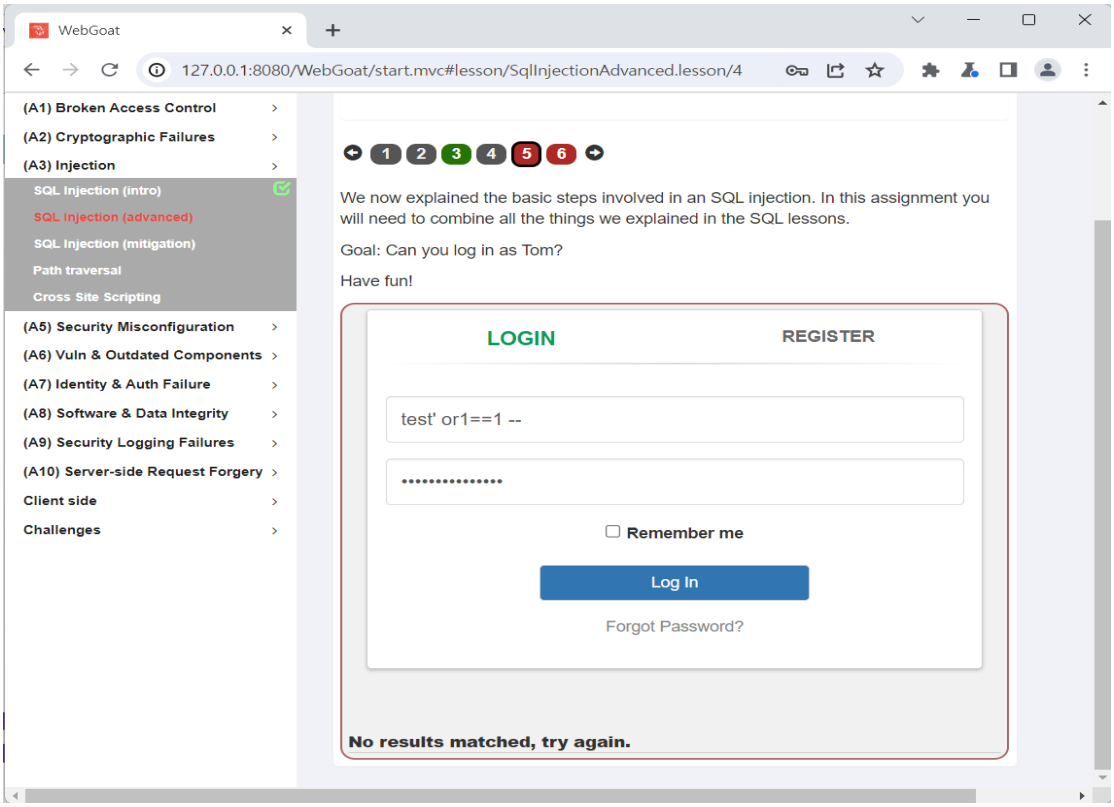
인터넷응용보안 7주차 과제

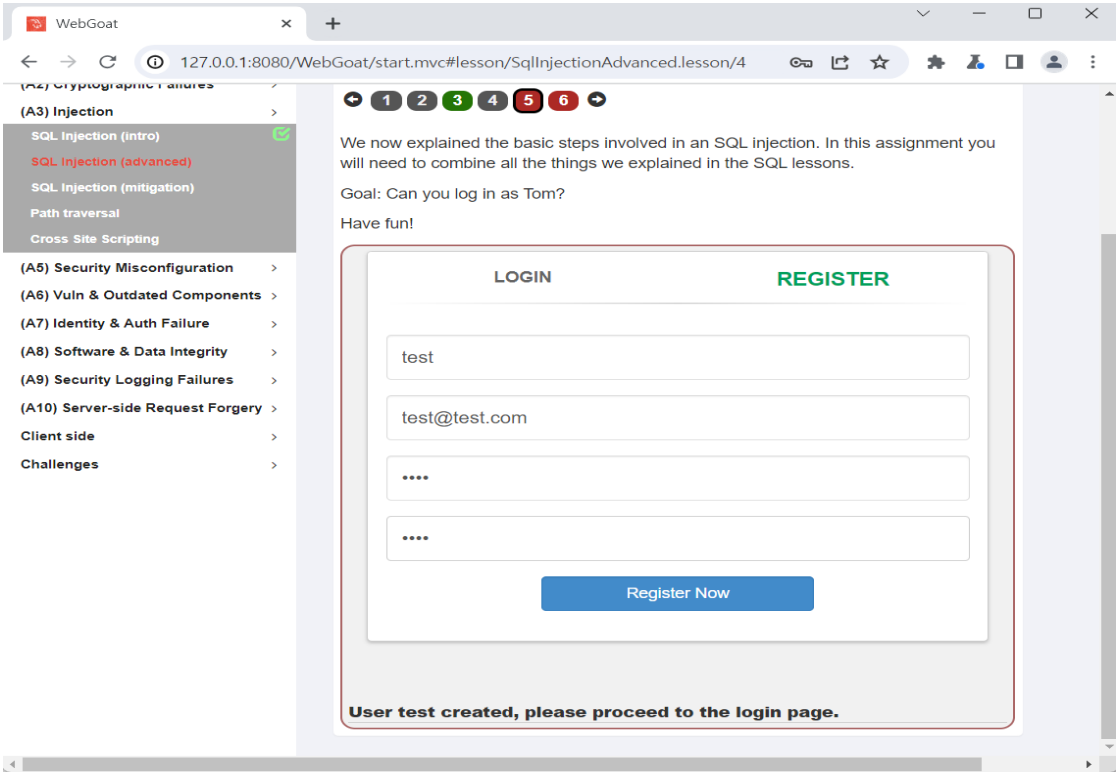
202121556 곽지현

Blind SQL Injection 문제

test' or1==1 – 공격문을 id 입력창이나 패스워드 입력창에 넣어봐도 모두 실패

