# Zadanie 1.

W tym zadaniu musisz wykorzystać techniki OSINT (Open Source Intelligence), aby zlokalizować ukryte flagi. Twoje umiejętności wyszukiwania informacji zostaną poddane próbie, a zadanie to sprawdzi Twoją zdolność do kreatywnego myślenia oraz efektywnego korzystania z dostępnych narzędzi.

Podkreślamy, że to zadanie obejmuje tylko OSINT pasywny. Kandydaci mogą korzystać wyłącznie z publicznie dostępnych źródeł danych i nie mogą angażować się w żadne aktywne próby uzyskania dostępu lub ingerencji w systemy czy sieci.

**Dane wejściowe:**

Marlena Daberek

**Format flagi:**

KPMG_RT{s0m3_str1ng}

# Zadanie 2.

Twoim zadaniem będzie zaprojektowanie kampanii socjotechnicznej typu phishing, skierowanej przeciwko danej firmie. Celem jest przetestowanie Twoich umiejętności w zakresie rozpoznawania słabych punktów w bezpieczeństwie informacji oraz tworzenia przekonujących fałszywych komunikatów.

Podkreślamy, że jest to zadanie czysto teoretyczne. Kandydaci mają przygotować poszczególne elementy kampanii tylko w wersji opisowej i nie mogą angażować się w żadne aktywne próby realizacji kampanii.

**Dane wejściowe:**

Domena: passeratti-leasingi.pl

Schemat adresów e-mail: imię.nazwisko@passi-leasi.pl

**Projektowanie kampanii socjotechnicznej**

1. **Wybór domeny:** Podaj domenę, z której będziesz przeprowadzał atak typu phishing. Domena ta powinna wydawać się wiarygodna dla pracowników firmy.
2. **Adresy e-mail:** Określ, na jakie adresy e-mail zostanie wysłana fałszywa wiadomość i uzasadnij dlaczego. Wybierz adresy tak, aby maksymalizować szanse na sukces kampanii.
3. **Ogólny pomysł na phishing:**
    - **Treść maila:** Opracuj przekonujący tekst e-maila, który skłoni odbiorców do podjęcia pożądanej akcji.
    - **Zawartość strony:** Opisz zawartość strony, do której prowadzi link w e-mailu.
    - **Cel phishingu:** Określ, co jest głównym celem kampanii (np. pozyskanie danych logowania, zainstalowanie złośliwego oprogramowania).