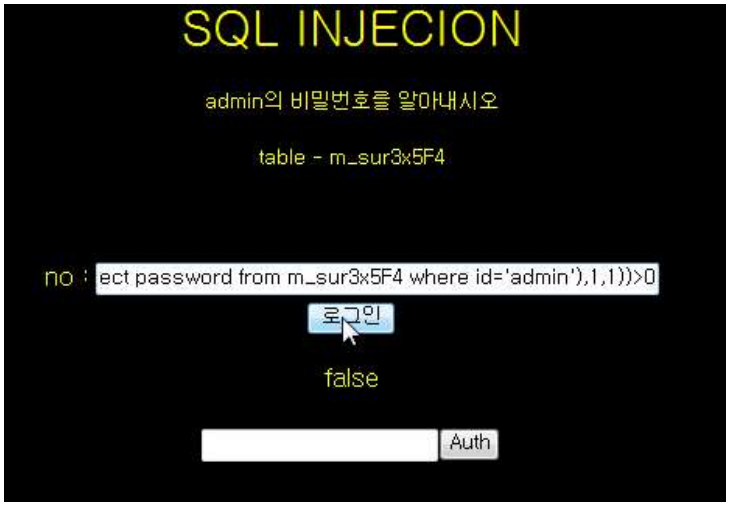
webhacking.pe.kr 8번문제

B1ackZer0
2011.03.21

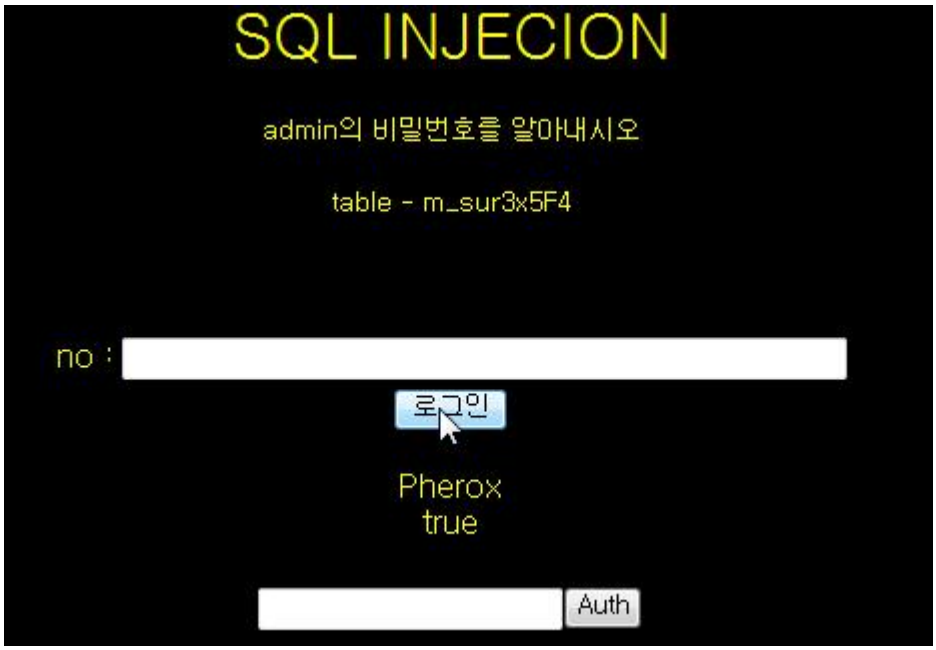
SQL injection이라고한다.
table은 m_sur3x5F4이고, 필드명은 게싱해야 한다.

1 and ascii(substr((select password from m_sur3x5F4 where id='admin'),1,1))>0
위의 쿼리문을 설명하자면,
우선 password라는 필드명을 게싱으로 알아냈고, id도 게싱으로 알아냈다.
m_sur3x5F4테이블의 'admin'인 아이디의 비밀번호의 첫글자가 0보다 크면, 즉 존재하면(NULL은 아스키코드로 0이니깐)true가 나타나게 된다.
no에 1인것은 true일테고, and로 뒤의 쿼리문이 맞으면 true and true로 true값이 출력되는 것을 이용한게 블라인드 인젝션이다.
즉, 좋게 말해 게싱, 안 좋게 말해 노가다를 뛰는 것이다.

한번 쿼리문을 입력해서 확인해보자.



true!!! 게싱에 성공했다.



그렇다면

1 and ascii(substr((select password from m_sur3x5F4 where id='admin'),1,1))<120

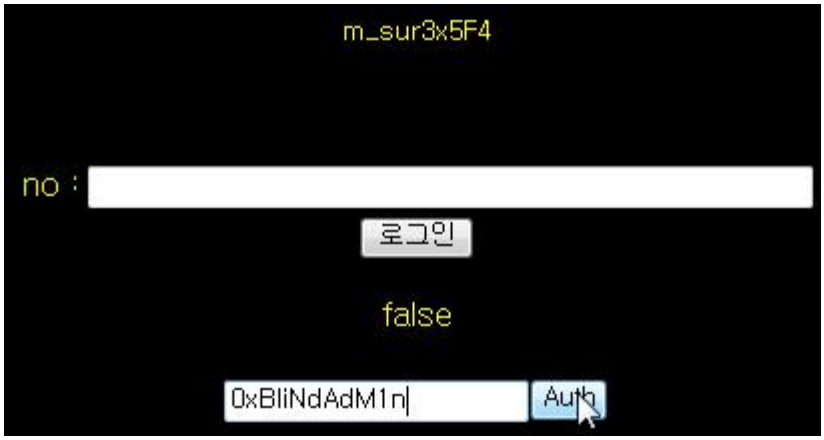
이렇게 값을 바꿔가며 하나하나 찾으면 된다.

※ ascii()와 substr()을 검색해보면 좋다.

그렇게 노가다를 뛰며 값을 찾으면, 48,120,66,108,105,78,100,65,100,77,49,110 이라는 비밀번호를 얻을 수 잇다.

ascii라고 가정하에 변환해보면, 0xBliNdAdM1n 이 나온다.

이것을 밑의 auth에 인증해보자.



auth에 성공했고, 진짜 패스워드를 알아내었다.