개인 신상

성　　명 : 최윤선

생년월일 : 1995 년 08 월 31 일

연 락 처 : 010-9438-5248

E-mail : cysun31@naver.com

학력	
기간	학 교
2015 ~ 2019	가톨릭대학교 (전공 : 물리학과, 복수전공 : 컴퓨터정보공학부)

자격사항		
자격 증명	취득일	발행처
정보처리기사	2019.08.16	한국산업인력공단

주요 경력 사항		
기간	회사명 / 부서	주요 업무
2018 년.07 월 ~ 2019 년 01 월 (06 개월)	NCSOFT 보안점검팀 (계약직 직원)	- 사내의 주요 홈페이지에 대한 취약점 점검
2018 년.04 월 ~ 2018 년. 12 월 (09 개월)	포스코 ICT (외주)	- 계열사의 주요 홈페이지에 대한 취약점 점검

대외/내 활동 사항		
기간	활동명	활동내용 및 주요역활
2016 년.03 월 ~ 2020 년 02 월 (48 개월)	보안 동아리 활동 CAT-Security	- 주 3 회 보안 스터디 참여 - 매 방학마다 학내의 주요 홈페이지에 대한 취약점 점검 진행

사용 가능 기술	
Language & Tools	JAVA, C, Python
Database	Oracle, Mysql
OS	Linux
Tools	Burp Suite

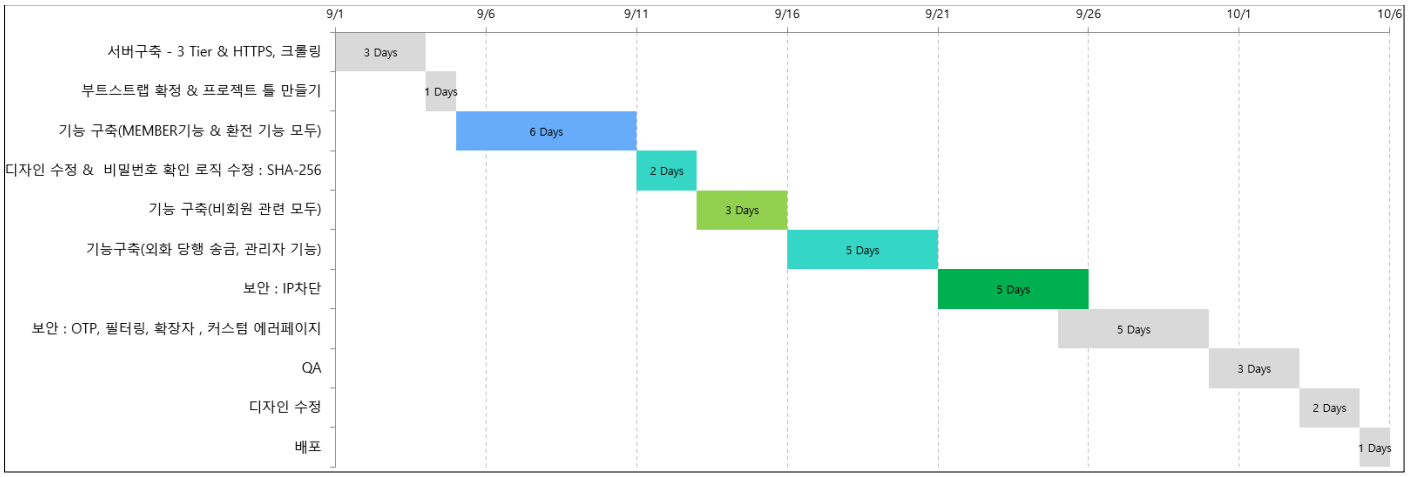
프로젝트 # 1

1. 실습 과제명 : 안전한 환전지갑	
수행 기간	2020. 09. 02 ~ 2020. 10. 07
홈페이지 주소	https://sbank.ml/SBANK
개발환경	- OS : Ubuntu 20.04, Windows 10 - JAVA : JAVA SE 8 - WAS : Tomcat 9.0 - DB : Oracle 12C
Language/Tools	- Language : Java, Python3, Shell Script, JSP, HTML, CSS, JavaScript, - Tools : Eclipse, XShell, SQL Developer - Framework : Spring, Mybatis, Bootstrap - Database : Oracle DBMS - Server : Apache2 - Etc : Git
사용 기술	- 카카오 아이디로 로그인 - 카카오 페이 결제 연동 - Morris Chart - 그래프 - Python3 - 웹 크롤링 : 환율정보 크롤링 - Google OTP 로 본인 인증 - Naver Lucy XSS Filter

