[Misc] **Interpreter** (436 points)

By: Achideon

Soal Interpreter tidak memiliki file apapun, hanya disediakan sebuah *netcat* yang berisi flag yang dicari. Saat *netcat* dijalankan, keluar perintah seperti berikut:

```
┌──(achideon㉿ LAPTOP-NR5N5KT9)-[~]
└─$ nc 20.198.224.34 8037
The flag is stored in memory, and to get started you can print Hello, universe! twice with the following program:

    oioioioioioioioioioioioioddddddddddddddoioioioioioioioioioioioio

Valid instructions are: i d o
payload>
```

Jika input dimasukkan ke dalam payload, maka menunjukkan dua kali print “Hello, world!”

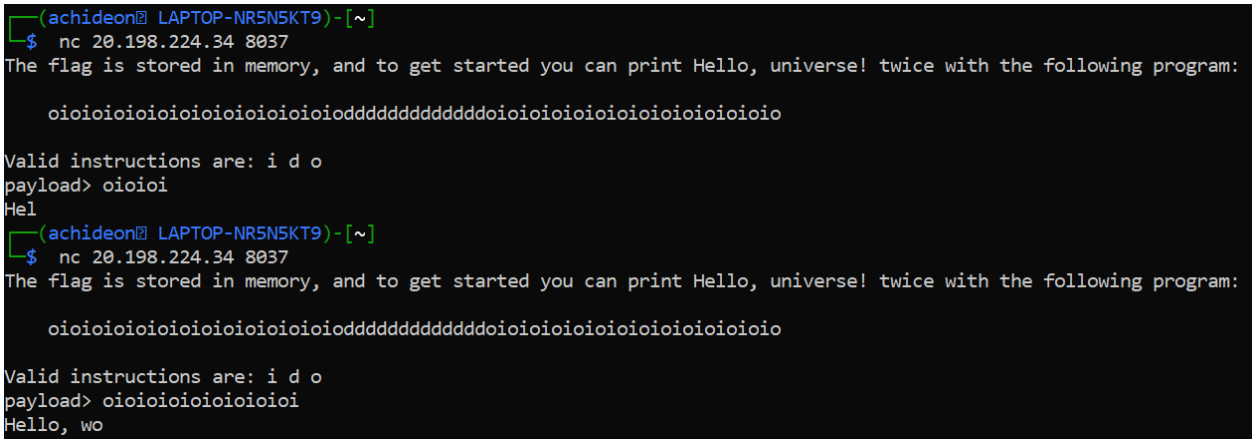
```
    oioioioioioioioioioioioioddddddddddddddoioioioioioioioioioioioio

Valid instructions are: i d o
payload> oioioioioioioioioioioioioddddddddddddddoioioioioioioioioioioioio
Hello, world!
Hello, world!
```

Namun apabila coba menginput karakter lain selain *i, d,* dan *o* maka program akan mengembalikan error message

