**2022년도 졸업프로젝트**

**팀이름: 황제펭귄**

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

|  |  |  |  |
| --- | --- | --- | --- |
| **작성자** | 정경재 | **작성일자** | 2022.03.23 |

* **금일 진행 상황**

|  |  |
| --- | --- |
| **진행 상황** | **비고** |
| **질문 및 진행방식에 대한 논의**  **진행 중**   1. Server에 TLS 1.2(HTTPS) 적용을 위한 작업 - 개인키 및 공개 키를 저장할 공간을 생성 Desktop/ssl에 저장 - 개인키(Secret Key)를 생성(2048bits) openssl genrsa -out private.key 2048 텍스트이(가) 표시된 사진     자동 생성된 설명 - 공개키(Public Key)를 생성 openssl rsa -in private.key -pubout -out public.key 텍스트이(가) 표시된 사진     자동 생성된 설명 - CSR을 생성한다, 각종 정보들을 입력한다. openssl -req -new -key private.key -out private.csr KR Seoul Jongno-gu Sangmyung\_EmperorPenguin Security EmperorPenguin Email challenge-password: EmperorPenguin 텍스트이(가) 표시된 사진     자동 생성된 설명텍스트이(가) 표시된 사진     자동 생성된 설명 - CRT를 생성 openssl req -x509 -days 365 -key private.key -in private.csr -out EmperorPenguin.crt -days 365 텍스트이(가) 표시된 사진     자동 생성된 설명 - CRT를 PKCS12로 변경 openssl pkcs12 -export -in EmperorPenguin.crt -inkey private.key -out .keystore -name tomcat 비밀번호는 **“미공개”.** 텍스트이(가) 표시된 사진     자동 생성된 설명 - 생성 모습 텍스트이(가) 표시된 사진     자동 생성된 설명 2. 사이트에 적용된 모습 텍스트, 스크린샷, 모니터, 화면이(가) 표시된 사진     자동 생성된 설명 3. WireShark로 TLS1.2 적용과 패킷이동 확인.   **완료**   1. Server에 적용시킬 Cert생성. 2. Server에 TLS 1.2버전의 적용이 완료됨. 3. WireShark로 TLS1.2 적용과 패킷이동 확인함.   **진행 예정** |  |
| * **특이사항 / 협업 사항**   현 시각부터 Back-End의 코드는 각자 환경에서 작성과 테스트까지 하고 업로드해서 확인하는 작업은 팀장의 정경재의 환경에서 한다. 🡪 TLS 1.2를 적용했기에 Cert를 배포해야함. | |