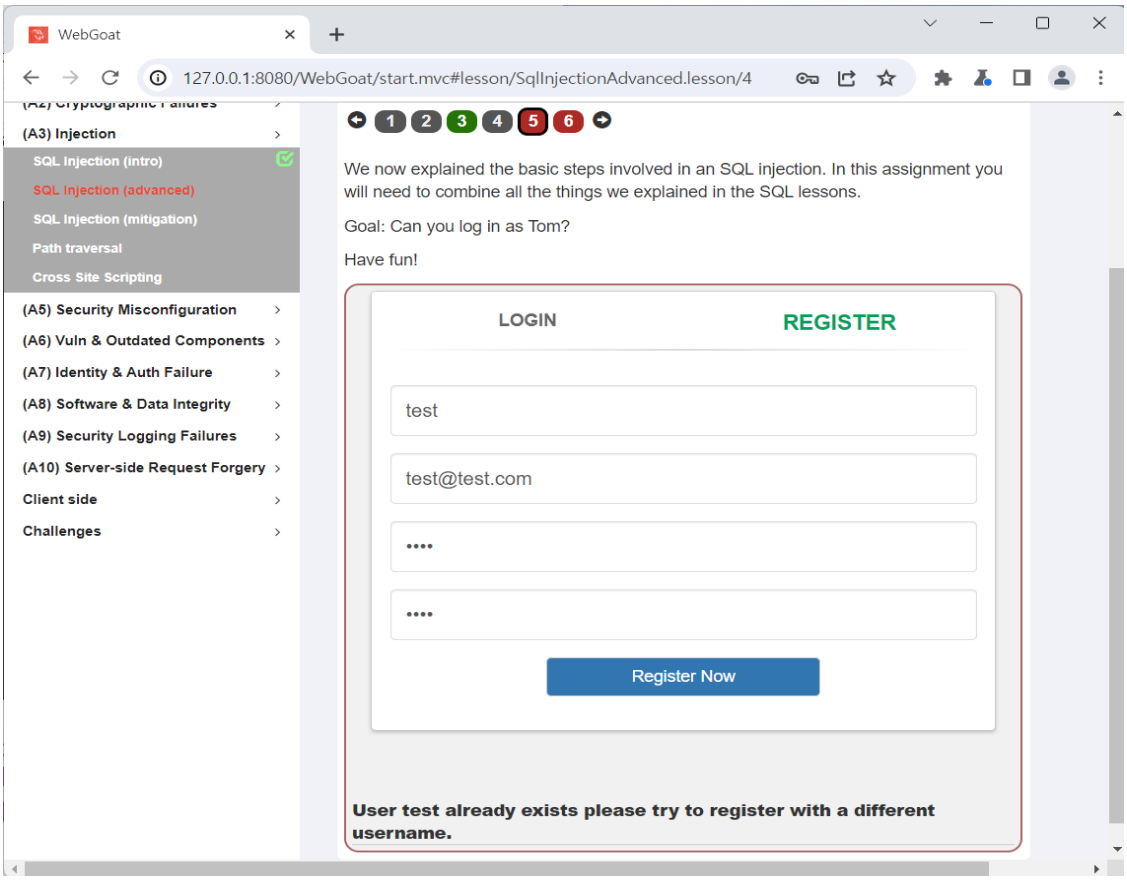


REGISTER 메뉴로 가서 임의의 계정(test)을 등록

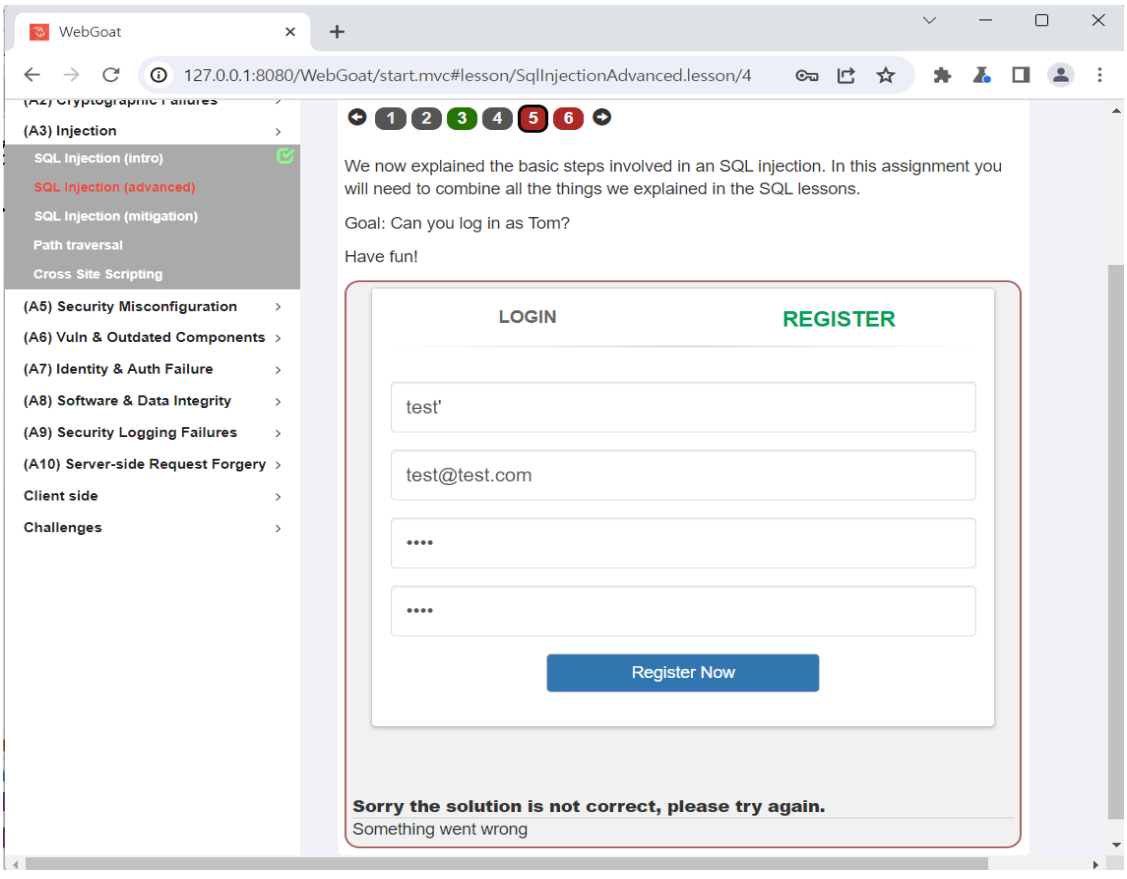


다시 동일한 id로 중복 가입을 시도 -> 이미 존재하는 계정이라고 나온다.

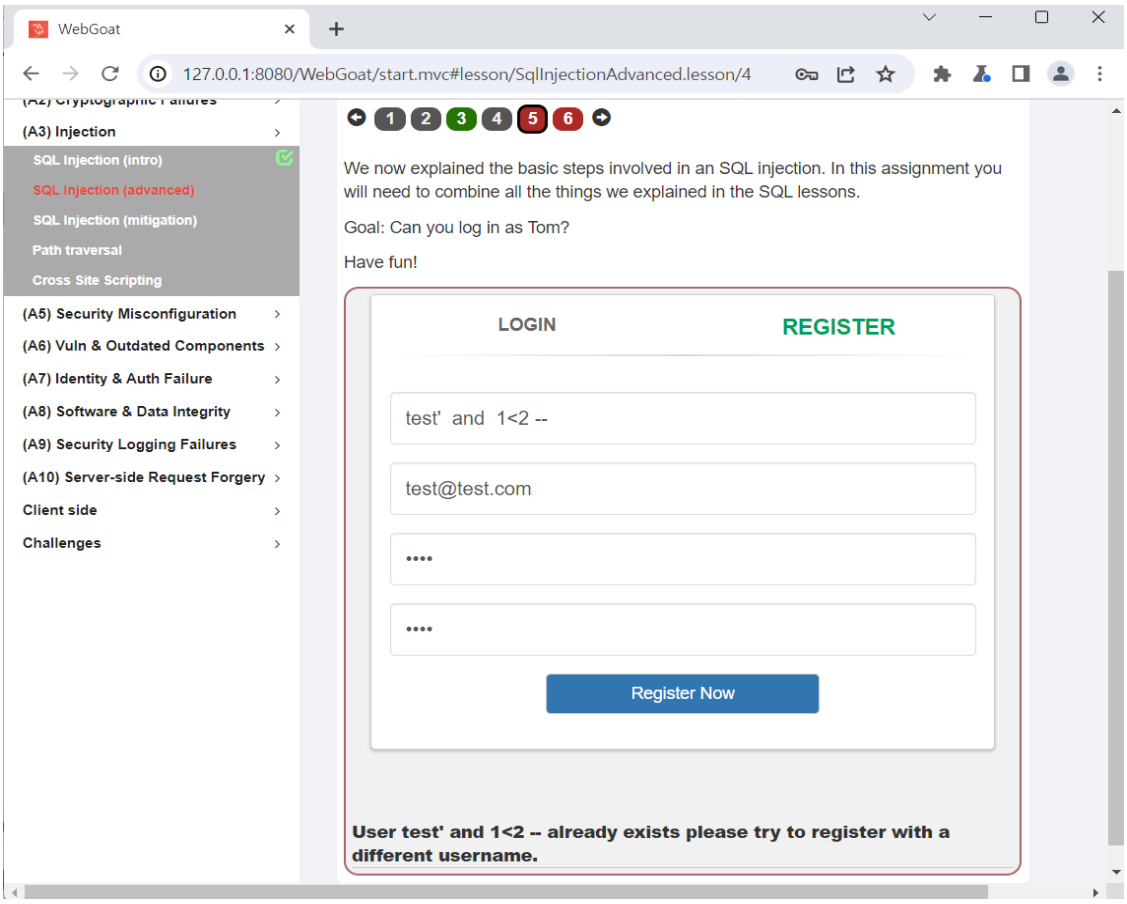
(계정명을 DB에 조회하고 있음)



