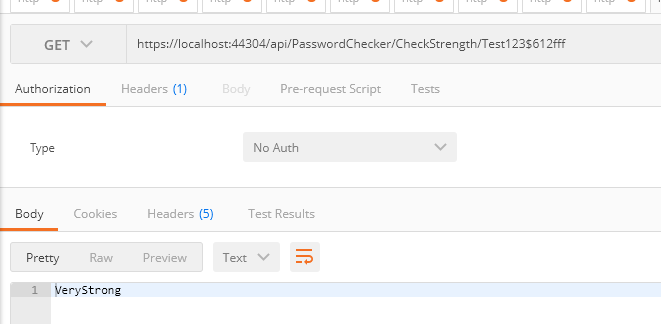
Technical Specification

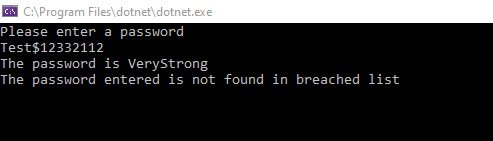
# Requirement Realisation

A rest based api to check the password strength is developed.

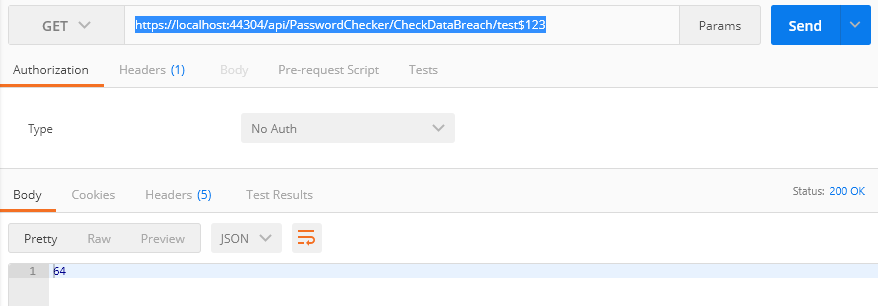


## 

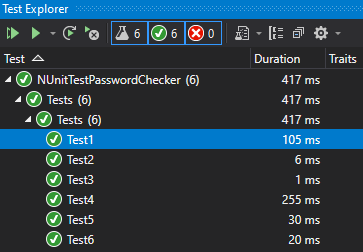
A console application to consume the api services has been developed.



Created the service that checks whether the password has appeared in data breaches, and provides the number of times the password has appeared in those breaches. The k-anonymity model is being used to secure the data being searched for. Console application displays the results from second api.



Basic level NUNIT test cases are created to check the logic.



# Notes

Configuration for the API is configured in the appsettings.json.

"HIBPApiKey": "1f1e5caf16ac4a3c8572f301e38af583",

"UserAgent": "PasswordCheckerApi",

"PWNEDApiURL": "https://haveibeenpwned.com/api/v3”,

"RangeApiURL": <https://api.pwnedpasswords.com>

The api URL is configured in the console application like below.

private static readonly string URL = "https://localhost:44304/api/PasswordChecker/";