APTIKOM
Nusantara Cyber Security 2025

WRITE UP

Sabtu, 20 September 2025

Nama Perguruan Tinggi : UPN "Veteran" Yogyakarta
Nama Tim : Soft Spoken
Ketua Tim : Muhammad Luqmaan
Anggota : 1. Muhamad Akbar Riziq
2. Muhammad Adel Harits
E-mail Tim : Muhammad Luqmaan (mluqmaan22@gmail.com)
Muhamad Akbar Riziq (akbarriziq348@gmail.com)
Muhammad Adel Harits (adel.harits18@gmail.com)

Daftar isi

[Easy]

[Medium]

1. **Soal No 1 (Seorang tokoh nasional meninggalkan pesan yang disandikan)**

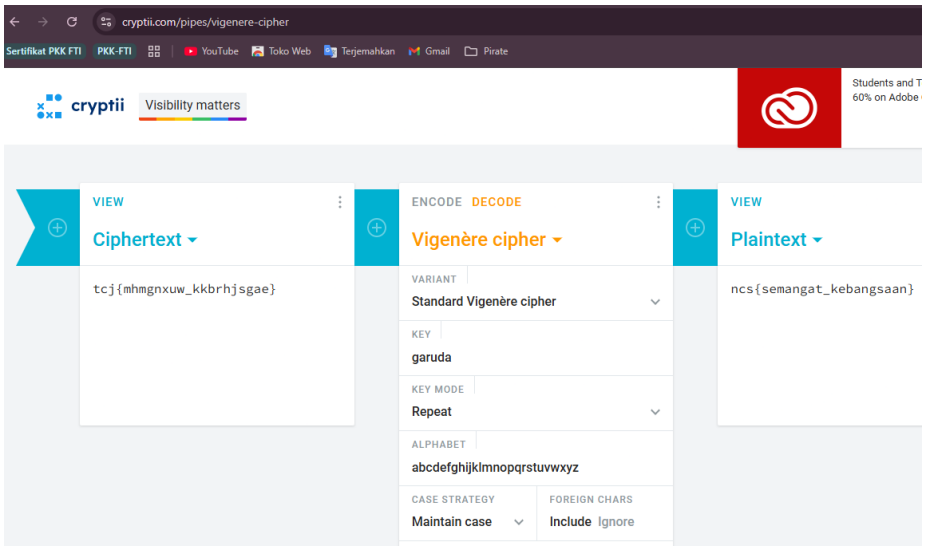
   Flag :
   ncs(semangat_kebangsaan}

   Deskripsi :
   Seorang tokoh nasional meninggalkan pesan yang disandikan menggunakan metode Vigenère Cipher. Berikut adalah pesan yang ditemukan:

   tcj{mhmgnxuw_kkbrhjsgae}

   Kunci yang digunakan untuk mengenkripsi pesan adalah: Lambang Negara

   Solusi :
   Pada soal sudah dijelaskan kalau algoritma yang digunakan adalah vigenere cipher dengan kunci lambang negara. Kita bisa menggunakan website https://cryptii.com/pipes/vigenere-cipher untuk memecahkan sandi tersebut dengan memasukkan ciphertext dari soal dan kunci garuda yang merupakan lambang negara indonesia.