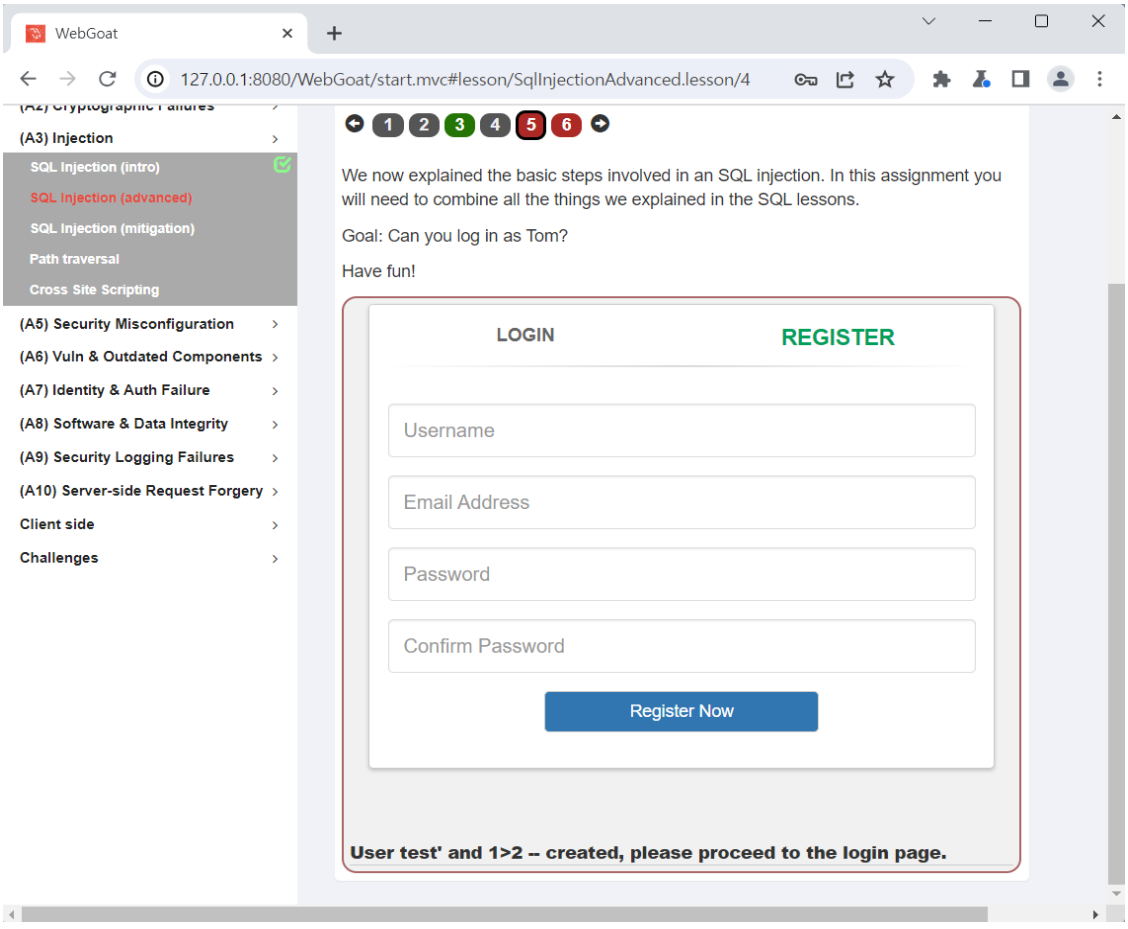
계정명을 test' 로 변경하여 공격 -> 내부에서 오류가 발생 (취약점 존재)



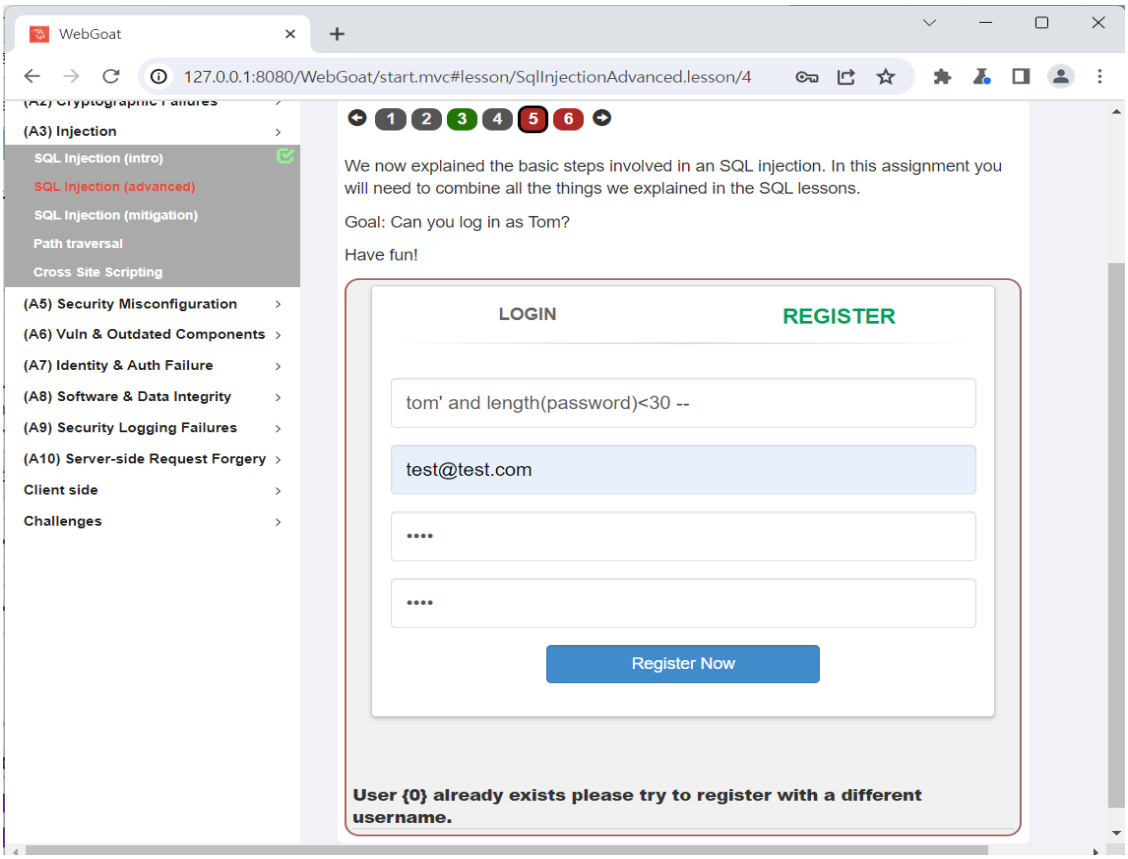
계정명에 test' and 1<2 -- 를 입력하여 공격 -> 계정이 이미 존재 (Blind SQL 삽입 공격이 적용됨)



