Cyber Youth Singapore

Blockbuster's Workers’ Union

horizontal line

**Creator Name: Kok Rui**

# Setup:

## **Static Files:**

* 1. NA

## **Usage:**

* 1. Run Python Flask app with nohup
  2. Setup DB

# Description:

* **Description:**
  + The last surviving Blockbuster Video store in the world is struggling to stay afloat in light of the COVID-19 situation :O They’ve since launched an e-service… but all their `workers` seem to have left! Can you leak out their reasons for leaving?
* **Hint:**
  + Just because the table on the webpage shows 4 columns doesn’t mean the DB table has just 4 columns… how do you figure out the number of columns? Why is this important?
  + The `workers` table doesn’t have many columns - the company doesn’t seem to care too much
  + If you’re trying to guess things (column names), you’re doing it wrong

# Solution

1. TL;DR Simply leak the in the `workers` table, one of the values will be the flag

SOLN 1:

1. Figure out how many columns in current table:
   1. Brute force: " or 1=1 union select 1,2,3,4..n; --
   2. If no error is thrown, n = correct number of columns!
   3. From this step, you will also be able to figure out which columns actually appear in the webpage.
2. Leak data from the `workers` table:
   1. Brute force: " or 1=1 union select \*,1,2,3...m from workers; --
   2. Make sure the data coming out from \* appears in webpage: edit positions by (example) " or 1=1 union select 1,2,\*,3...m from workers; --

SOLN 2:

1. Figure out how many columns in current table:
   1. Brute force: " or 1=1 union select 1,2,3,4..n; --
   2. If no error is thrown, n = correct number of columns!
   3. From this step, you will also be able to figure out which columns actually appear in the webpage.
2. Leak column names from INFORMATION\_SCHEMA.COLUMNS
3. Leak column exit\_reasons from workers