UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Make
today
matter

Make today matter

COS 330 – Practical 1

Password Cracking & Hashing

Due date: 6 August 2025 @ 11:00 am

Background

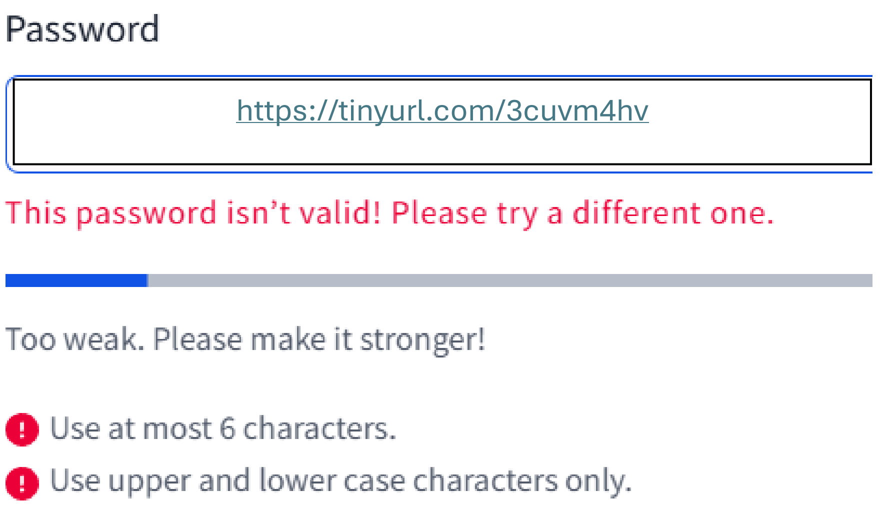
Passwords are one of the most common forms of authentication, but they are also among the most targeted and exploited by attackers. This assignment is designed to help you understand how passwords are protected using cryptographic hashing and why simple or improperly stored passwords can be easily compromised. You will learn how hashing works, how attackers use techniques like dictionary attacks to guess passwords, and how adding security measures like salting or using advanced hashing algorithms (e.g., bcrypt) makes passwords much harder to crack. By simulating both password protection and password attacks, you will develop a clearer understanding of how to think like an attacker and how to apply secure practices to defend against these threats. This assignment reinforces key concepts in cryptography and highlights the importance of secure authentication systems in real-world environments.

Instructions

For this practical, you have to implement the tasks below as well as write a report on your findings. Be sure to document all you have done, including screenshots and the commands you ran or any custom algorithm you have made. You are welcome to use any programming language to perform these tasks. You are not allowed to use 3rd party software (GitHub/Web) or AI generated code, you may use libraries provided by the programming language only. In your report, make sure you document your system specifications, such as processor, RAM and GPU.

Scenario

You have been employed by **hackernetZA** to secure a clients database. They are a small company and make use of SQLite because they do not have technical knowledge on how to set up a MySQL server. They have asked you as an aspiring security engineer to assist with securing their database as currently they store their passwords in plain text 🤮. You later find that they have a signup page that looks like the screenshot below.



Password

https://tinyurl.com/3cuvm4hv

This password isn’t valid! Please try a different one.

Too weak. Please make it stronger!

❗ Use at most 6 characters.

❗ Use upper and lower case characters only.

Task 1 – [10 marks]

An SQLite database (***users_realistic.db)*** containing usernames and passwords have been uploaded to ClickUP. You task is to take the plain text passwords and hash it with 3 different hashing algorithms (justify your choices in your report) and store the hashes in separate columns in the same database (this will be used in Task 2). Take a screenshot of the database schema, and the first 5 rows and include it in your report.

Hint: Use at least 1 insecure hashing algorithm to aid you in Task 2.

Task 2 – [30 marks]

For this task, you have to take the hashes of the 3 hashing algorithms you implemented in Task 1 and perform a dictionary or brute-force attack. You have to demonstrate at least 1 of the 3 hashing algorithms have been successfully "cracked" for at least 5 users. You may use John the Ripper for this task. Report on the commands used, time for each password to be "cracked", average time, total time, and screenshots. If the process does not finish after 2 hrs, simply make estimations as to how long it would have taken. Marks here will be awarded based on the methodology followed or any optimizations that have been performed.

Task 3 – [20 marks]

Now, that you have seen firsthand the effects of using strong hashing algorithms, and how easy it is for an attacker to figure out user passwords once they have the hash. Now, you become paranoid and perform **salt** and **pepper** to the most secure hashing algorithm you chose in Task 1. You then become further paranoid and explore encryption algorithms to secure the salt. Justify your choices in your report and write up an example of how it will work, as well as the code to successfully login a user. This can simply be a function to demonstrate the functionality, or a CLI tool.

Bonus – [5 marks]

As a bonus, there are 5 password hashes provided to you in the ***crackme.txt*** uploaded to ClickUP, your task is to get the plain text password.

Submission

Submit your report as a PDF file along with your code, and database in an archive called uXXXXXX_NAME_P1.zip to ClickUP before the deadline. Please upload well in advance, as there will be **ABSOLUTELY NO LATE SUBMISSIONS!!!**.

ALL THE BEST, you done reading now, so get cracking ….