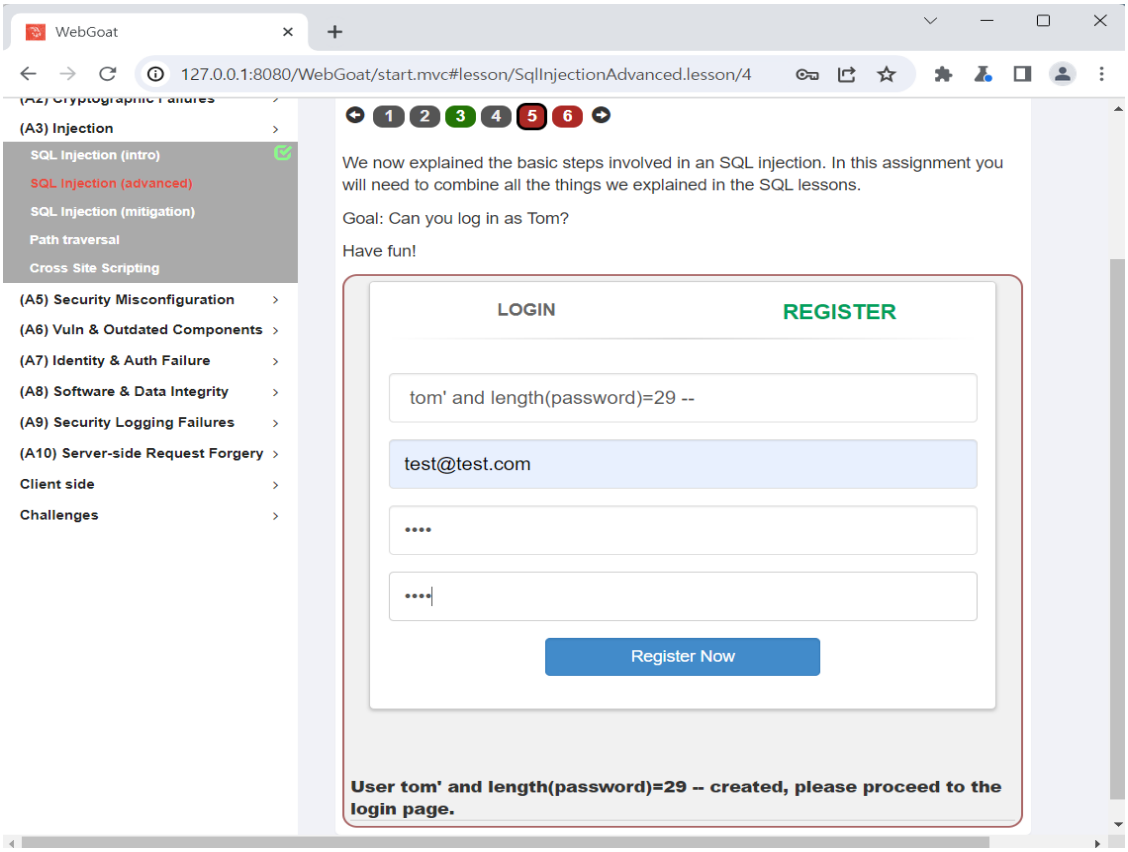
계정명에 test' and 1>2 -- 를 입력하여 공격 -> 계정이 만들어졌다고 나온다.



tom' and length(password)<30 -- 이라고 공격 -> password의 길이가 30보다 작다는 명제가 참 임을 알 수 있다.

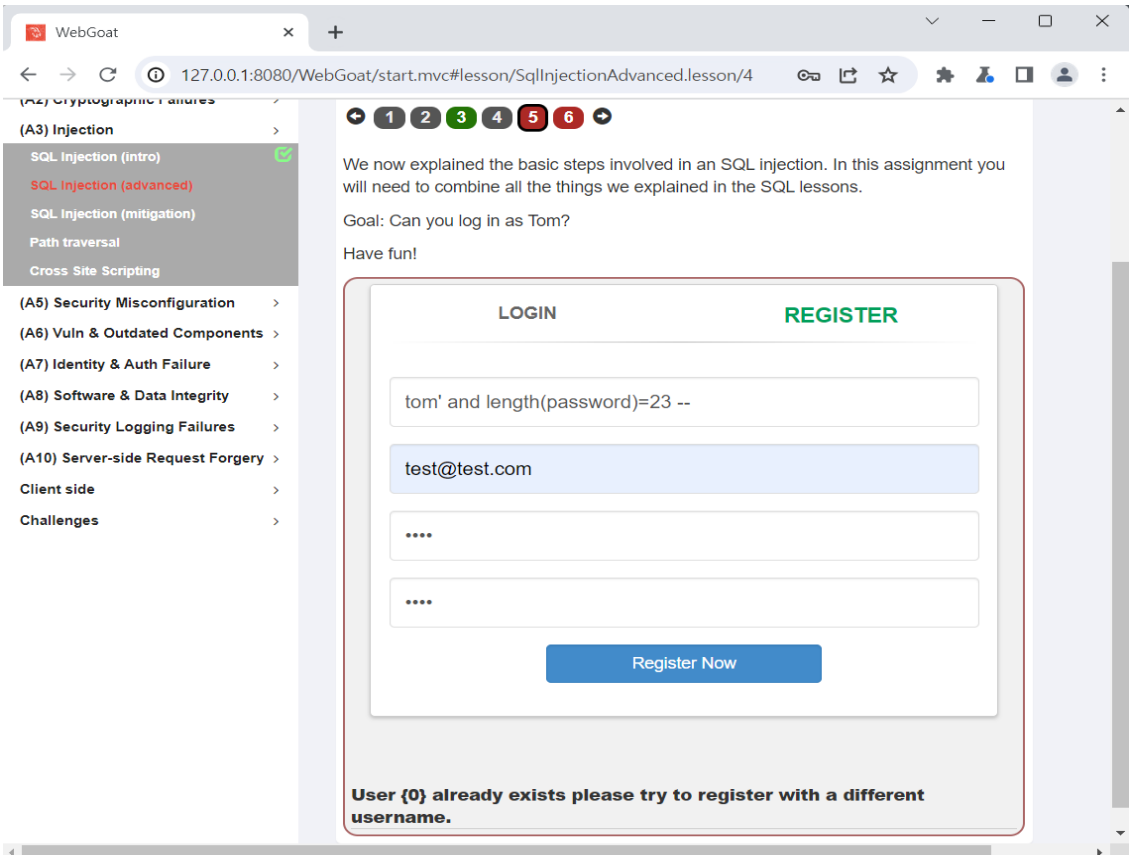


tom' and length(password)=29 -- 라고 공격 -> 계정이 생성되었다는 메시지가 나옴 -> 거짓 (패스워드 길이 29 아님)



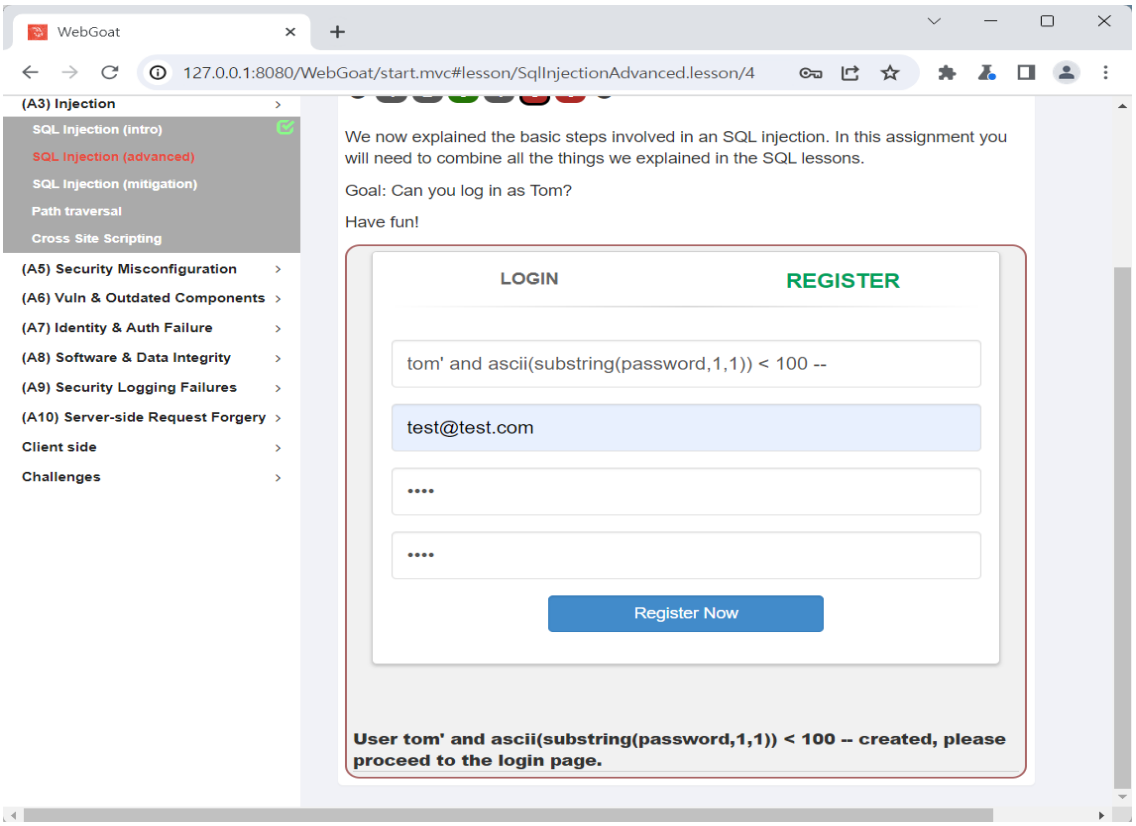
패스워드 길이를 하나씩 줄여 나가기 -> 패스워드 길이가 23일 때 계정이 존재한다는 메시지가 출력

