**2018.05.08 제 3차 보고서 SQL INJECTION이란?**

**탐구 분야** : SQL INJECTION 정의, 종류 및 기법

**탐구자** : 신정희

**날짜** : 2018.04.20 금

**탐구 내용** :

**SQL (Structured Query Language Injection**) :  데이터를 관리하기 위해 설계된 특수 목적의 프로그래밍 언어

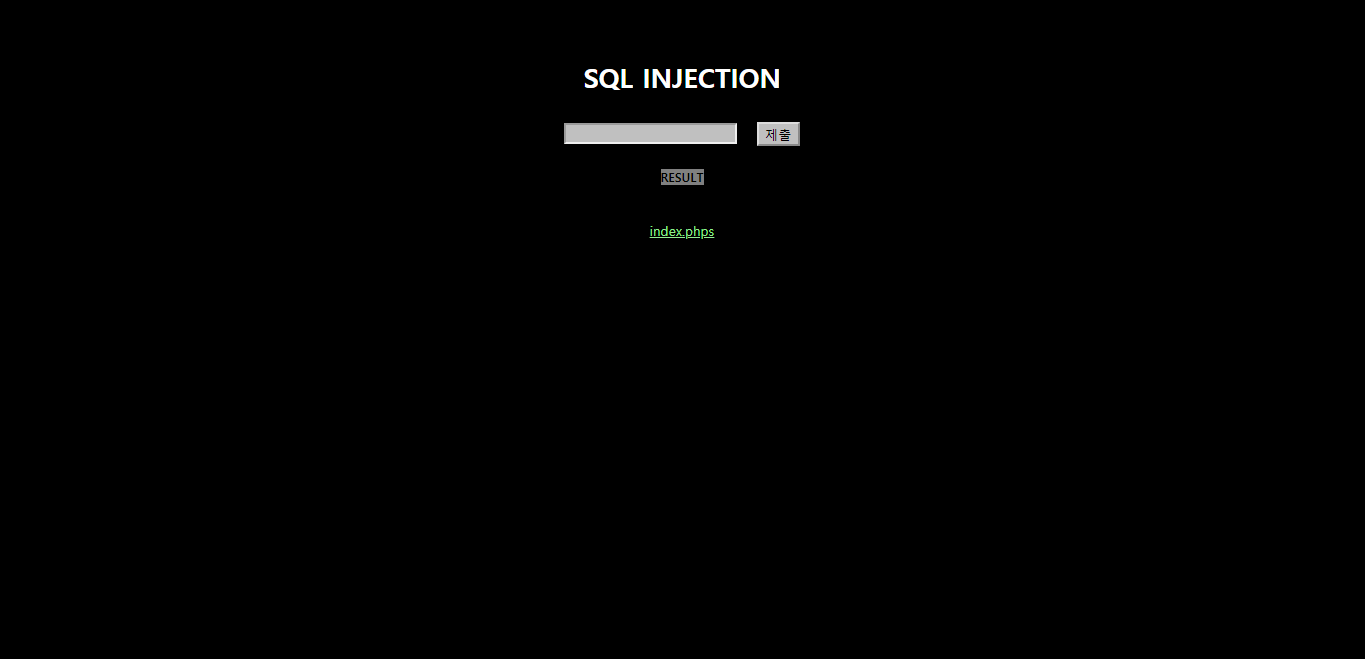
**SQL INJECTION** : 보안 상의 허점을 의도적으로 이용해, 악의적인 **SQL**문을 실행되게 함으로써 데이터베이스를 비정상적으로 조작하는 코드 **인젝션** 공격 방법이다.

