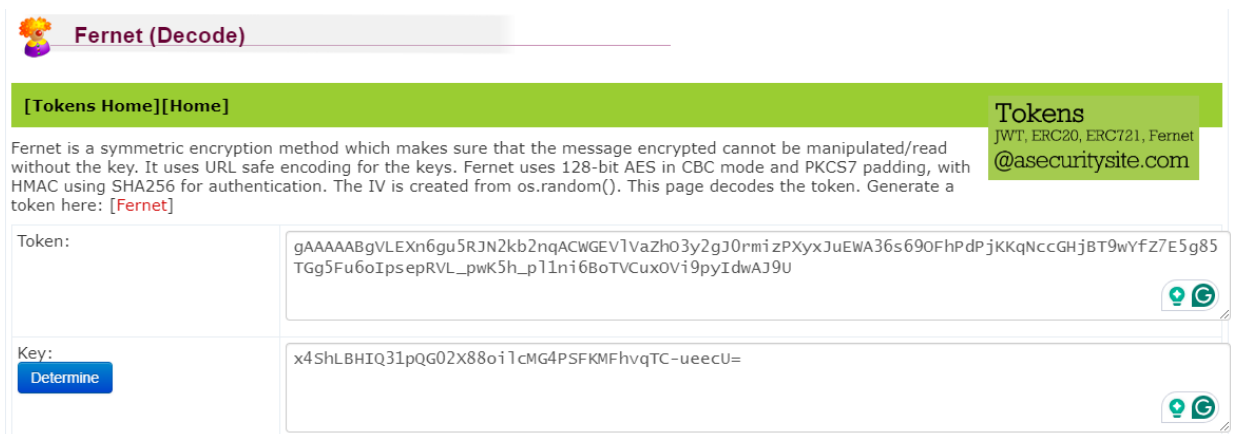
Category: Cryptography

Description:

Cryptography challenges turn the learning process into a secret code-breaking adventure. Participants decipher hidden messages, honing the basics of cryptography, and understanding how to safeguard information from prying eyes.

Challenge Overview: Feather dust :Decode it to get the flag! This encryption use URL safe encoding, AES with CBC. Enough Info right?

1. Went to the website : <https://asecuritysite.com/tokens/ferdecode>
2. Enter the value :



The screenshot shows the 'Fernet (Decode)' tool interface. At the top, there's a navigation bar with '[Tokens Home][Home]' and a 'Tokens' dropdown menu showing 'JWT, ERC20, ERC721, Fernet @asecuritysite.com'. Below this, a text box explains Fernet: 'Fernet is a symmetric encryption method which makes sure that the message encrypted cannot be manipulated/read without the key. It uses URL safe encoding for the keys. Fernet uses 128-bit AES in CBC mode and PKCS7 padding, with HMAC using SHA256 for authentication. The IV is created from os.random(). This page decodes the token. Generate a token here: [Fernet]'. The main form has two sections: 'Token:' with a text input containing a long URL-safe encoded string, and 'Key:' with a text input containing a 32-character hex key and a 'Determine' button. Both input fields have a copy icon on the right.

3. Get the flag :

```
Decoded:      flag{f3rn3t_3ncrypt1on_@r3_s1m1lar_t0_b@s3}
Date created:  Fri Mar 19 14:11:35 2021
Current time:  Fri Mar 15 17:55:44 2024
```