(Tom의 패스워드 길이 : 23)

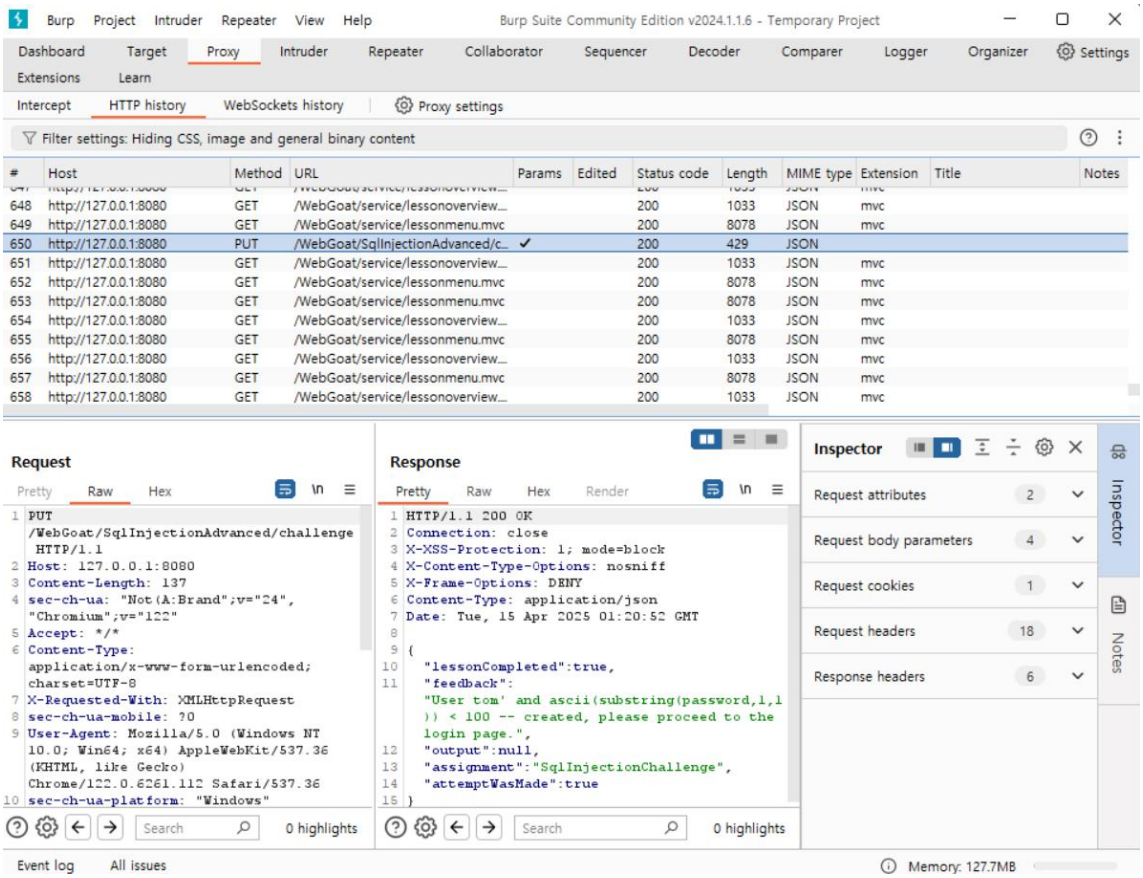


tom' and ascii(substring(password,1,1)) < 100 – 이라고 공격 -> 계정이 생성됨

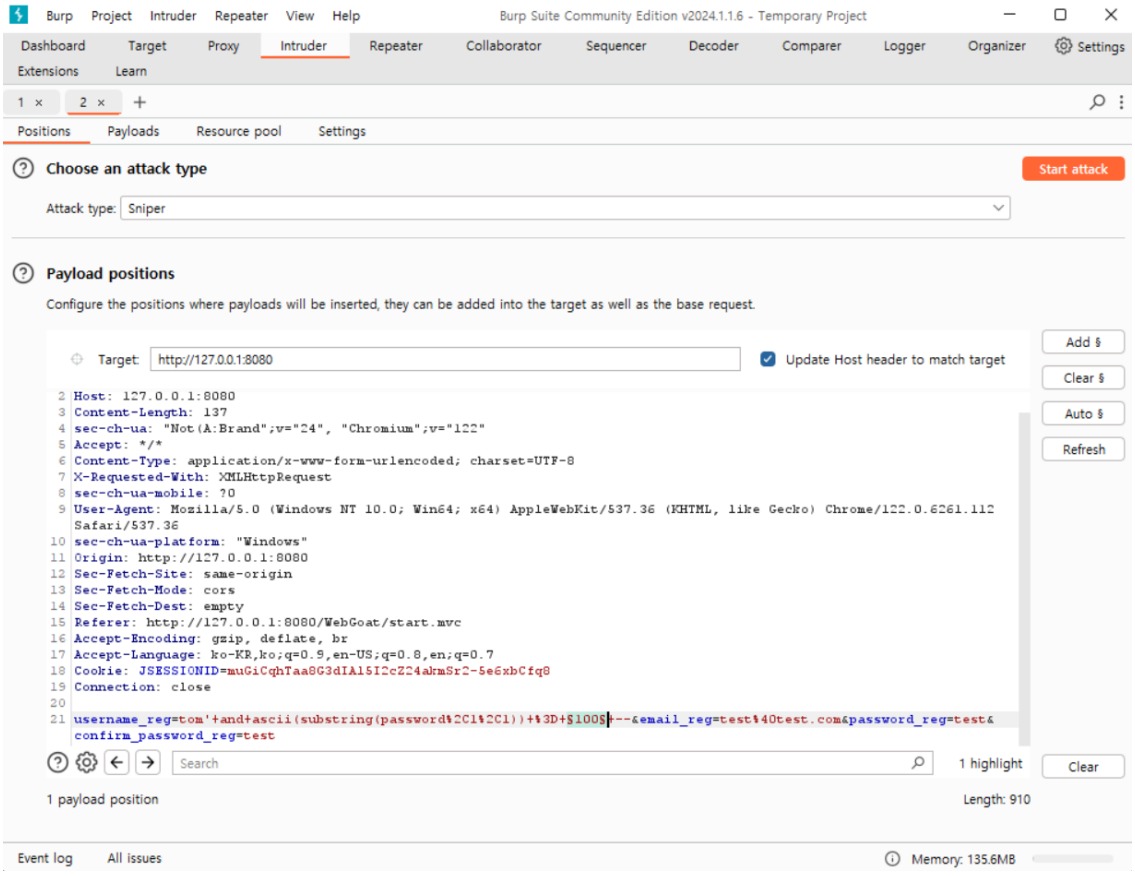
and 뒷부분이 거짓 -> 패스워드의 첫 글자가 ASCII 코드로 100 이상의 값