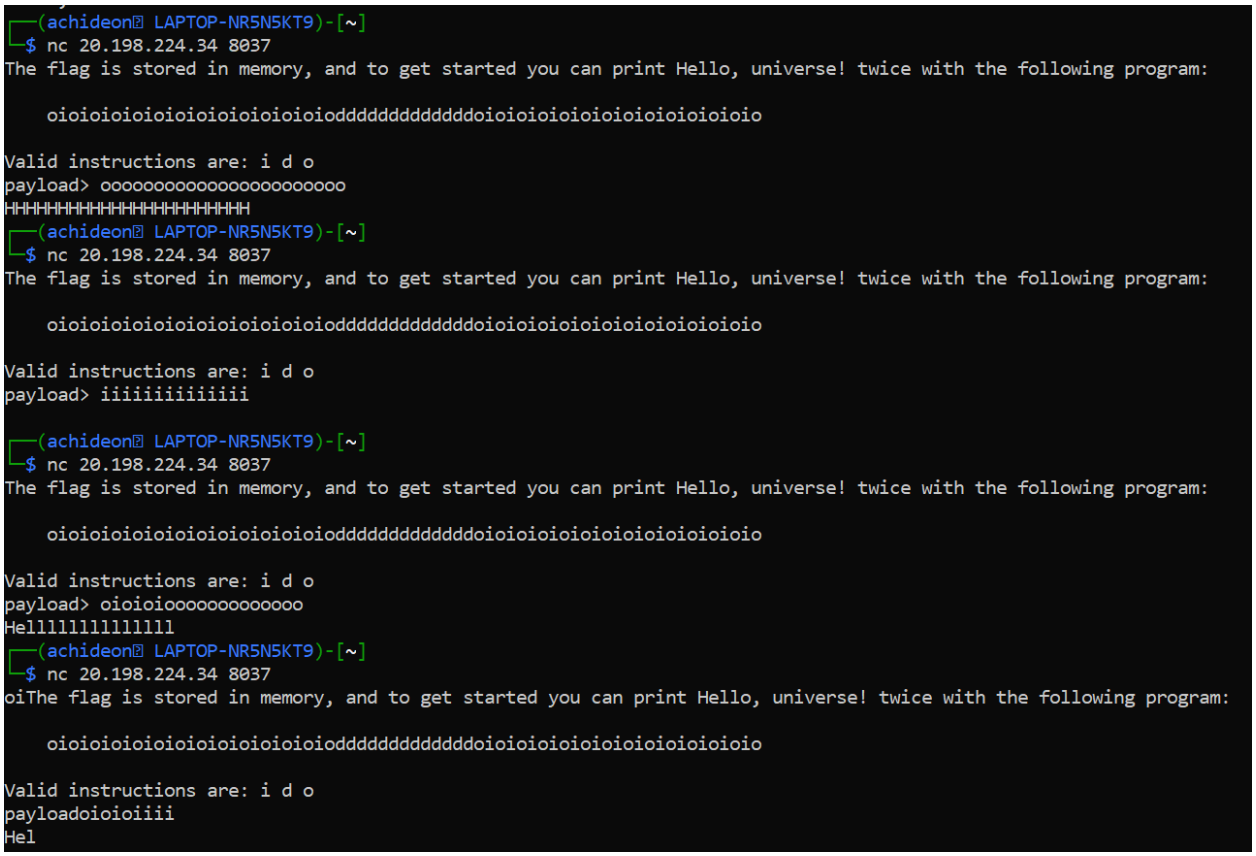
```
Valid instructions are: i d o
payload> test
You have used an invalid instruction. 't'
```

Hal ini menandakan bahwa input yang mau diterima program hanya boleh mengandung karakter *i d o*

Kemudian program dicoba dengan menggunakan string oioioi berulang, menghasilkan output seperti di bawah



Berarti string oioioi adalah string yang membentuk output, tapi bagaimana jika cuman o dan i? Bagaimana jika kombinasinya bukan hanya oi bergiliran?



Maka bisa disimpulkan jika karakter *o* membuat program menuliskan satu huruf, dan karakter *i* membuat program memilih huruf selanjutnya untuk ditulis. Bagaimana jika input berupa string oioioioioi yang sangat panjang?

```
┌──(achideon㉿ LAPTOP-NR5N5KT9)-[~]
└─$ nc 20.198.224.34 8037
The flag is stored in memory, and to get started you can print Hello, universe! twice with the following program:

    oioioioioioioioioioioioiodddddddddddddoioioioioioioioioioioioioio

Valid instructions are: i d o
payload> oioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioio
ioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioi
We cannot interpret programs that are this large!

┌──(achideon㉿ LAPTOP-NR5N5KT9)-[~]
└─$ nc 20.198.224.34 8037
The flag is stored in memory, and to get started you can print Hello, universe! twice with the following program:

    oioioioioioioioioioioioiodddddddddddddoioioioioioioioioioioioioio

Valid instructions are: i d o
payload> oioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioioio
ioioioioioioioioioioioioioioioioioioioioioioioioioioioioioi
Hello, world!
This is the last sentence from me. Bye.
"g\mWr`}Dh]J6dRd]:P%ata;M:yKl?.
```

Output berakhir setelah dua line, dan kemudian memberikan string dengan karakter acak yang terus berganti setiap input. Berarti kemungkinan besar flag tidak ada jika kita terus meminta program memberikan output.

Kembali ke input yang diminta oleh program, kalau diperhatikan terdapat substring panjang oioioioioi dengan substring dddddd di tengah. Input tersebut menghasilkan dua line "Hello, world!" maka dapat disimpulkan bahwa substring dddddd menyebabkan newline pada output program.

