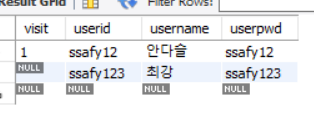
1. 제목 : 알고리즘적용기획서 #2
2. 내용 : 카이사르 암호화 알고리즘을 이용한 패스워드 암호화
3. 적용 알고리즘 : 카이사르 암호화 알고리즘
4. 알고리즘 개요 :

카이사르 암호화 알고리즘을 활용한 패스워드 암호화는 DB에 있는 개인 정보를 노출하지 않도록 하기 위한 보안 강화 서비스이다.

현재 사용자 정보 DB => 패스워드 값 노출 위험



- 패스워드가 문자열로 되어있을 경우 -> 암호화를 할때 현재 문자를 다음 문자 값으로 변환한다.

a b c d e f

b c d e f g

a -> b

b - > c

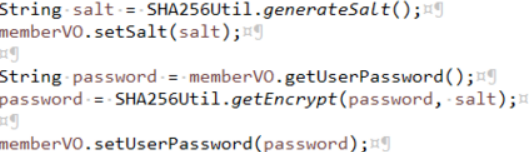
c -> d

가나다라

-> 나다라마

- 패스워드를 가져와서 위의 경우와 반대로 복호화 알고리즘을 실행한다.

1. 적용 서비스 : 패스워드 보안 강화
2. 적용 서비스 개발 개요

1) 회원가입을 할 때 비밀번호를 받아 암호화 한다.  
- 암호화 할 때 짝을 이루는 난수를 발생시켜 암호화에 이용한다. 이 난수를 일컬어 Salt라 한다.  
- DB에 암호화된 비밀번호와 Salt 값을 저장한다.  


2) 로그인할 때 ID에 맞는 Salt 가져온다.  
  
3) 입력한 Password와 Salt를 통해 암호화 시킨 값을 비밀번호로 해 쿼리문을 수행한다.