Security report

Sixth Form App

Finlay Boyle

Contents

No table of contents entries found.

# Passwords

## Hashing

If the system is to be used in a live environment, it is important that students and staff can be confident that their passwords are safe from malicious attacks as well as safe from viewing by other staff and the developing team. The idea behind hashing is to have a one-way function which takes input of arbitrary length (like passwords) and converts it to a completely unrelated fixed length set of characters. This secures passwords – both from hackers and people with legitimate access to the database – by making it impossible to reverse the passwords without guessing every combination.

To do this, we have made use of a cryptographically secure algorithm known as BCrypt[[1]](#footnote-1). This should ensure that the passwords are safely stored in the database. In addition to this, it is not possible to tell if two users have the same password as it automatically appends a random code to the password before hashing it.

### Technical Details

Hashing needs to be balanced between the time taken to generate a hash and the time taken to guess the hash. This is controlled by the hash cost in BCrypt. Currently, this is set to 12 but can be increased with little effort. This is a suitable cost as it should take approximately 1 second to generate hash. The following calculation approximates how long it would take to crack a single password which has been hashed by the BCrypt algorithm[[2]](#footnote-2) with cost 12 (the method has been adapted to account for uppercase and lowercase letters).

Even using generous rounding, the time taken is extortionate which clearly suggests that the passwords will be safe.

In addition to this security, the passwords are salted so it is not possible to tell if two users have the same password which also protects against rainbow table attacks.

Over time, it would be important that the cost is increased in order to maintain this security because hardware will improve which means that the number of hashes per second increases which, in turn, decreases the time taken to guess each password.

## Resets

Password resets can only be done by an administrator. This means that it cannot be abused to enable access to the system. Additionally, there is no method for requesting a reset via the app which prevents random people requesting the reset of an accounts password. Instead, it is advised on the login page to ask a member of staff to reset passwords.

Furthermore, as the hash of the default password (Passw0rd) is randomly generated, it is not possible to tell which users still have the default password set which offers a further layer of protection.

## Changes

1. https://en.wikipedia.org/wiki/Bcrypt [↑](#footnote-ref-1)
2. https://security.stackexchange.com/questions/182111/mathematically-how-long-would-it-take-to-crack-a-bcrypt-password-hash [↑](#footnote-ref-2)