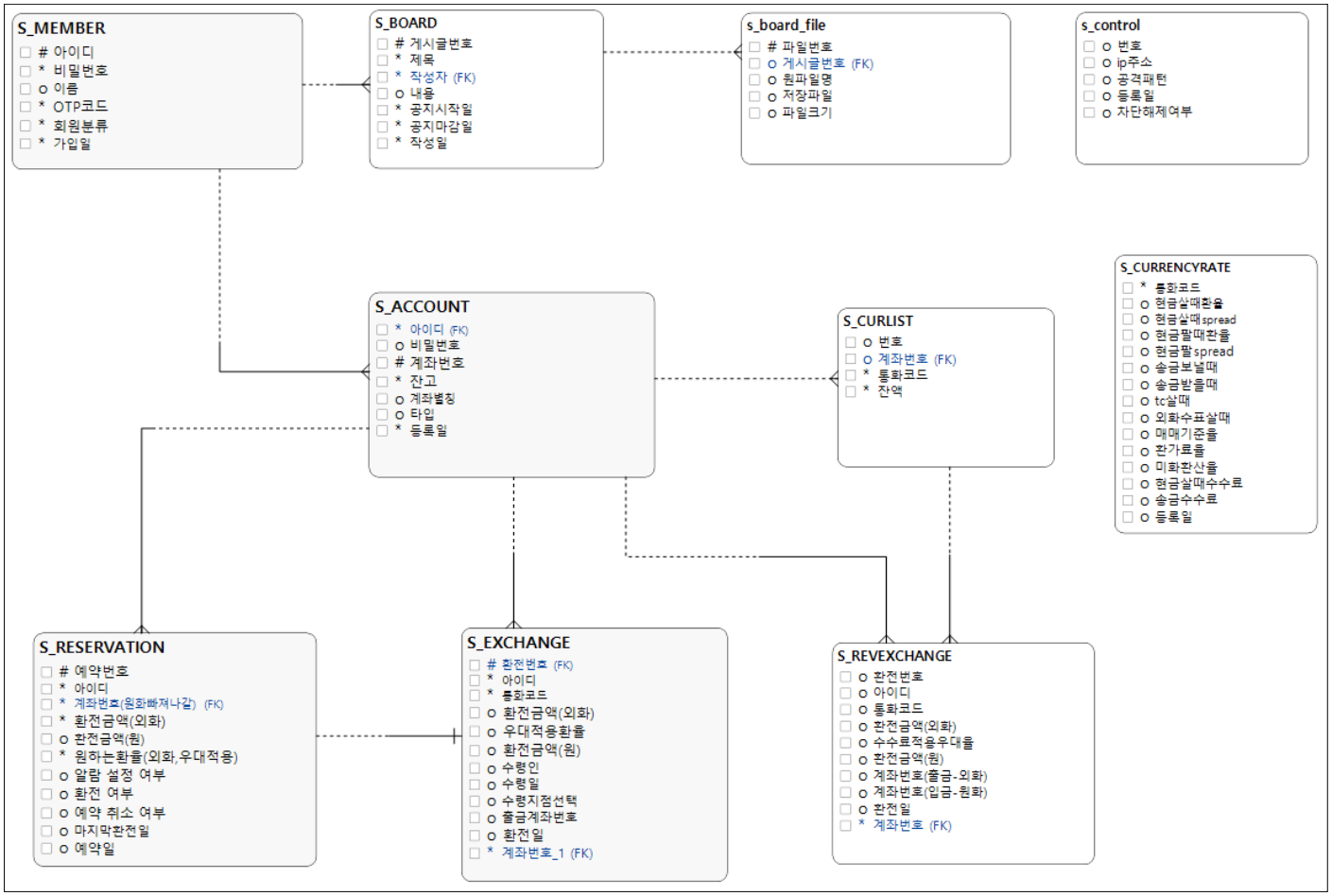
▶ 개요 및 목적

- 웹 어플리케이션에서 안전하게 외화를 환전하고 보관할 수 있는 '환전 지갑' 서비스.
- 특징 : 타깃 경쟁사는 신한은행이며, 신한은행과 하나은행의 서비스의 장점을 벤치마킹.
  : 개발 후 보안성(OTP, 보안 필터링, IP 차단 등)을 높임.

