ZZCA9209 – Security Engineering Capstone

(H424 Online)

Software Development Project

Week One Progress Report

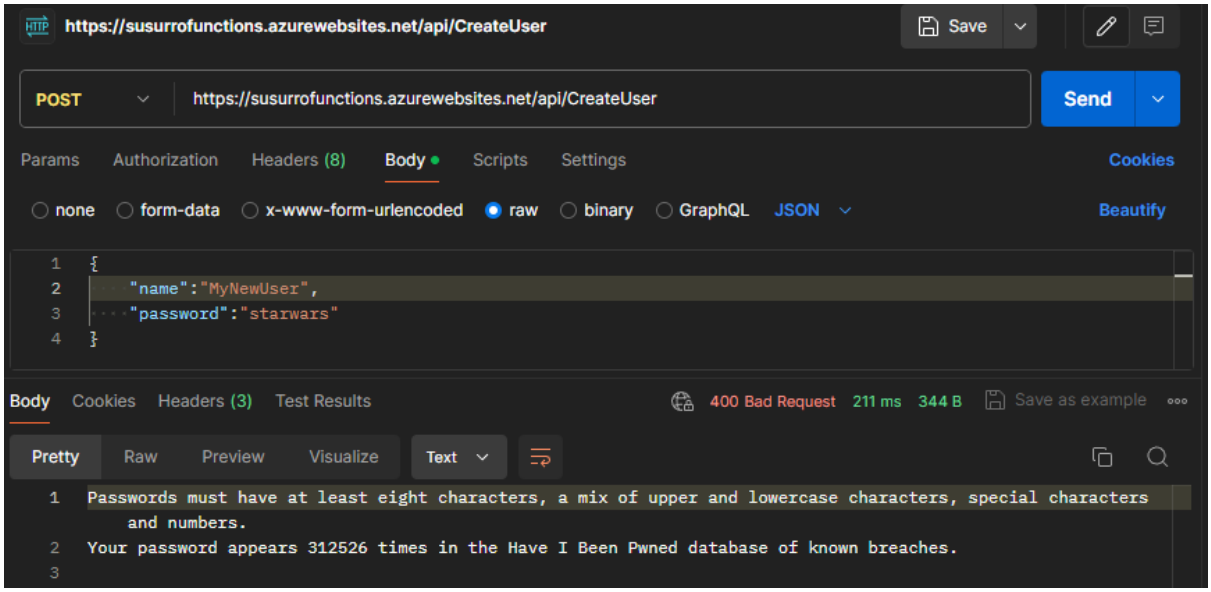
Dave Catling

Student ID: 5430029

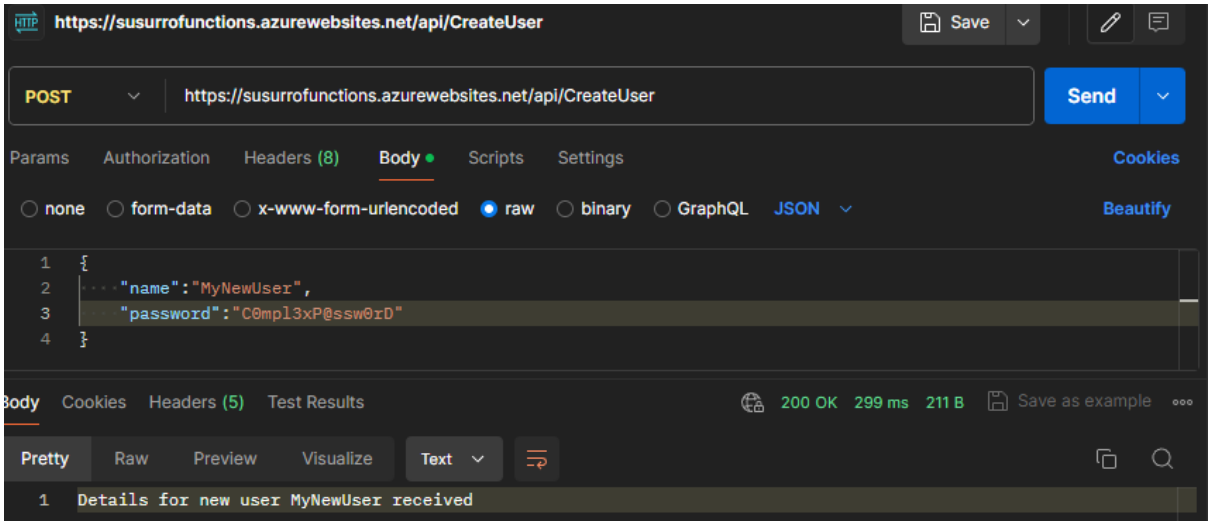
Work Completed

The public GitHub repository has been established at https://github.com/davecatling/Susurro. Three key cloud resources have been provisioned, the serverless function application to serve as a backend API, an Azure storage account containing the data table for account details and an Entra managed identity allowing interaction between the API and storage.

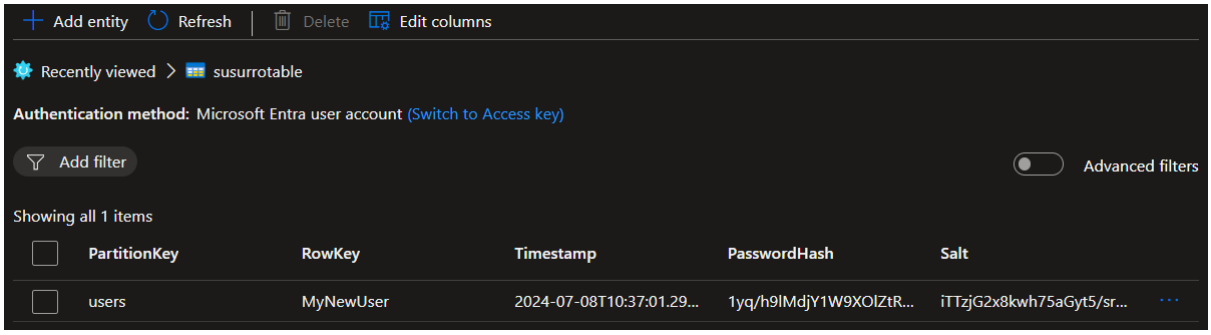
The cloud API presently consists of only a single endpoint, CreateUser (https://susurrofunctions.azurewebsites.net/api/CreateUser). This endpoint takes a POST request for new user creation, which presently requires only a JSON payload defining requested username and password. If the name is not already in use the password is examined for some simple complexity requirements and the HIBP API called to check its previous use in known data breaches. If these checks fail guidance is returned via a 400 response.



Bad Request response for a weak password appearing in HIBP >300k times



Successful user creation with a safe (well, better) password



Created username, salt and hashed password in the Azure portal

Reflections

The work completed this week included my first usage of the HIBP API (inspired by a discussion following the O week seminar). It was also my first experience with Entra managed identities (https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview). It was very rewarding to get the managed identity working, and it's clearly a better solution then managing secrets myself between the web application and other resources (the storage account in this case). However, it did prove frustratingly difficult to configure. Now I know what to look for though I'm sure I'll be using this concept a lot more in the future.

Summary

With some critical back-end assets now in place, this week I am confident that I can expand the application to achieve generation, storage and exchange of keys. The SignalR service may potentially be provisioned by the end of this week as well, though I have rethought how it will be employed. Rather than providing the mechanism for message exchange itself, this real time messaging service will deliver notifications only, triggering the client to retrieve the encrypted messages directly from my API.