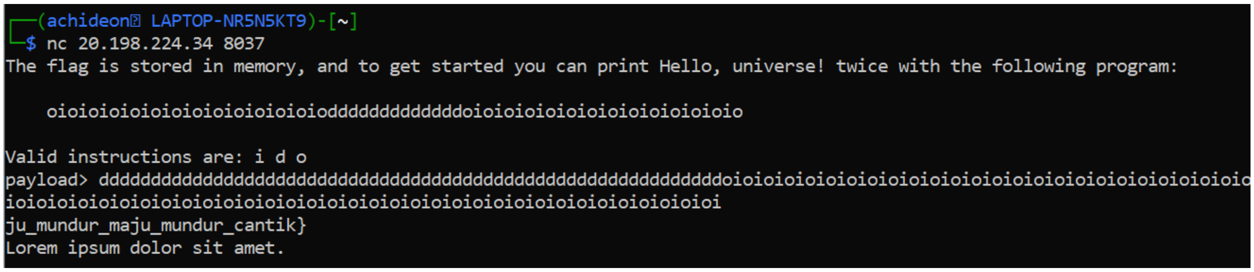
Kuncinya ada di substring 'ddd', kemudian dicoba lagi menggunakan beberapa kombinasi serupa namun lebih pendek

```
┌──(achideon㉿ LAPTOP-NR5N5KT9)-[~]
└─$ nc 20.198.224.34 8037
The flag is stored in memory, and to get started you can print Hello, universe! twice with the following program:

    oioioioioioioioioioioioiodddddddddddddoioioioioioioioioioioioioio

Valid instructions are: i d o
payload> oioioioioiddddoioioioioi
HelloHello
┌──(achideon㉿ LAPTOP-NR5N5KT9)-[~]
└─$ nc 20.198.224.34 8037
The flag is stored in memory, and to get started you can print Hello, universe! twice with the following program:

    oioioioioioioioioioioioiodddddddddddddoioioioioioioioioioioioioio

Valid instructions are: i d o
payload> oioioioioidddoioioioioi
Helloello,
```

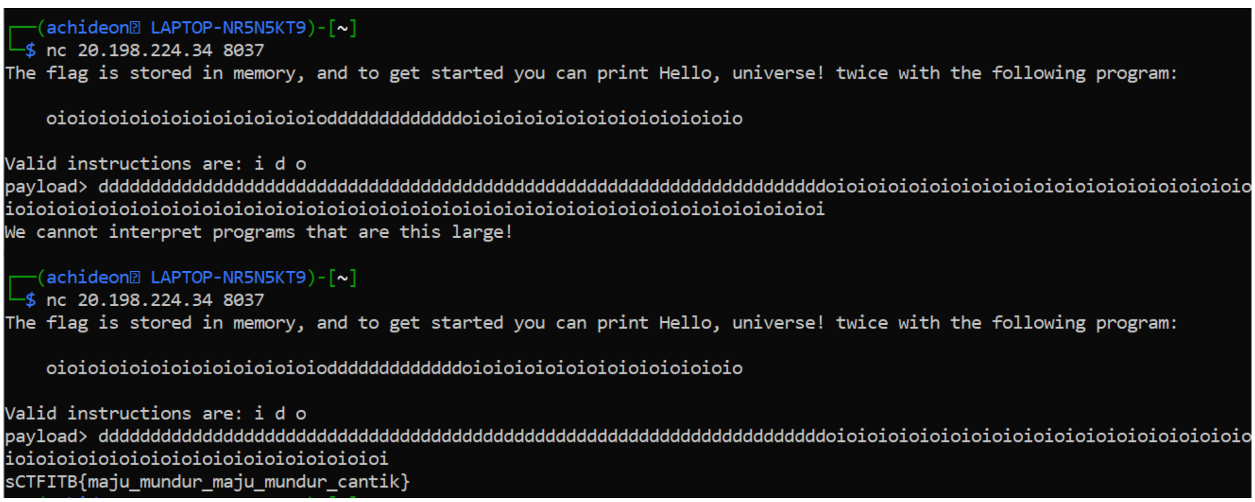
```
┌──(achideon㉿ LAPTOP-NR5N5KT9)-[~]
└─$ nc 20.198.224.34 8037
The flag is stored in memory, and to get started you can print Hello, universe! twice with the following program:

    oioioioioioioioioioioioiodddddddddddddoioioioioioioioioioioioioio

Valid instructions are: i d o
payload> oioioioioiddoioioioioi
Hellollo,
```

Semakin sedikit jumlah karakter d, semakin bergeser ke kiri juga output “Hello” yang kedua. Hal ini kemungkinan besar terjadi karena karakter d berfungsi untuk menggeser posisi awal string “Hello, World!” ke kanan. Tapi bagaimana jika karakter d merupakan input di awal?

Dapat terlihat output yang sebelumnya tidak muncul. Apabila karakter d dan oi lebih banyak lagi maka muncul sebuah potongan flag di belakang



Agar menghindari character limit dengan jumlah d yang semakin banyak, maka jumlah oi dikurangi secukupnya, hal ini tidak akan berpengaruh dengan flag karena yang terhapus di belakang hanya string “Lorem ipsum dolor sit amet.”



Setelah sejumlah ujicoba juga menyesuaikan character limit, akhirnya didapatkan flag yang dicari.

FLAG: CTFITB{maju_mundur_maju_mundur_cantik}