CROSS ORGIN RESOURCE SHARING(CORS)

CORS is a security mechanism used by web browsers to allow web pages to access resources from a different domain.

In our example we were connecting from ***http://localhost:3000/*** to ***https://localhost:44315/***

When a web page tries to access a resource from a different domain, the browser sends a CORS request to the server hosting the resource. The server responds with a set of headers that indicate whether the request is allowed or not. If the request is allowed, the server can also specify which methods (e.g. GET, POST, etc.) are permitted, and what type of data (e.g. JSON, XML, etc.) can be sent and received.

CORS is important because it helps **prevent malicious websites from accessing sensitive information from other websites**. It also enables developers to build web applications that consume resources from multiple domains.

In react we need to do the following

```
import axios from 'axios';

axios.get('https://example.com/api/data')
    .then(response => {
        console.log(response.data);
    })
    .catch(error => {
        console.error(error);
    });
```

In .Net Web API we need to do the following

```
public void ConfigureServices(IServiceCollection services)
{
    services.AddCors(options =>
    {
        options.AddDefaultPolicy(builder =>
        {
            builder.AllowAnyOrigin()
                   .AllowAnyHeader()
                   .AllowAnyMethod();
        });
    });
}

public void Configure(IApplicationBuilder app, IWebHostEnvironment env)
{
    app.UseCors();
}
```