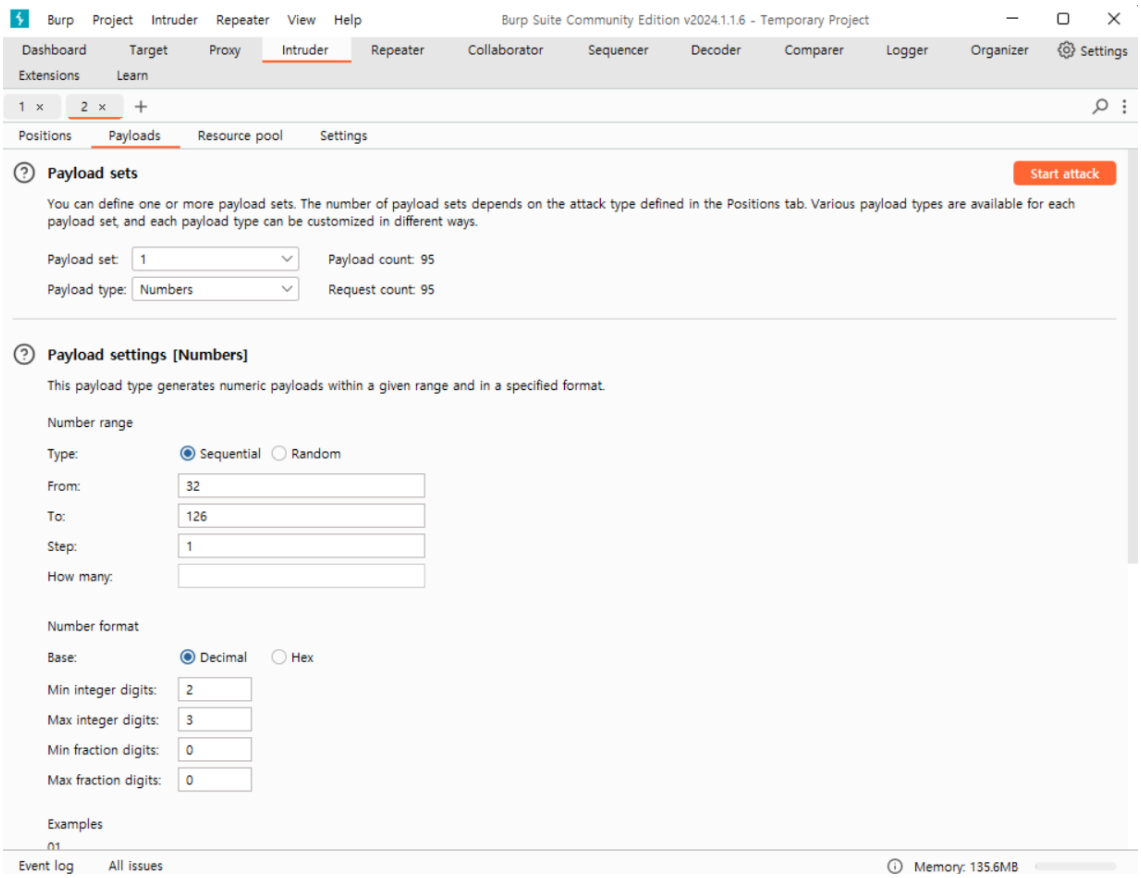
HTTP history에서 이 요청을 찾아 Send to Intruder 메뉴 클릭



