

다음과 같이 BLIND SQL INJECTION 이라는 문구와 함께 쿼리 전송 폼이 보인다.  
BLIND SQL INJECTION으로 풀어보자.

## BLIND SQL INJECTION

select를 이용해 blind sql injection을 하니 from을 필터링하여 no hack이라는 문구가 뜨고 쿼리문이 실행되지 않는다.

## BLIND SQL INJECTION

no hack

select 문이 안되므로 컬럼을 이용해서 다음과 같이 블라인드 인젝션을 했다.  
`http://webhacking.kr/challenge/bonus/bonus-1/index.php?no=2 and ascii(substr(pw,1,1))>0`

위와 같이 인젝션을 하면 blindsqliinjectionkk 라는 문장을 얻게 되고 인증에 성공했다.