**2022년도 졸업프로젝트[Back-end]**

주제: TLS를 구현을 통한 홈페이지 제작 및 보안 채널 로그인 기능 구현

|  |  |  |  |
| --- | --- | --- | --- |
| **작성자** | 이유민 | **작성일자** | 2022.09.21 |

* **금일 진행 상황**

|  |  |
| --- | --- |
| **진행 상황** | **비고** |
| **질문 및 진행방식에 대한 논의**  **진행 중**  **1.OTP와 보안카드의 차이점:**   1. OTP   -알파벳과숫자를 섞어 만든 랜덤문자열이용(Seed=날짜)  String randomString = RandomString(); String salt = String.*format*("%d%d%d",pk4,num1,num2); String hashData = hashingData(randomString+salt);  \*랜덤문자열 생성함수(아스키코드 변환 이용)  public String RandomString() {  int leftLimit = 48; // numeral '0'  int rightLimit = 122; // letter 'z'  int targetStringLength = 20;  String generatedString = keyRandom.ints(leftLimit, rightLimit + 1)  .filter(i -> (i <= 57 || i >= 65) && (i <= 90 || i >= 97))  .limit(targetStringLength)  .collect(StringBuilder::new, StringBuilder::appendCodePoint, StringBuilder::append)  .toString();  return generatedString; }   1. 보안카드(SecurityCard)   -사용자의 refreshtoken+salt값으로 해쉬  String Data = member.getRefreshToken(); String salt = String.*format*("%d%d%d",pk4,num1,num2); String hashData = hashingData(Data+salt);  **2.AccountController**  -4개의 컨트롤러 사용(보안카드,OTP중 하나는 논의 후 삭제)  GET:랜덤넘버 두개 추출(보안카드,OTP 검증 값 전달)  POST:해시 데이터 비교(보안카드,OTP 검증)  POST:계좌 검증  POST:계좌 이체  **완료**  **진행 예정** | re |
| * **특이사항 / 협업 사항** | |