Team Delta

Cybersecurity Evaluation

We are building a Web Application using Asp.net core platform. All the data are stored on the server side. The users can only interact with Html pages, and only those with authorization can access the server database. More importantly, for the usernames and passwords we use to login into our system will not be stored in plaintext in our database. We will be using a vetted, packaged identity solution called ASP.NET Core Identity. Or if the users decide to use their social media logins, we use OpenID Connect to login without the need to store password altogether. These methods are well tested, independently verified, and supported solution. Therefore, data are rest well protected.

For date in motion, we would need https to secure the data. luckily, https is enables by default in ASP.NET Core. The HttpRedirection middleware class provides us the necessary functionality to redirection from http to https.

Our entire project was implemented on the Visual Studio IDE, it provides many extension and libraries that we can use to build. By using Asp.net core, we can write C#, Html, and Sql command in one page, it provides us with stable, supported, and convenient working environment. Our server located in the Microsoft Azure, and it is a cloud service very compatible with Visual Studio. It’s also very stable and maintained daily by Microsoft technicians.

Our project does not have any physical security form except the Azure Server which the project is hosted on. I believe it is very hard to penetrate and damage the server. Even so, there are backup server that will immediately take over.

Since it is a website, it has many ways to attack it as every other website. Methods like DDoS or Phishing. Form human/social “engineering” aspect, it could be our administrator’s account been compromised by phishing, password stolen.