The aim of this project is to create a password universe (PU) modelled on a web application. This PU is used to visualise a given password database as the “universe” and the entries of it as “stars”. The user is treated as the centre of this universe by choosing a keyword to compare with the database**.** Database doesn’t necessarily need to be with passwords, it can be any combinations of strings such as an English dictionary. It’s mostly aimed at password researchers and cyber security experts allowing them to see patterns thus helping them to gain further understanding of how passwords are related to one another. It can allow users to compare the same password with different databases and gain results of how users come up with their passwords.

## **Introduction**

An Introduction on the issue, there are billions of accounts hacked every year, unhashed data being spread around the internet that can be gathered if you know where to look. Recently there was a leak of millions of emails and passwords stolen and a lot have been unhashed and are spreading around [1], making hacking users easier using standard password cracking techniques such as dictionary attack, brute force attack and rainbow table attack. There is a problem that with such huge database of real unhashed user passwords, that many other can be potentially at risk because they have had a similar or the same password as the one that got hacked causing a leak of for example 10 million, possibly affect a much larger population. This project aims at using any password database to visualize any potential patterns people have whilst creating their passwords which can be used to potentially strengthen the requirements for passwords on websites. Currently, most websites have password meters but how does one decide what rules to add to their password requirements for these password meters. Different password meters perform differently [2] [3]. There was a research made in 2010 stating that our current password creation policies are still vulnerable to online attacks [4] and this issue still persists as more and more users are keeping the same passwords [3], using the same patterns of creation without knowledge of them being hacked and vulnerable.