Cracking passwords

Since TAs know a lot about computer security, and against all recommendations, they decided to develop the class's website and its authentication from scratch. The TAs hear a rumor about a leaked password database that got to the students. As the TAs have hashed all passwords with SHA-256 before saving them they claim that the leak is not important because passwords are secure. To reinforce their argument, they make public the student's username/hash database and challenge students to guess the user/pass pairs.

Hint 1: The site only accepts passwords if they only contain printable ASCII characters.

Hint 2: If the username contains "-HARD" you may want to side with TAs ;)

Hint 3: It's not necessary to check password dictionaries which include more than 1 million entries.

Rubbing salt in the wound

After this incident, TAs decided to improve the site's password management. They add a unique salt for each password, and use scrypt, a specifically-designed password hashing algorithm, instead of SHA-256. To show the improved security, they released the new database. Can you prove them wrong?

Questions to reflect upon:

1. Does user behaviour impact the cracking difficulty?
2. How does adding salt and using scrypt impact the system?

You do not need to write an answer to these questions.

Submission

TAs provide the following files:

$sciper_auth.json a JSON file containing usernames and their corresponding salts and hashes with base64 encoding.

auth.py a script which replicates how TAs computed the password hashes in both approaches. This script allows you to validate your guesses and provides a grade token for each correct answer.

After validating your guess in the *auth.py* script, you **must** submit the token to Com-301 grading system.

Warning: since your grading is online, any manual change in the *auth.py* or *$sciper_auth.json* may lead to an invalid token. You can get full score by cracking 12 out of 16 accounts.

Warning: If you need to compute more than 3 hours to crack the password of one account, then you may rethink your approach.