Esta prueba la realice con Angula 8 y para la base de datos se utilizó firebase, la configuración de la misma se encuentra en el archivo environment.ts en la ruta `src/environment`.

Dentro de `src/app/app.module.ts` se configura la conexión a la base de datos por medio de una importación: `AngularFireModule.initializeApp(environment.configFirebase)`

Dentro de `src/app/models/customer.interface.ts` se encuentra el modelo de datos que se está utilizando.

En el archivo `src/app/services/customer.service.ts` se encuentra la clase CustomerServices, en el constructor de la misma se encuentra contiene las funciones que realizan el crud.las cuales son:

- Listado de productos

```
getAllCustomers(){
  return this.custumers
}
```

- Ingreso de producto

```
addCustomer(customer: CustomerI){
  return this.customerCollection.add(customer);
}
```

- Edición de producto

```
editCustomers( customer: CustomerID){
  return this.customerCollection.doc(customer.id).update(customer);
}
```

- Eliminación de producto

```
deleteCustomer(id: string){
  return this.customerCollection.doc(id).delete();
}
```

Como se puede observar en las funciones de la clase, gracias a angular la realización del CRUD es de forma sencilla por medio de métodos que tiene ya el framework, aparte de que el se encarga de tener un mínimo de seguridad en ellos, ya de resto el manejos de los datos es por parte de los componentes del sistema como lo es el de mostrar el detalle que se realiza en `src/app/components/list-customer/list-customer.component.ts`

Como mejora y medidas de seguridad que implementa sería que al momento del login se tenga una encriptación asimétrica en la que el front del sitio maneje una clave pública para encriptar información sensible al momento de realizar un login en el sitio y que el back sea el único que conozca la clave privada que funciona para encriptar y desencriptar. Una de las encriptaciones más conocidas dentro de este tipo es la encriptación AES.

Aparte cada petición dentro del sistema una vez ingresado debe llevar un token y un id dentro del header de la petición y en algunos casos mezclan la encriptación asimétrica con la simétrica para mejorar la seguridad y el resguardo de los datos.

Tipos de encriptaciones

Estándar de cifrado avanzado (AES) `Encriptación asimétrica`

AES es un algoritmo de clave simétrica y utiliza un cifrado de bloque simétrico. Comprende tres tamaños de clave: 128, 192 o 256 bits. Además, hay diferentes rondas de encriptación para cada tamaño de clave. Una ronda es el proceso de convertir texto sin formato en texto cifrado. Para 128 bits, hay 10 rondas. 192 bits tiene 12 rondas y 256 bits tiene 14 rondas.

Como tal, el gurú del cifrado Bruce Schneier no “cree que alguien pueda descubrir un ataque que le permita a alguien leer el tráfico de Rijndael”, fuera de los límites teóricos del cifrado académico. El algoritmo de cifrado Twofish de Schneiers (discutido a continuación) fue un rival directo de Rijndael durante la competencia para seleccionar el nuevo algoritmo de seguridad nacional.

RSA `Encriptación asimétrica`

RSA (llamado así por sus creadores Ron Rivest, Adi Shamir y Leonard Adleman) es uno de los primeros algoritmos criptográficos de clave pública. Utiliza la función de encriptación asimétrica unidireccional que se encuentra en el artículo vinculado anteriormente.

Muchas facetas de internet usan extensamente el algoritmo RSA. Es una característica principal de muchos protocolos, incluidos SSH, OpenPGP, S / MIME y SSL / TLS. Además, los navegadores usan RSA para establecer comunicaciones seguras sobre redes inseguras.

RSA sigue siendo increíblemente popular debido a su longitud clave. Una clave RSA suele tener una longitud de 1024 o 2048 bits. Sin embargo, los expertos en seguridad creen que no pasará mucho tiempo antes de que se resuelva el RSA de 1024 bits, lo que provocó que numerosas organizaciones gubernamentales y empresariales migren a la clave más fuerte de 2048 bits.