**SQL INJECTION 종류**

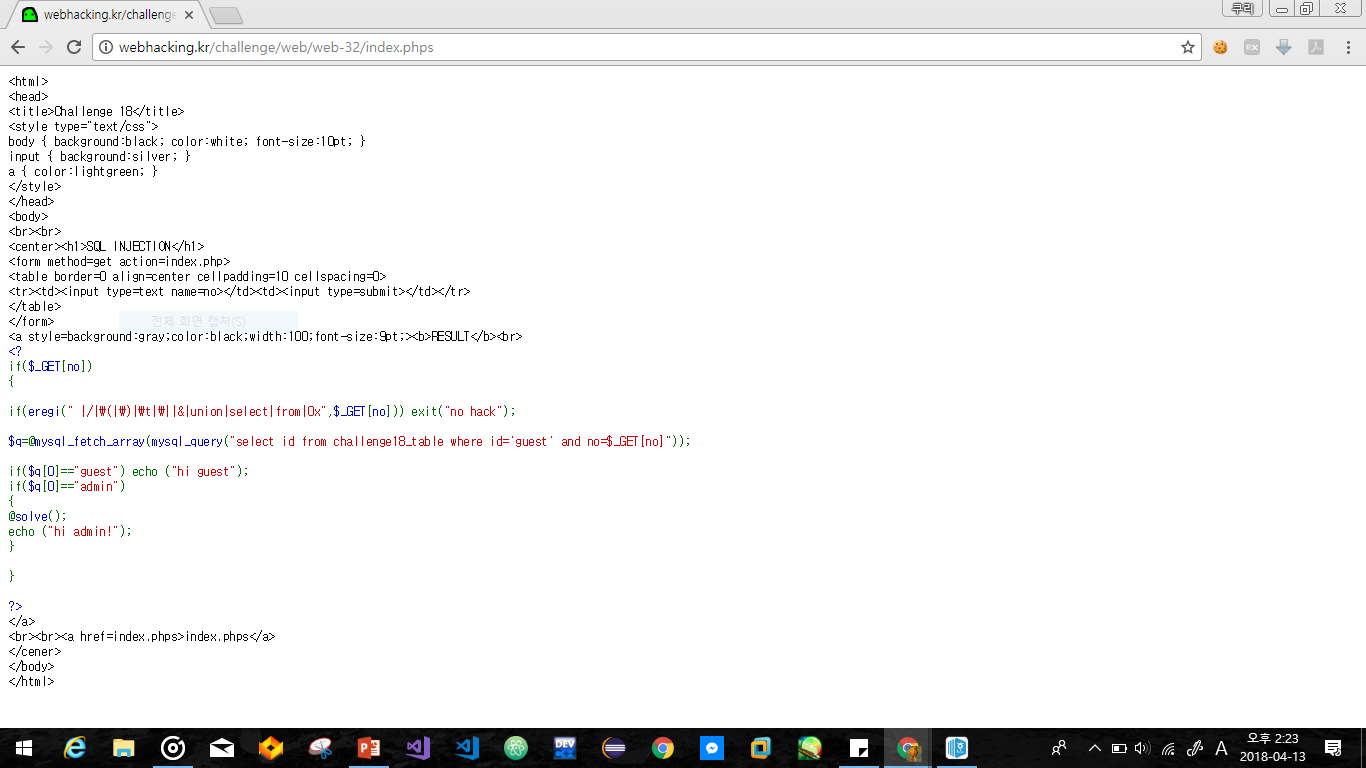
* SQL Injection : 논리적 에러 이용
* Blind SQL Injection : 참 거짓 no = 0 and 1=1
* Union SQL Injection : 2개 이상의 쿼리 이용
* Stored Procedure SQL Injection : 저장되어 있는 sql 이용

**Web hacking no.18 풀이**

1. 18번 문제의 첫 화면이다. SQL Injection 문제라고 명시되어 있다.