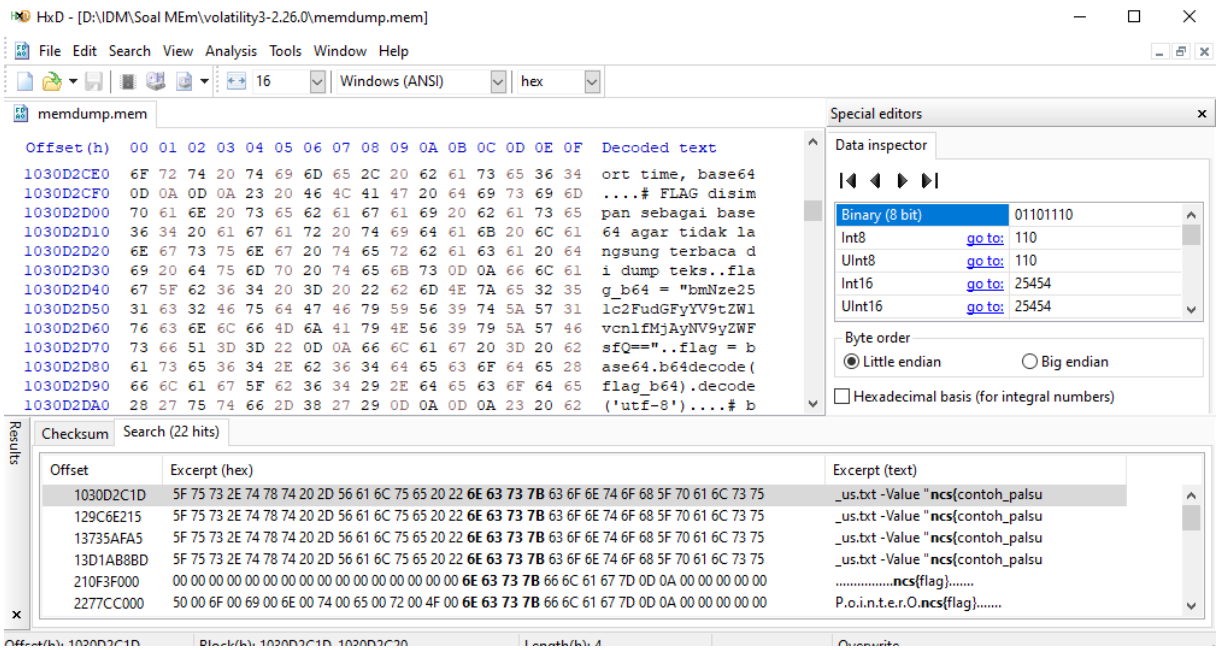
   Hasilnya flagnya muncul yaitu **ncs(semangat_kebangsaan}**

2. Soal No 2 (Looking for something)

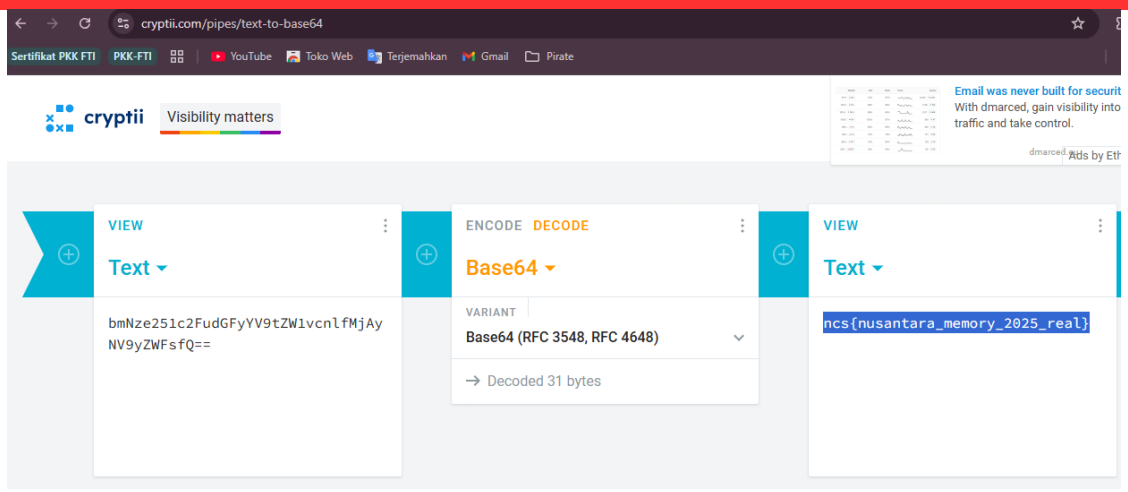
Flag:
ncs{nusantara_memory_2025_real}

Deskripsi :
Silahkan Download file berikut : https://drive.google.com/file/d/19tg1lHIdYFaj9f6jMMLpb4PFxpqQERNr/view?usp=sharing

Solusi:
Pada file 7z yang diberikan, bisa langsung di unzip dan akan mendapatkan file yaitu memdump.mem. Lalu gunakan hxd untuk melihat isi pada file tersebut. Karna penasaran, langsung search apakah ada string dengan format ncs{}, setelah dicari ternyata terdapat string dengan format ncs yang palsu untuk menipu.



Pada hxd tersebut terdapat tulisan jika flag disembunyikan menjadi base64 agar sulit untuk diketahui. Akhirnya menggunakan website https://cryptii.com/pipes/text-to-base64 untuk mendecrypt base64 tersebut menjadi string seperti biasa



Dan hasilnya flagnya terbaca yaitu **ncs{nusantara_memory_2025_real}**

3. **Soal No 3 (Jangan iseng baca chat teman)**
Flag:
ncs{SQL-oH_sql-1974}

Deskripsi:
Tanpa sengaja aku melihat backup database di laptop teman, aku iseng saja mencoba melihat apa isi didalamnya, aku penasaran dengan isi chat teman-teman ku, aku yakin disana ada info flag yang kubutuhkan.

