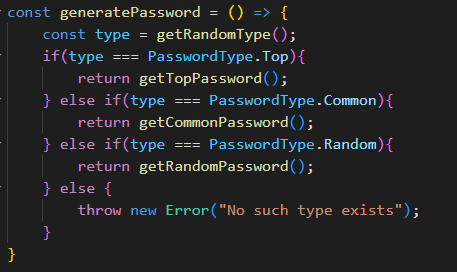
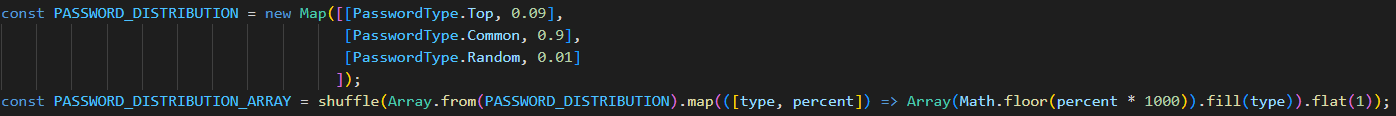
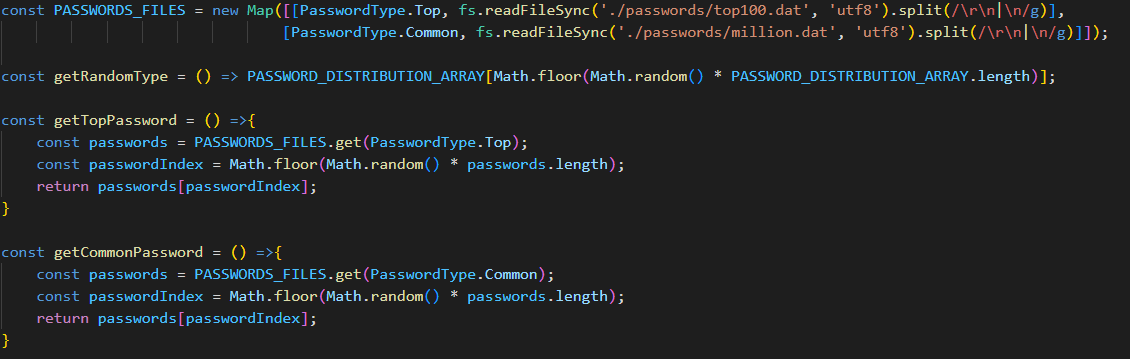
1. To create passwords this function is used.



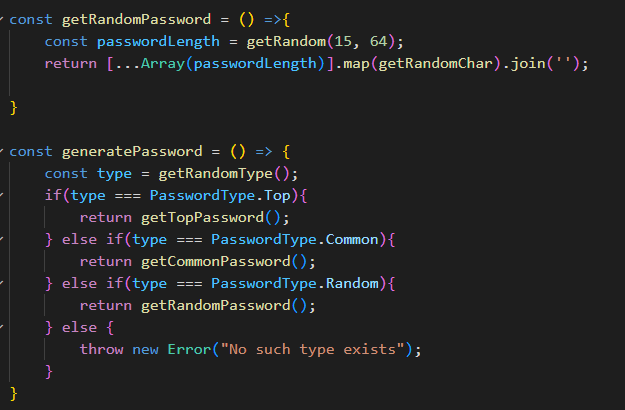
1. To get random type such code is used. There we create array of 1000 elements which has shuffled duplicating values of type. And then randomly choose type from the array.



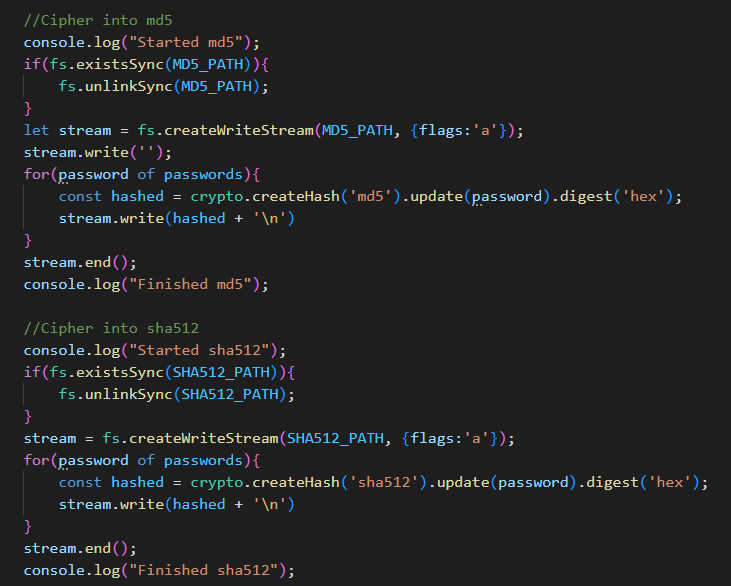
1. Getting passwords from file looks the same.



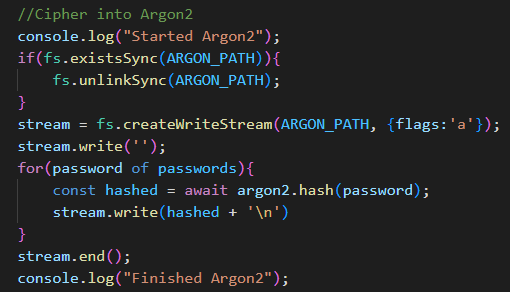
1. Here is the function for generating strong passwords.



1. For hashing md5 and sha256 standard node.js library ‘crypto’ is used.



1. And for Argon2 external library is used.



Part 2

1. For hashcat let’s take hashes from here(<https://hashkiller.io/leaks>) for site avito.ru.
2. There was dictionary attack.

For dictionary is used 1 billion list.

<https://github.com/piotrcki/wordlist>

But passwords wasn’t found.

3. Recommendations:

Use Argon2 for password encryption. It drastically reduce speed of guessing password if database will be leaked.

We shouldn’t limit password length.

Exclude common passwords.

Don’t limit charset.

Password length must be at least 8 symbols, recommended 16.

Password should be generated.