Problem 6: TigerHub 2.0 [HackerRank]

By Henry Tang

At the end of every semester, your roommate tweets a picture of her straight A-plus transcript. Except, she didn't do it last fall — fishy! You decide to investigate. You know the net-id of your roommate (it's `tygasan`), but not her password. Luckily for you (a tiger with questionable ethical values), Princeton University just splurged big bucks on TigerHub 2.0, a "new and updated" portal for its students to check their grades without the hassle of Duo security.

Why lucky for you? Because it's brought to you by the same company that "developed" TigerHub, so you know that TigerHub 2.0 has an SQL Injection vulnerability. However, you don't know exactly what it is. Pretending to be an inquisitive student taking COS 333, you call OIT and come to learn that the login information of users is stored in a SQLite database within a table called `users`, where two of the columns are `username` and `password`. While on the call with OIT, you hear in the background that every student has an override password *consisting of only numeric digits* that can be used to log into their account.

You really want to know what grades your roommate received in her 6 classes last semester. Can you leverage the information you overheard to figure them out? Once you do, write a program on HackerRank to spit out a string consisting of your roommate's grades, without any spaces or commas.

Website Specifications

The website for TigerHub 2.0 can be found here: `https://sql-injection-problem.herokuapp.com`. Marvel in it's glory!

Be mindful of the fact that there are two pages to the website: a login page, and a forgot password page. Logging in with a proper set of credentials on the login page will present you with the information you desire. To make sure you understand how this page works, you can enter the username *coscon* and the password *12345*, and you will see the message "Your grades are A+, A+, A+, A+, A+, A+".

Important Note

You should NOT be writing a script that brute forces password combinations. The point of this problem is to strategically implement a SQL injection attack to figure out the password, and login using it. Utilizing a script is not required to solve this problem, and moreover, it won't work, since you are automatically limited to at most 20 queries per minute on the website.

Input
No input will be provided.

Output
Your output should be a single string of length between 6 and 12. For instance, if your roommate's grades are straight A's, you should output "AAAAAA". On the other hand, if her grades are B+, C+, A-, A, P and F, you should output "B+C+A-APF". Note that if you successfully hack into her account, the grades will always be displayed in a specific order. Use that order when you submit your solution on HackerRank.