COMPX518 Assignment 1, Part 2: Authentication System Report

Stefenie Pickston

6-05-2022

Abstract

This report will cover the design and structure of the password based authentication system. I implemented my solution in Java.

1 Block Diagram

2 Username Requirements

2.1 Usernames Should Be Case Insensitive

This is implemented by converting all letters in the String to lowercase.

2.2 Usernames Should Only Use Certain Characters

The subset of these characters are: *[a-zA-Z0-9_]*

If there exists a character in the username that falls outside of the subset then the system will produce an error message.

2.3 Usernames Must Not Have Profanity

The username goes through a refactoring process before being checked against a dictionary of swear words.

The refactoring process includes removing leetspeak (see 2.4), removing repeated letters and underscores. The dictonary is checked twice, where consecutive repeated letters are reduced down to one instance, and another where they are reduced down to two instances. This is because there are certain swear words with double letters that could potentially be missed in the initial search.

The dictionary *Word_Filter.csv* is stored as a csv as it includes both blacklisted and whitelisted phrases. The blacklisted phrases are stored in the first collum. If there exists a whitelisted word that contains the blacklisted word it is stored in the second collum.

2.4 Leetspeak Is Not Allowed To Bypass 2.3

Before the username is checked against the dictionary of banned words, it goes through a filter in order to remove leetspeak. The numbers below are converted to their corresponding letters:

```
1 = i     3 = e     4 = a     5 = s     7 = t     9 = g     0 = o
```

2.5 Character Limit

The username length is checked in the *lengthu(username)* method to ensure it is between 2 and 20 characters. If not the system will produce an error message.

3 Password Requirements

According to the NIST password guidelines, it is required that passwords are between 8-64 characters and are not commonly used.

3.1 Character Limit

The password length is checked in the *lengthp(password)* method to ensure it is between 8 and 64 characters. If not the system will produce an error message.

3.2 Passwords Must Not Be Commonly Used

The password is checked against a list of around 14 million commonly used passwords, contained in a file called *rockyou.txt*. The passwords within *rockyou.txt* are the most commonly used passwords that have been collected from various data breaches.

3.3 Password Attempts

In the case that an adversary is trying to brute force the login system, after 5 incorrect login attempts the system locks for 30 seconds.

4 Storage

I have stored my user credentials in a csv file. The username is stored in plaintext and the password is hashed with Argon2id.

4.1 Password Hashing

According to NIST guidelines Argon2 hashing is reccomended for password hashing, specifically Argon2id as it has both benefits of Argon2d and Argon2i. A random 16 byte salt is generated for each new password and is stored along with the hash.

The parameters I have used for the hashing follows the NIST guidelines:

```
- Salt Length: 16 Bytes (at least 32 bits is reccomended)
- Memory: 64MB (at least 15MB of memory is reccomended)
- Parallelism: 2 (at least 1 is reccomended)
- Output Length: 32 Bytes (32 Bytes reccomended)
- Iterations: 4 (at least 2 is reccomended)
```

The hash and salt are stored in base64 in the Argon2 hash format, along with the parameters.

4.2 Displaying Passwords

According to the NIST guidelines passwords must be viewable by the user. For confidentiality reasons passwords are hidden on the terminal after the user has pressed ENTER.

5 Error Messages

5.1 Registration

If a user account already exists, the system does not tell the user this, as it may give the user an incentive to carry out a bruce force attack on the user account. Instead it shows a generic error message: *"Invalid Input, try again."*.

If any of the other username requirements fail, the error message provides information as to why the username was rejected. This also applies to the password requirements.

5.2 Login

When either the username or password is incorrect, the system will display a generic error message: *"Invalid details!"*. This is to prevent any potential malicious parties from gathering any information about the accounts.

6 Program Instructions

Please refer to the README.md file for installation and execution instructions.

References

[1] NIST, "NIST Special Publication 800-63B," Nist.gov, 2019. https://pages.nist.gov/800-63-3/sp800-63b.html