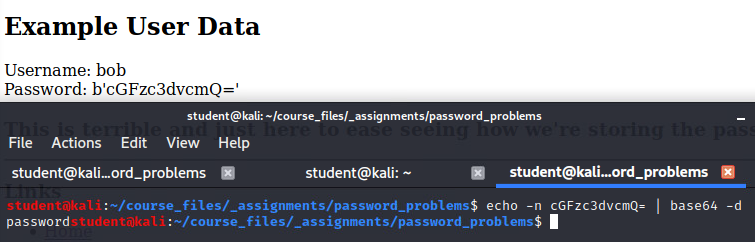
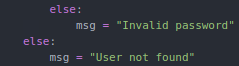
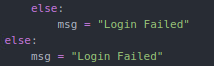
Discovery:

1. the password is stored as a base64 encoded value, which can be reversed.   
     
   the b’[…]’ was messing with thej decode… I don’t think it was salt though, since the same thing shows up on the tutorial I’m looking at for bcrypt. Maybe it’s just a big coincidince. Probably not.
2. The error messages give away too much info. Can bruteforce usernames by checking the error.

Remediation:

1. Change the stored passwords to a hash, and then check against the hash. Not sure if you wanted the changes made to update\_password.py or not so I’m sticking the caps in here.  
     
   app.py:

update\_password.py:

1. make it so the fail cases don’t reveal as much.