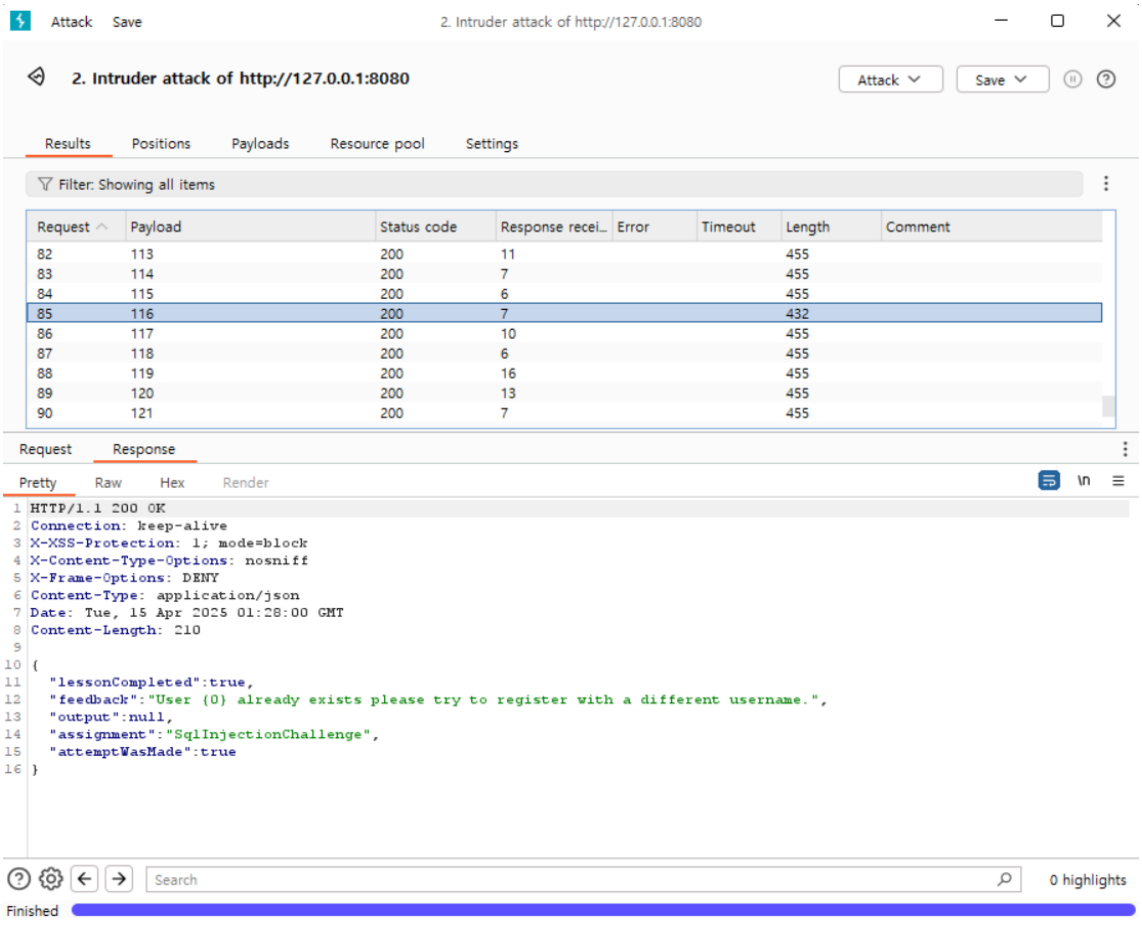
%3C -> %3D 로 수정 / 100 -> 100 형태로 수정



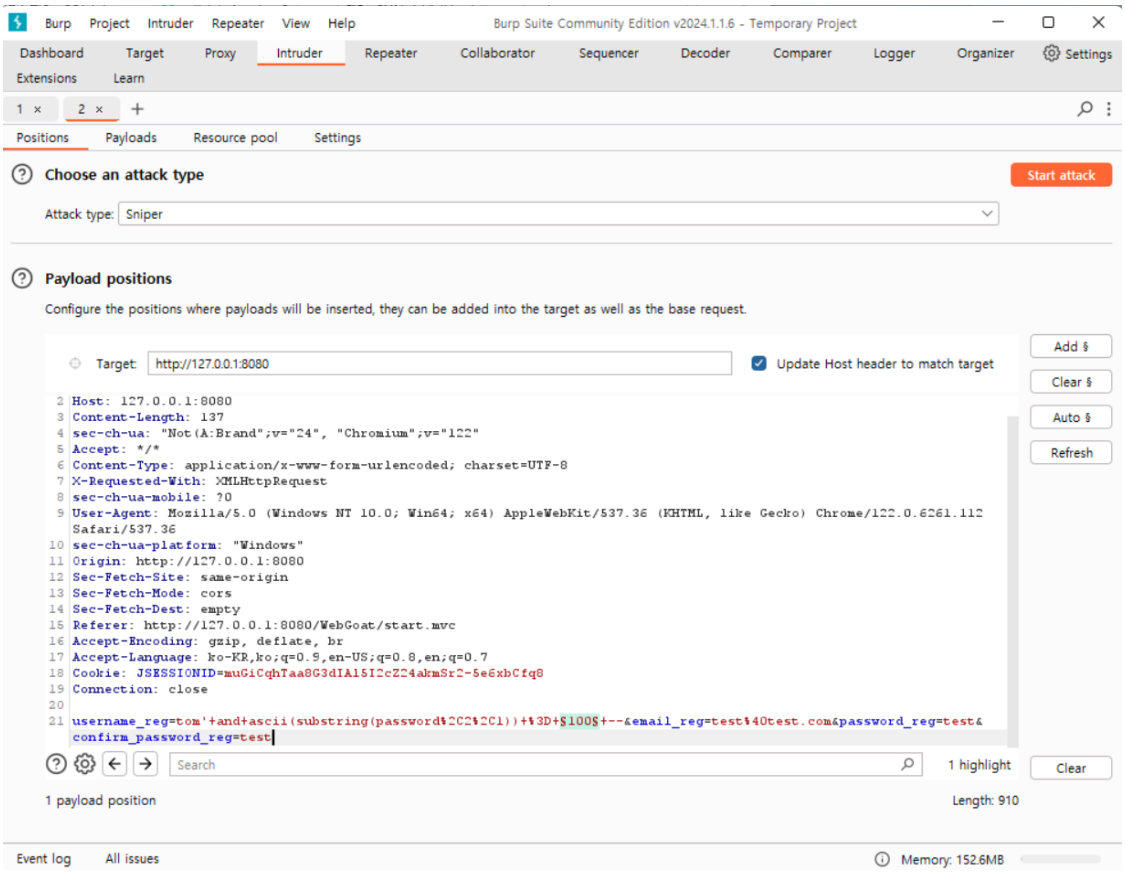
Payload 설정하고 공격



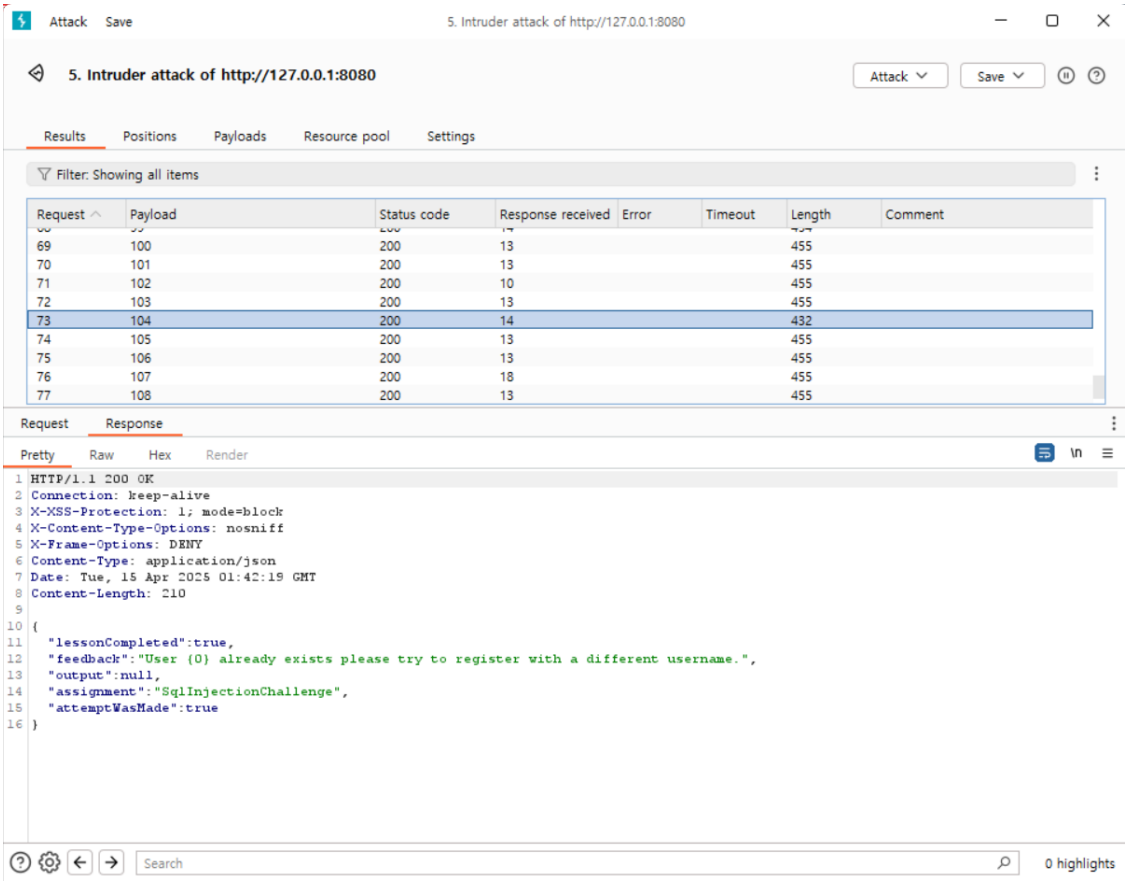
공격에 대한 Response를 살펴보면 응답 길이가 다른 요청과 다른 것이 116 값일 때 계정이 만들어졌다는 메시지가 나온다. (패스워드의 첫 글자 : ASCII 코드 116, 소문자 t)



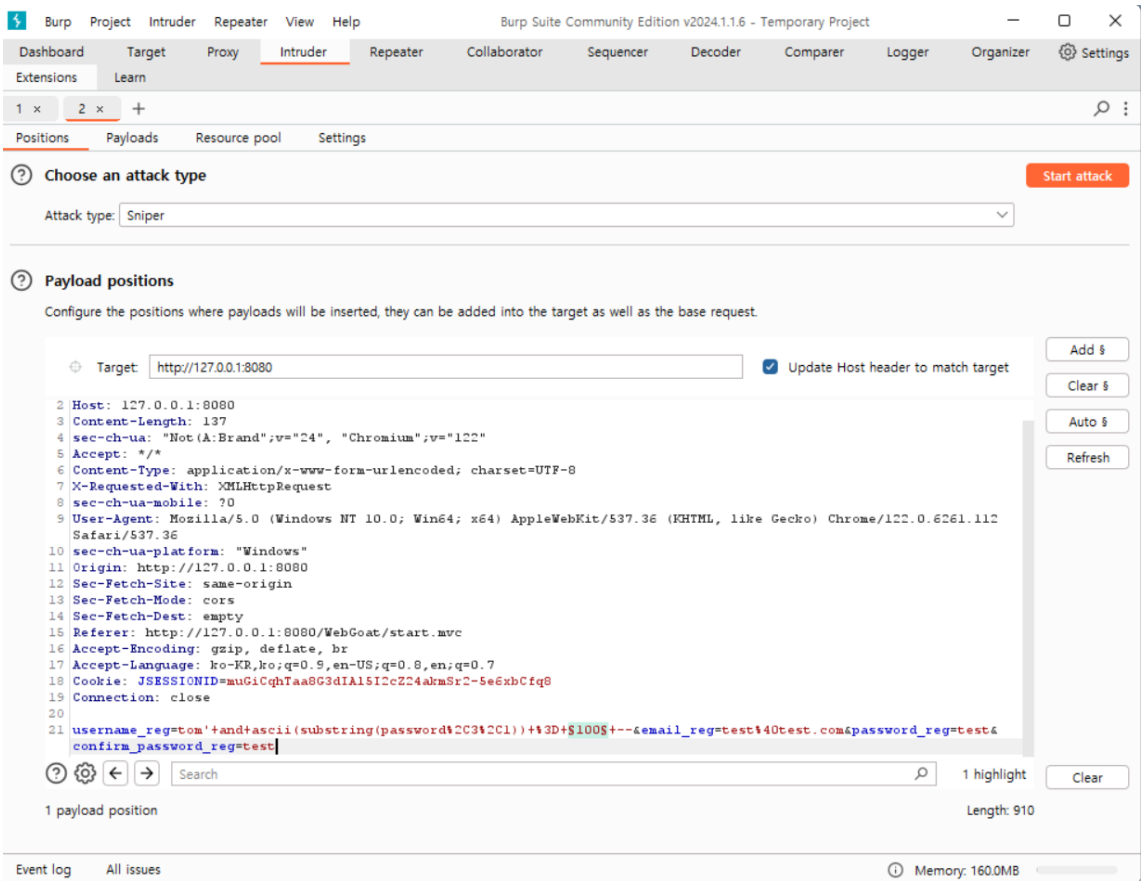
Position 탭에서 substring(password%2C1%2C1) -> substring(password%2C2%2C1) 로 수정



