

# Thr34t\_4ct0r

Player: constantine

Kategori: OSINT

Challenge

7 Solves

Thr34t\_4ct0r

430

Medium-Hard

Pada tanggal 2 maret 2025, terdapat sebuah kebocoran data pada Menara Imperium Business Center yang menyebarkan 4.47GB data perusahaan, postingan tersebut di upload oleh user **LordVoldemort** pada darkweb "BreachForums". Tolong bantu tim intelijen kepolisian untuk mengungkap siapa dibalik akun tersebut.

Contoh flag : FORESTY{namapanjangpelaku}

author: sn0wden

Flag

Submit

---

## Phase 1: Recon

Dari deskripsi challenge, kita mendapatkan beberapa informasi kunci:

- **Username Target:** Lord Voldemort
- **Platform:** Darkweb "BreachForums"
- **Deskripsi Insiden:** Kebocoran data 4.47GB di Menara Imperium Business Center (2 Maret 2025).
- **Tujuan:** Mengungkap identitas asli di balik akun tersebut.

Berdasarkan petunjuk ini, strategi kita adalah fokus mencari informasi terkait username **Lord Voldemort** pada database yang berhubungan dengan BreachForums. Platform OSINT lookup yang paling relevan untuk ini adalah [bf.based.re](https://bf.based.re), yang mengindeks data dari forum tersebut.

---

## Phase 2: Query & Analysis

Kita langsung melakukan query ke database [bf.based.re](https://bf.based.re) menggunakan username target yang sudah kita identifikasi.

basic_info	
username	email
LordVoldemort	leonardoreynaldi@gmail.com

Hasil query sangat jelas dan langsung memberikan data yang kita butuhkan. Platform tersebut berhasil mencocokkan data *leaked* dengan username target:

- **username:** Lord Voldemort
- **email:** leonardoreynaldi@gmail.com

Dari temuan ini, identitas pelaku sudah sangat jelas: **leonardoreynaldi**.

---

## Phase 3: Build Flag

Setelah identitas pelaku didapatkan, kita kembali ke deskripsi challenge untuk melihat format flag yang diminta.

Format Flag:

```
FORESTY{namapanjangpelaku}
```

Kita hanya perlu memasukkan nama identitas yang kita temukan (**leonardoreynaldi**) ke dalam format tersebut.

---

## Flag Final

**FORESTY{leonardoreynaldi}**