Flag: flag{f3rn3t_3ncrypt1on_@r3_s1m1lar_t0_b@s3}

Category: Cryptography

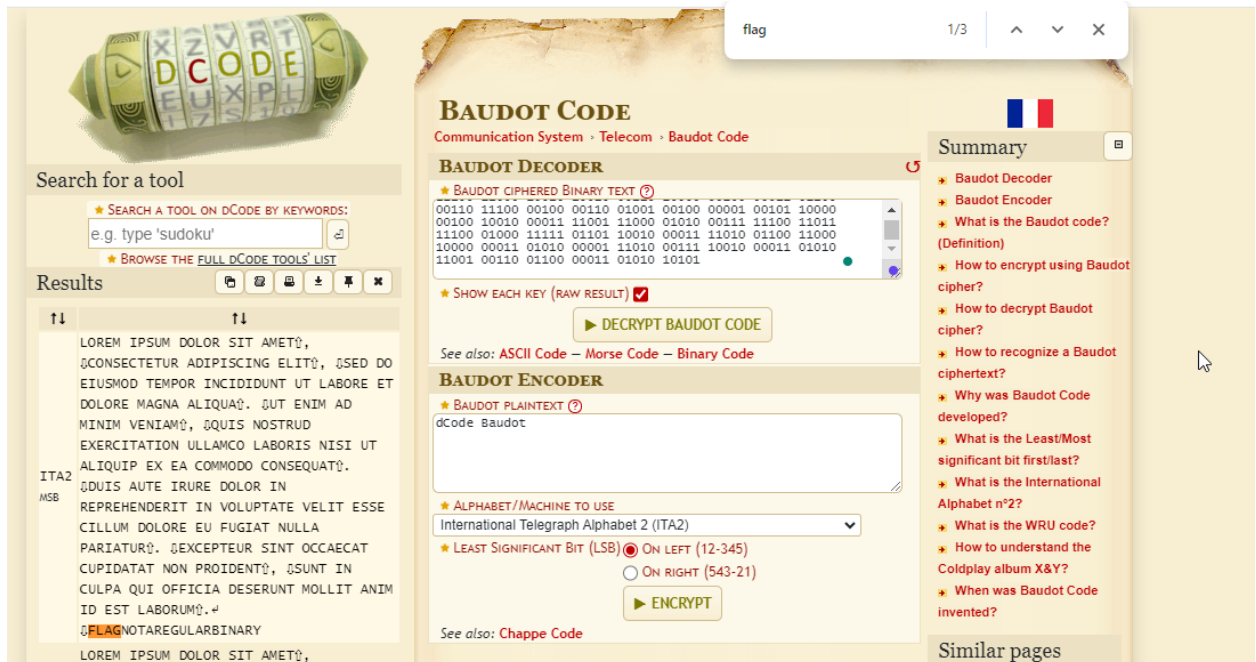
Description:

Cryptography challenges turn the learning process into a secret code-breaking adventure. Participants decipher hidden messages, honing the basics of cryptography, and understanding how to safeguard information from prying eyes.

Challenge Overview: RulerOfTheWorld Mr. Bob sent us this file and asked us to retrieve the secret, he also mentioned that follow these electrical impulses,

Steps for Finding the Flag:

1. Went to : <https://www.dcode.fr/baudot-code>
2. Decode it :



3. Find a flag

Flag: flag{NOTAREGULARBINARY}

Category: Network Forensic

Description: Forensics challenges transform participants into digital detectives, analyzing clues to uncover hidden information. This skill is vital in cybersecurity, responding to incidents, and becoming guardians of the digital realm.

Challenge Overview: shadow web : A brief description of the challenge (in 2 sentences)

Steps for Finding the Flag:

1. Open the pcap file
2. Follow tcp stream and found :

```
POST / HTTP/1.1
Host: 192.168.1.1:80
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary
m
-----WebKitFormBoundary
```

3. Each time letter show up
4. Resemble the letters from each stream
5. Found based 64 encode flag
6. Decode it

Flag: flag{mult1pl3p4rtsc0nfus3s}

Category: Network Forensic

Description Forensics challenges transform participants into digital detectives, analyzing clues to uncover hidden information. This skill is vital in cybersecurity, responding to incidents, and becoming guardians of the digital realm.

Challenge Overview Mystic connections : shARP analysis? shARPen your analysis skill to unhide the hidden secret. Fact: Data is everywhere to be found

Steps for Finding the Flag:

1. If you check every ARP packet, there is certain character placed in the data
2. And, there is Time for every packet.
3. And, there is Time for every packet.

Normal Order:

-0.005770 -0.004130 -0.009211 -0.002814 -0.009877 -0.003463 -0.005128 -0.006726 -
0.008487 -0.007051 -0.010344 -0.006099 -0.004448 -0.004770 -0.005445 -0.007450 -
0.002497 -0.006418 -0.007825 -0.009540 -0.008789 -0.008158

Descending Order —>

-0.002497 -0.002814 -0.003463 -0.004130 -0.004448 -0.004770 -0.005128 -0.005445 -
0.005770 -0.006099 -0.006418 -0.006726 -0.007051 -0.007450 -0.007825 -0.008158 -
0.008487 -0.008789 -0.009211 -0.009540 -0.009877 -0.010344

4. We associate each letter in respect to time

```
-0.002497 - }  
-0.002814 - 3  
-0.003463 - l  
-0.004130 - p  
-0.004448 - m  
-0.004770 - 1  
-0.005128 - s  
-0.005445 - _  
-0.005770 - g  
-0.006099 - n  
-0.006418 - 1  
-0.006726 - 3  
-0.007051 - b  
-0.007450 - _  
-0.007825 - P  
-0.008158 - R  
-0.008487 - A  
-0.008789 - {  
-0.009211 - g  
-0.009540 - a  
-0.009877 - l  
-0.010344 - f
```