Solusi:
Dari format file chat_backup.db saya langsung mencoba sqlite untuk mencoba melihat isi file tersebut, ada banyak message dengan format yang tampak terenkripsi. Beberapa terlihat jelas jika itu adalah format base64. Namun saat dekripsi dilakukan, ada yang tidak berhasil menjadi string jelas yang kemudian dilakukan dekripsi lagi, tetapi malah ada ncs{n0t-th1s_chAt} yang di mana itu bukanlah flagnya. Kita sangat kebingungan hingga akhirnya memutuskan untuk membuka hint dan mendapatkan hint 0x42. Saya terpikirkan jika itu merupakan operasi xor dengan kunci 0x42. Kemudian saya membuat script yang isinya untuk ‘setelah di-decode sekali dengan base64’.

Jawaban:

```python
import base64
import re

def extract_the_flag():
    fragments = [
        "me3JSrECt+rKpxcEWXVuo2FAjDr1NcXtDNqh5VwSVSf47ameaHvH47zmKVBnRKEphw==",
        "TtoDPEj54cMmiF1HO011OUmAcMOVU7Bk",
        "jHXaa9x2p1mrGhMrA2nJhIrFGE/Tu5p01CM9p+11rOTx",
        "ZbrjCSEDoajyBM45X1URJPcmuiO9OFvuWX6sOagLN7EOxqN9IpqJ5Wk=",
        "Uvo6noeBzccc492sEb/p8hjfSc2c8TbgGnxFKfPCYVRJjdxETCcf/Y0=",
        "PUDdiclejecRkd94M8cvHp8nsLW569O2im7cbZ1h7f8MLbqT",
        "aGhoLCExORETDm8tCh0xMy5vc3t1dj9oaGg=",
        "+lIPmi6mOreftNpyTSJHVyqVbeKHjfCwM5ZSPNTV7/0yu5IATygHKEtn4CJH9/bxGuD+AAE3NDG6fg=="
    ]

    ciphertext = b""
    for i, frag in enumerate(fragments):
        try:
            missing_padding = len(frag) % 4
            if missing_padding:
                frag += '=' * (4 - missing_padding)
            ciphertext += base64.b64decode(frag)
        except Exception as e:
            print(f"Error saat men-decode fragmen #{i+1}: {e}")
            return

    print(f"[*] Total panjang ciphertext setelah digabung: {len(ciphertext)} bytes")

    xor_key = 0x42

    decrypted_data = bytearray()
    for byte in ciphertext:
        decrypted_data.append(byte ^ xor_key)

    flag_pattern = rb"ncs\{.*?\}"

    match = re.search(flag_pattern, decrypted_data)

    if match:
        found_flag = match.group(0).decode('utf-8')
        print("\n[+] Flag berhasil ditemukan dan diekstrak!")
        print(f"    {found_flag}")
    else:
        print("\n[-] Flag tidak ditemukan di dalam data hasil dekripsi.")
        print("    Mungkin ada kesalahan pada daftar fragmen atau kunci.")

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

Saat kode tersebut dijalankan, akan menghasilkan hal berikut dan menemukan flagnya:

```
PS D:\kuliah> python solve.py
[*] Total panjang ciphertext setelah digabung: 308 bytes
[*] Total panjang ciphertext setelah digabung: 308 bytes