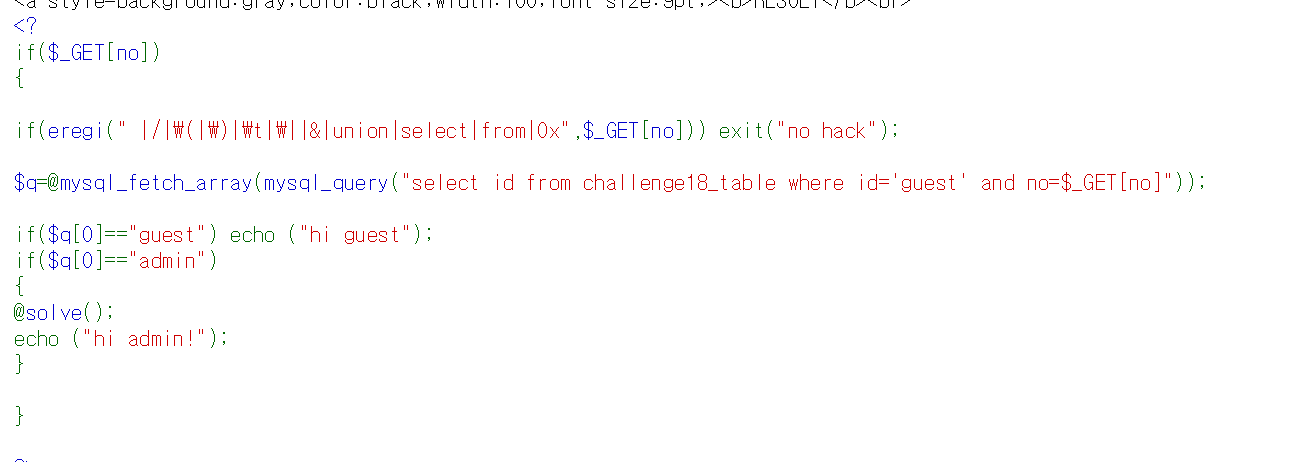
1. Index.phps 열기



1. Eregi로 묶인 문자들을 입력할 시 no hack가 출력된다.

get형식으로 받아오는 no의 값이 guest라면 hi guest를 출력한다.

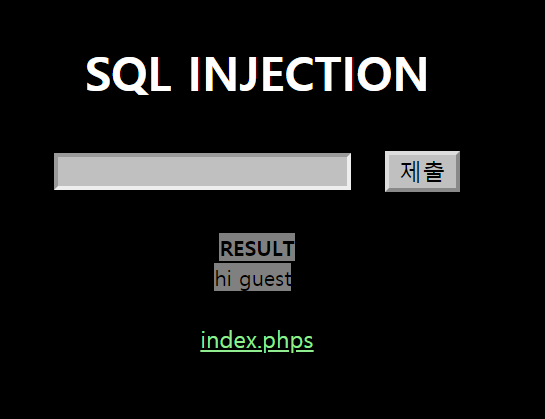
만약 no의 값이 admin이라면 성공이다.

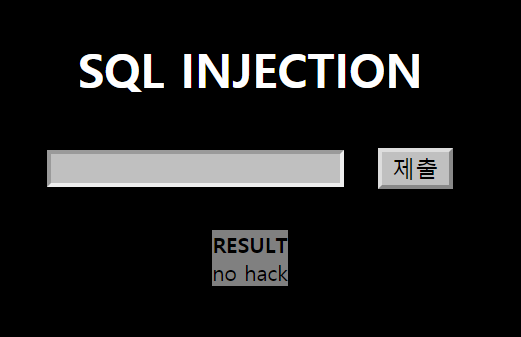


1. 숫자를 입력하여 대응하는 값을 찾아본다.

1을 입력하면 hi guest가 출력된다. 즉 1은 guest라는 소리이다.

그럼 admin의 값은 0이나 2일 것이라고 추측할 수 있다.





1. 0보다는 2일 가능성이 높기 때문에 no = 2를 입력한다.

No=0 or no = 2를 입력하여, 맨 처음 no =0 은 참이 아니기 때문에 뒤의 연산 no=2를 수행한다는 것을 이용한다.

이때 or 주위에 공백을 만들어주어야 하는데, eregi 함수에 의해 필터링 됨으로 %0a로 우회한다.

No=0%0aor%0ano=2 를 입력하면 문제는 풀린다

**알게 된 점**

: SQL Injection 분야에 대해선 그리 공부한 것이 많지 않다. 너무 아는 것이 없다고 생각하여, 일부러 이 분야를 택하여 공부하기로 결심했으나, 조금 밖에 못 한 것 같다.

사실 이 문제 역시 전에 풀어본 적이 있다. 다만 저번에 풀어볼 때는 풀이를 보고 풀었다면, 이번에는 스스로 이해해서 풀었다는 점이 달라진 점이라 할 수 있는 것 같다.

전에는 잘 이해하지 못했던, sql의 작동 원리 및 sql의 정의에 대해서 알 수 있었다.