5. We get :

Flag: flag{ARP_b31ng_s1mpl3}

Category: Phishing – Phish Guard

Description

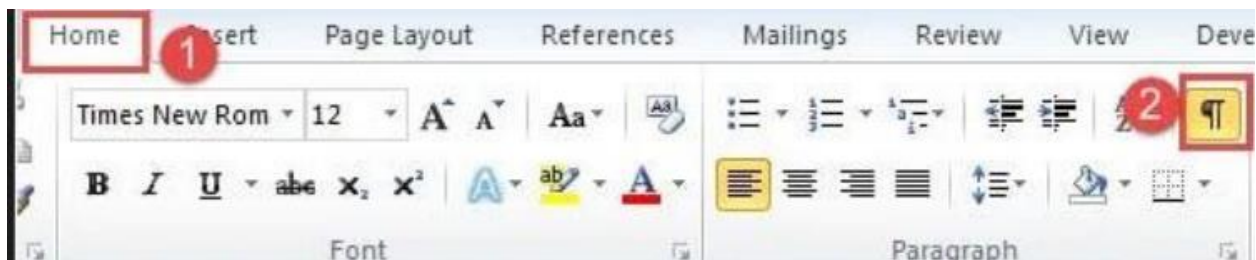
Aren't spam emails just the worst? I could miss something important!! Like this one email from Amazon. I don't recall making a payment for a Samsung TV but this looks like it could've been me.

Challenge Overview:

We are provided a document that is three pages long. If we select all the content on the pages, we can see that there is text hidden within the document

Steps for Finding the Flag:

We're given a document that is 3 pages long with hidden text. Using the ribbon, we can select Home -> Paragraph -> Show/Hide.



We're now able to see the hidden text.

From: security-alert@amazon.in

To: user@gmail.com

Subject: Payment-Rejected



Order Confirmation

#982-324975-354149

Dear Customer,

The Samsung 138 cm (55 inches) Crystal Smart 4K Ultra HD Smart LED TV UA55CUE60AKLXL (Black) you ordered is unable to be dispatched because we couldn't charge the full ₹67,599 to your card.

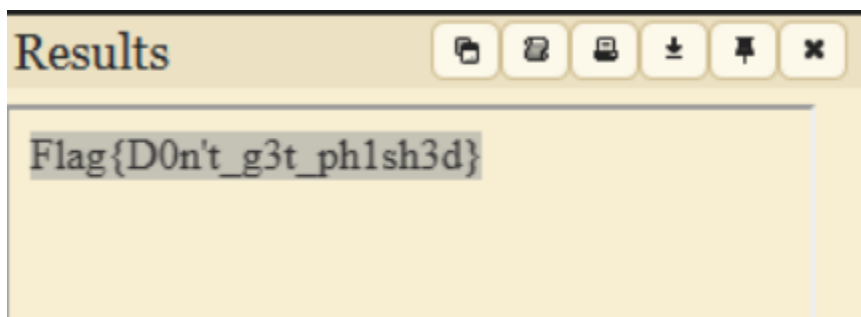
Because this is a high-value item, we always double-check the identity of the customer when a card payment is rejected. To confirm that this order was made by you or to raise a concern, please visit:

<https://amazon.in/security/verify>

If you need further assistance or to Cancel your order, Call us Customer Service +91 2032906778

```
... → ... → →
    →
..... → → . → →
    →
..... → → .... →
    →
..... → → .. → → →
    →
..... → → → → . → →
    →
..... → → →
    →
```

We can decode the whitespace language using a decoder.



Flag: Flag{D0n't_g3t_ph1sh3d}

Category: OSINT – Social Hunt

Description:

One of my tech-savvy friends constantly claims that using Linux these days is akin to trying to light a fire with stones. We often tease him by saying, 'One day, you'll be the one known as the LinuxKiller and go by the online persona of 'LinuxKiller69'. Despite not being a frequent social media user, he occasionally checks his account, where the platform's mascot is 'Snoo'. We're curious to know where else he has created accounts and what tech-related thoughts he's sharing there.

Challenge Overview:

Given a username LinuxKiller69. We have to perform some research on various social media platforms, leading us to find a flag in their profile picture.

Steps for Finding the Flag:

We're given a user account LinuxKiller69. Perform a search on Instagram and we find a profile for them.



In the bottom left-hand corner of the image we can make out what looks like the flag.

To get the profile picture we can use a tool such as instaloader and view the full flag.

<https://github.com/instaloader/instaloader>



Flag: flag{cr0ss_pl\$tf0rm}