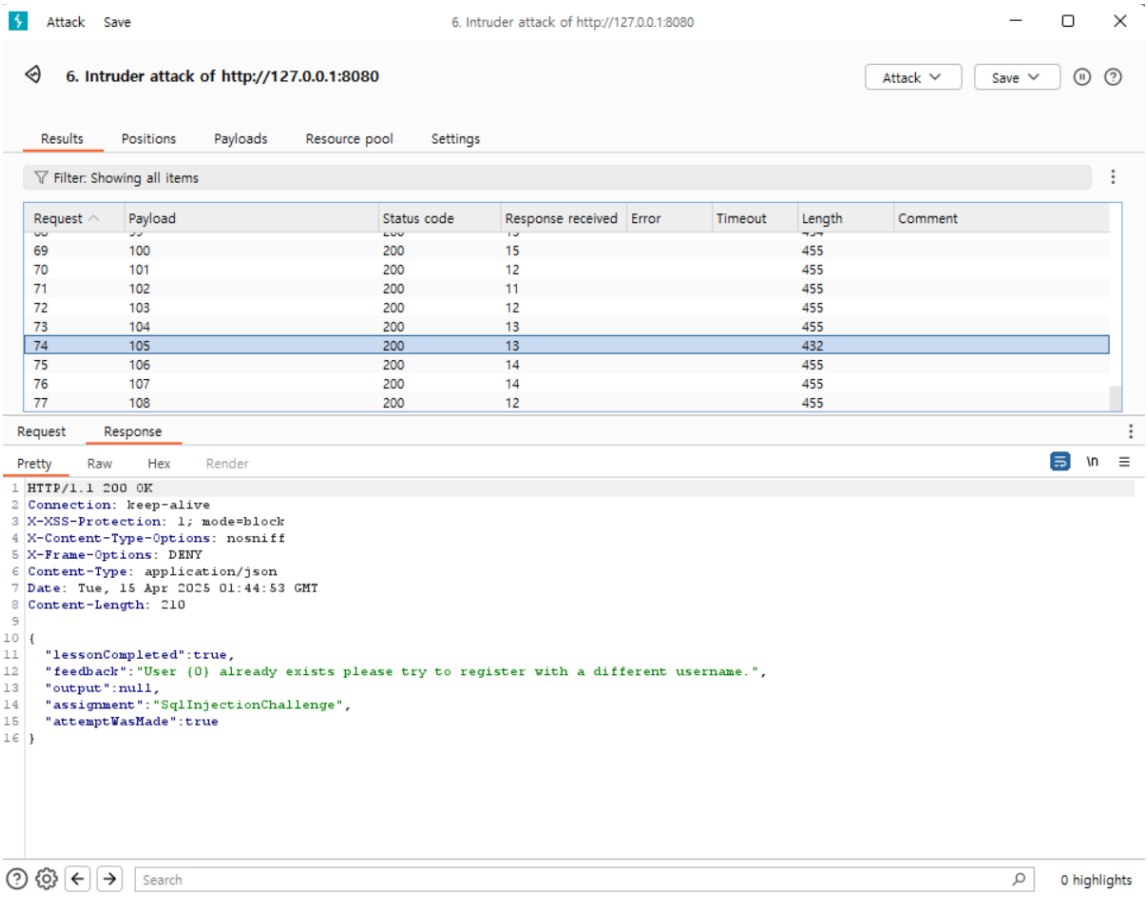
공격에 대한 Response를 살펴보면 응답 길이가 다른 요청과 다른 것이 104 값일 때 계정이 만들어졌다는 메시지가 나온다. (패스워드의 첫 글자 : ASCII 코드 104, 소문자 h)



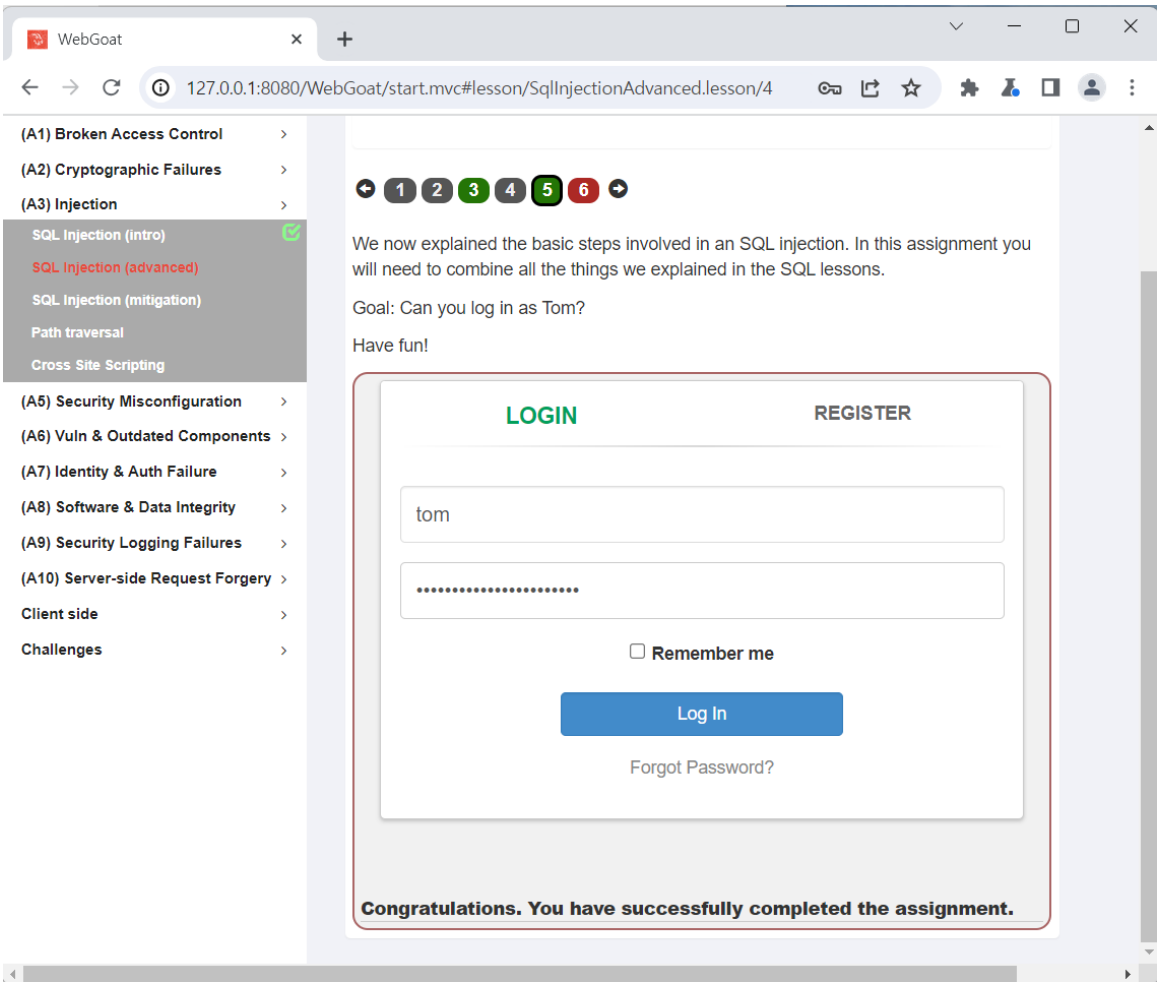
Position 탭에서 substring(password%2C2%2C1) -> substring(password%2C3%2C1) 로 수정



공격에 대한 Response를 살펴보면 응답 길이가 다른 요청과 다른 것이 105 값일 때 계정이 만들어졌다는 메시지가 나온다. (패스워드의 첫 글자 : ASCII 코드 105, 소문자 i)



Tom의 패스워드 : thisisasecretfortomonly



모든 문제 성공!