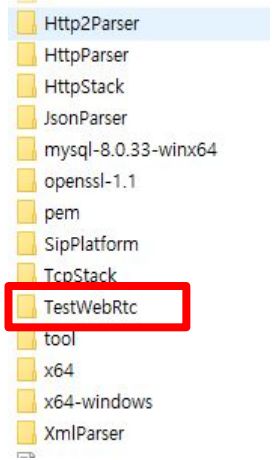
VideoChat

3조 보안연대
Team David Belasco

OpenSource



Download from MySQL connector website
Download OpenSSL 1.1.1u build
Self-signed credentials added

Main project requirements added(R1 ~ R16) / 2 factor authentication
DB minimum privilege batch
Execution files
SMTP porting library

Functional Requirements

No	Requirements	Satisfactory	Security
R1	1. The ability for the user to register with the system	YES	**TLS based wss used with port 443**
R1.1	1.1 The user shall provide the system their email address and password.	YES	
R1.1.1	1.1.1 The system shall ensure that the user's password is secure.	YES	**Password is saved SHA-256 with salt**
R1.1.2	1.1.2 Passwords must be a minimum of 10 characters long and include one number and one symbol.	YES	**LG Password rule is applied** **1. at least 1 alphabet** **2. at least 1 special character** **3. at least 1 number** **4. length should be 10 ~ 15**
R1.2	1.2 The system shall use two-factor authentication.	YES	**Google OTP is applied as well as user password** **Google OTP can be used with "QR code" or "Setup Key"**
R1.3	1.3 The system should force a user to periodically reset their password (at least once a month).	YES	**Detect 1 month past after setting password** **Password setting UTC time is saved in Database**
R1.4	1.4 If the user enters the incorrect password more than three times, then their account will be locked for one hour.	YES	**Password wrong count and UTC time tried is saved in Database / User blocked**
R1.5	1.5 The system shall allow users to change their email address in a secure way.	YES	**Email address can be changed securely using TLS**
R1.6	1.6 The system shall provide the ability for the user to recover or change their password in the event it is lost.	YES	**Password can be changed securely using TLS.** **Password can be sent to user's email by SMTP with TLS.**

Functional Requirements

No	Requirements	Satisfactory	Security
R2	2. After successful registration the system shall assign the user a unique contact identification name (contact identifier).	YES	**system has a functionality checking unique_id is unique Unique id is used for the system**
R2.1	2.1 this can be the user's email address or some other name chosen by the user if it does not conflict with other user's contact identifiers already in the system.	YES	**system has a functionality checking unique_id is unique**
R3	3. The system shall provide a contact list that associates a person with their contact identifier (last name, first name, address, e-mail, contact identifier).	YES	**System provide the contact list login-ed through TLS connection "Retrieved Logined ID" button support this requirement**
R3.1	3.1 . When a contact is associated with a contact identifier the VoIP application shall display the contact's name instead of the contact identifier.	YES	**All login user information is displayed**
R4	4. The system shall provide the ability to initiate a call using a contact identifier or the contacts list.	YES	**unique_id is used for peer connection**
R4.1	4.1 During the call initiation, the user shall be presented with call status and outcome (answered, busy or rejected).	YES	**system presents BUSY, REJECT, ANSWER**
R4.2	4.2 During call initiation the user shall have the ability to end the call at any time.	YES	**system has the ability to Call END**

Functional Requirements

No	Requirements	Satisfactory	Security
R5	5. The system shall provide the ability to accept or reject calls while not in a call.	YES	**System has the ability to Accept or Reject**
R5.1	5.1 Application shall show the caller's contact identifier or contact name during an incoming call.	YES	**During incoming call, user can see the contact name**
R6	6. The system shall notify the user of missed calls, either because the call was not accepted or because the called entity was in another call.	YES	**system notify missed call**
R7	7. Provide the ability to terminate a call at any time while in a call.	YES	**system can terminate call**
R7.1	7.1 If a call is terminated by one user, the other caller shall be notified.	YES	**system can notify it**
R8	8. Application shall be brought to the foreground during an incoming call.	YES	**We are using web browser(e.g. Google Chrome) as a client, so bringing the browser to the foreground might be challenging. However, we notify users through pop-up alerts.**
R9	9. This application is a point-to-point communication system. That is, each end point of the call should function as both a server and a client.	YES	**WebRTC peer connection is used**

Quality Attribute (Non Functional)

No	Requirements	Details	Satisfactory
R10	Performance	The system must deliver call video/audio as close to real time as possible.	**YES**
R11	Authentication	1. The system must use two factor authentication for sign on and user credentials must be protected. 2. Lost or compromised credentials must be handled in a reasonable way.	**YES**
R12	Communication privacy	1. The system must ensure that calls remain private. 2. No intermediary should be able to snoop or spy on an ongoing call.	**YES**
R13	Proof of identity (nonrepudiation)	Users should be confident that the entity they are on a call with is the one that they believe it is.	**YES**
R14	Reliability	1. The system must ensure that calls are reliable. 2. The system should recover from networking errors and dropped calls as soon as possible. 3. The goal is to maintain a secure, performant connection at all costs.	**YES** **If disconnected network, it recover again with QUIC protocol**

Security Requirements

No	Requirements	Details	Satisfactory
R15	Reliability	All transaction should be logged	**YES**
R16	SQL query safe	SQL query should be binded	**YES**