[+] Flag berhasil ditemukan dan diekstrak!
    ncs{SQL-oH_sql-1974}
```

4. **Soal No 4 (Pesan dari Pejuang)**
Flag:
ncs{this_is_a_message}

Deskripsi:
Seorang pejuang kemerdekaan meninggalkan pesan rahasia yang disandikan menggunakan metode klasik. Pesan tersebut ditemukan dalam bentuk berikut**:**

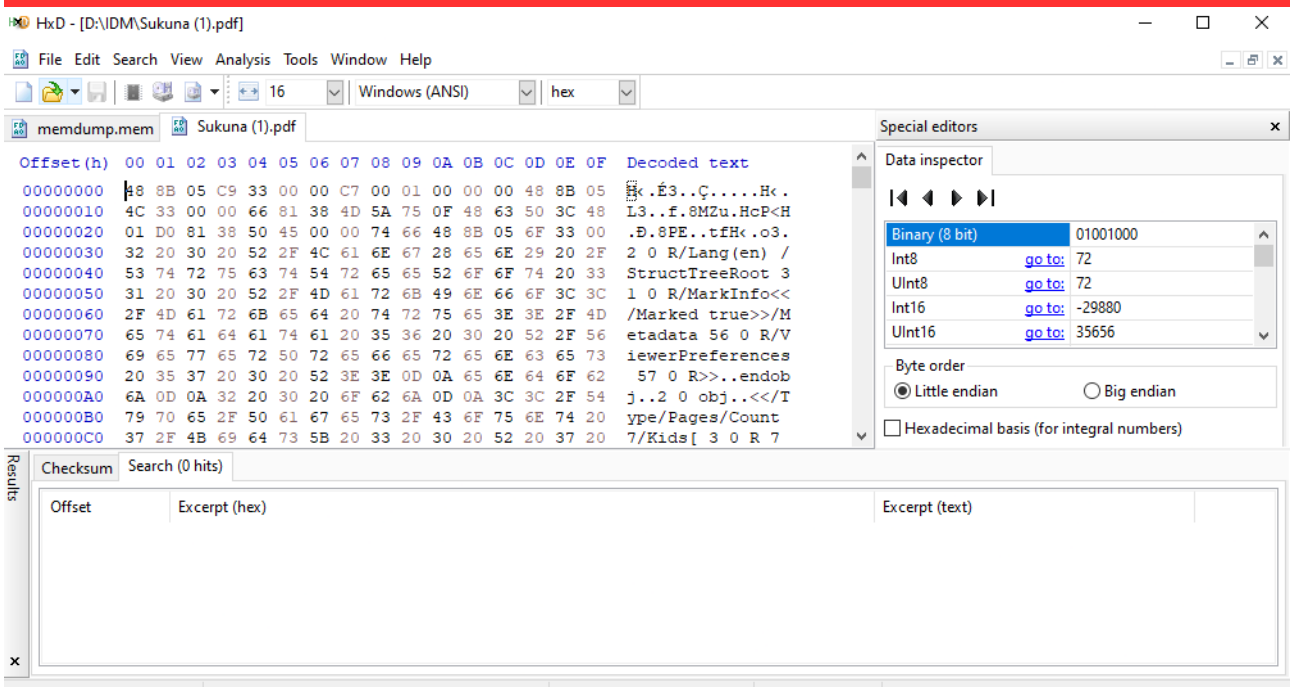
Wklv phvvdjh lv hqfubswhg: QFV{wklv_lv_d_phvvdjh}

Solusi:
Metode klasik yang langsung terpikirkan di awal merupakan caesar cipher karena kami sedang menjalani mata kuliah kriptografi juga di kampus, dengan format yang disampaikan adalah ncs{}, maka menyelesaikan bagian QFV terlebih dahulu dan mendapatkan bahwa kuncinya adalah pergeseran 3 huruf dan langsung melakukan decode hingga menemukan NCS{this_is_a_message} (yang ternyata ncs dan bukan NCS).

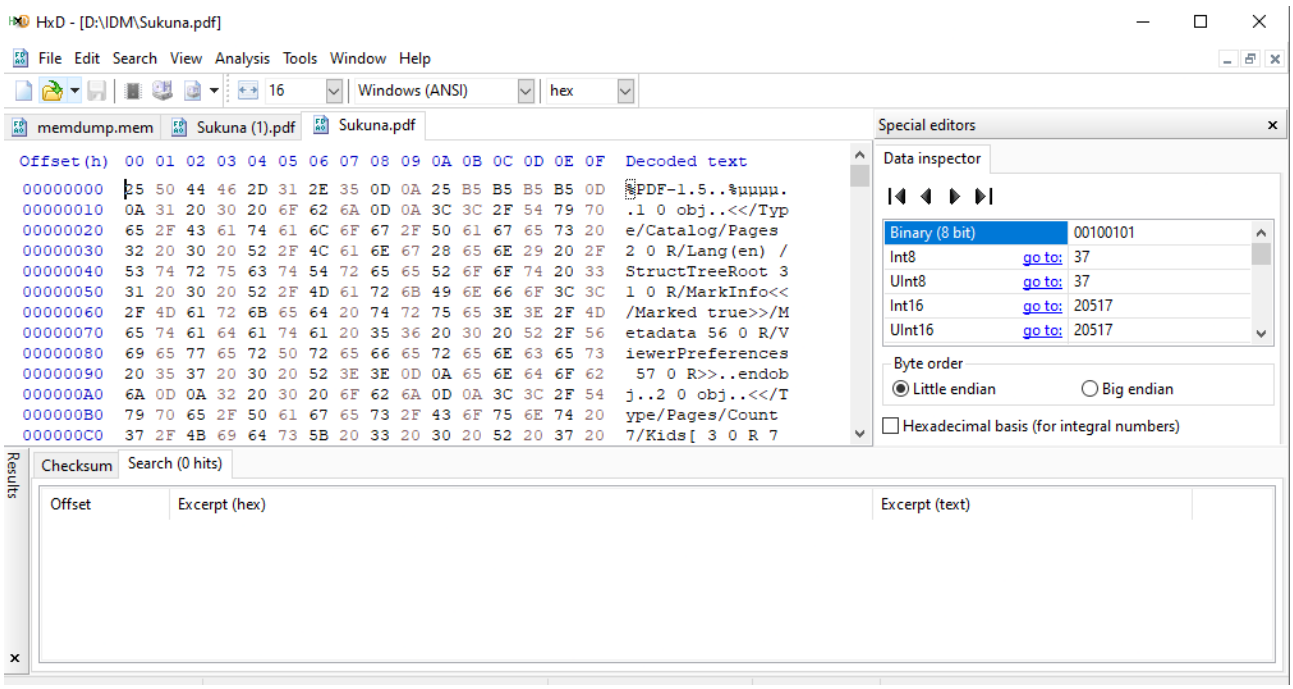