▶ 진행일정 (프로젝트 기간 : 2020.09.02 ~ 2020.10.07)



▶ ERD



▶ 보안관련

1. Google OTP

2 차 인증 수단으로써 사용하였다. Google OTP 는 시간 동기화 방식으로 TOTP(Time-Based One Time Password : OTP 를 생성하기 위해 사용하는 입력 값으로 시각을 사용하는 방식)이다. 서버와 사용자의 시간이 완전히 동일할 수는 없기 때문에 Google OTP 는 30 초 단위로 끊어서 사용한다. 필요한 라이브러리는 Apache Commons Codec 이다.

<진행 순서>

1. 서버는 Key 를 만들어 사용자에게 준다.
2. 사용자는 Google OTP 에 1 의 Key 를 등록한다.
3. 사용자는 Key 와 현재 시각을 섞어서 일회용 비밀번호를 만든다. (HMAC-SHA-1 알고리즘 사용)
4. 서버도 Key 와 현재 시각을 섞어서 일회용 비밀번호를 만든다. (HMAC-SHA-1 알고리즘 사용)
5. 서버는 3 와 4 의 비밀번호가 같은지 확인한다.
6. 5 의 결과에 따라 인증이 성공하거나 실패한다.

2. 보안 필터링

Naver Lucy XSS Filter : XSS 공격으로부터 웹 어플리케이션을 보호하기 위한 두 개의 방어 모듈로 구성된 오픈 소스 라이브러리. 화이트리스트 기반의 보안 정책을 따른다.

A) XssPreventer
apache-common-lang3 라이브러리를 사용하여 문자열에서 HTML 으로 인식될만한 요소를 제거한다.
(Ex : < → < , > → >)

B) XssFilter
Java 기반의 라이브러리.
HTML 요소를 허용하되 XSS 공격에 위험한 요소를 걸러내야 할 때 사용한다. HTML 이 허용되는 게시판의 본문 등에 적용 가능

필터링 전	필터링 후 (DB 저장 결과)
XSS	XSS
<img src="#" onerror="alert('XSS')">	<img src="#" onerror="alert('XSS')">

3. IP 차단

1 분마다 Apache2 의 access.log 를 분석하여 1000 개 이상의 로그가 있을 경우 공격으로 간주, 해당 IP 차단

차수	1 차	2 차	3 차	기준
결과	1345 개	1390 개	1317 개	1000 개 이상

A) Brute Force 툴로 생긴 로그의 개수 파악

→ "1 분에 1,000 개 이상"을 기준으로 삼았다.

B) route 명령어
리눅스에서 IP 차단 시 주로 사용되는 명령어는 route 와 iptables 가 있다. 둘의 차이가 있다면 route 는 실행한 곧바로 적용되지만, **iptables 는 차단/해제 시마다 데몬을 재가동** 시켜야 한다. 이러한 이유로 **route 명령어를 사용**해 주었다.

<진행 순서>

1. awk '{if($4 >= """$agoTime""" && $4 < """$nowTime"""){ print $1" "$7 }}' /var/log/apache2/access.log | sort | uniq -c | awk '{ if ($1 >= 1000){ print $2" "$3}}' > /home/lucidd831/ip/prac/testsearch.temp
→ access.log 에서 같은 IP 주소가 1,000 개 이상 발견된다면 testsearch.temp 파일에 저장

2. awk '{print "route add -host "$1" reject"}' /home/lucidd831/ip/prac/testsearch.temp > /home/lucidd831/ip/prac/testinput_iptable.sh
→ 1 번 과정에서 저장된 IP 주소를 차단하는 명령어 만들어줌.

3. sh /home/lucidd831/ip/prac/testinput_iptable.sh
→ IP 차단 명령어 실행

4. **DB 에 IP 주소와 공격 payload 삽입.**