5. Soal No 5 (Everything has changed)

Flag:
ncs{Pdf5_C4N_8E_P4Rt14Lly_rECOveREd_1f_they_4rE_D4m49Ed_Or_enCRYpTEd}

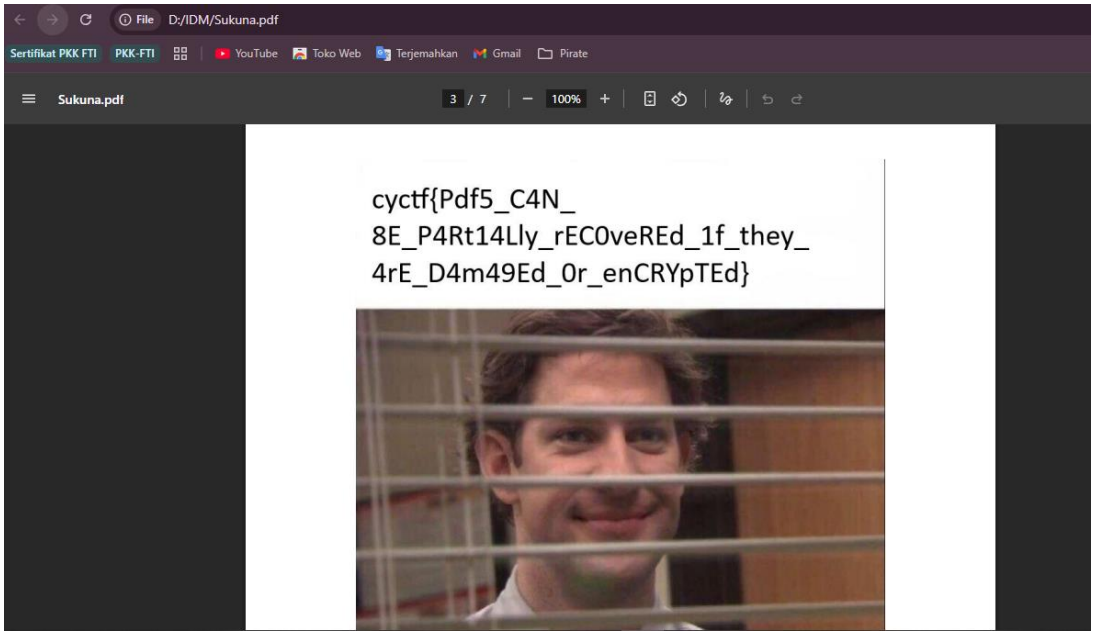
Solusi:
Diberikan sebuah file pdf yang rusak dan tidak bisa dibuka, kami curiga jika permasalahannya ada di file signaturenya. Menggunakan software hxd kami langsung mengecek header dari pdf tersebut. Ternyata benar saja bahwa headernya kurang untuk file signature pdf



Terlihat disini bahwa pada header yang seharusnya terdapat file signature pdf malah kosong. Akhirnya kami mengcopy header dari pdf yang normal ke dalam pdf sukuna tersebut yang bermasalah



Setelah kami tambahkan akhirnya file pdf bisa terbuka dan menampilkan 7 halaman, dan flag ditemukan pada halaman 3



Flag butuh disesuaikan sehingga hasilnya ncs{Pdf5_C4N_8E_P4Rt14Lly_rECOveREd_1f_they_4rE_D4m49Ed_Or_enCRYpTEd}