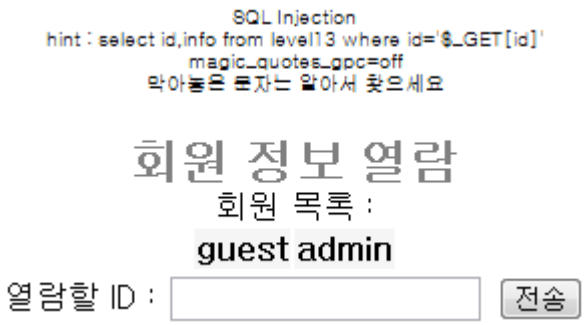
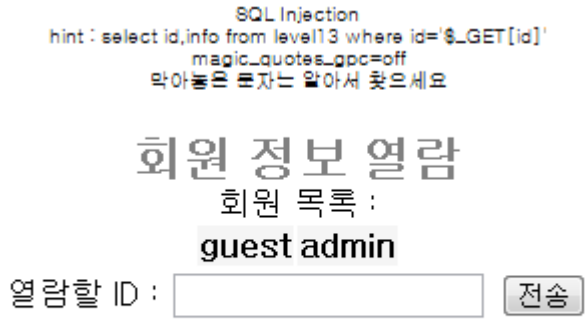
webhack.teamtmp 13 번문제

Xero
박준혁 (한국디지털미디어고등학교 2 학년)
2012-06-18
wnsgurzxc@nate.com

다음과 같이 소스가 보인다.



열람한 ID 에 guest 를 입력하면 다음과 같이 this is guest id 라고 출력된다.

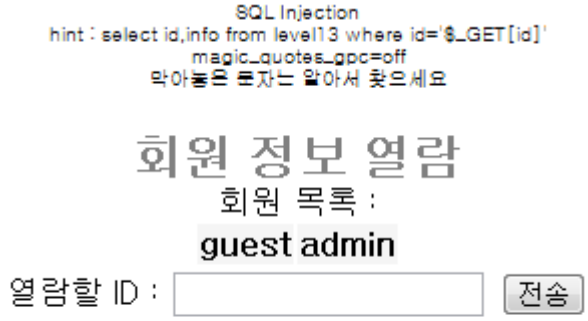


admin 아이디를 열람하면 답이 출력될 것이다.
열람할 ID 에 admin 을 입력하면 필터링은 되지 않지만 access denied 라고 출력되고 답이 나오지 않는다.
다른 SQL 구문을 이용해 admin 아이디를 열람해야 한다.
Like 명령어를 이용해 admin 아이디를 열람하기로 했다.
' || id like '%a% 를 입력하면 SQL 구문이 다음과 같이 될 것이다.
select id, info from level13 where id='' || id like '%a%'

하지만 공백을 필터링하므로 %0a (줄바꿈 문자)로 우회한다.
그리고 %를 %25 로 url 인코딩 한 값으로 바꾼다.
그러면 입력할 값이 다음과 같게 된다.
'%0a||%0aid%0alike%0a'%25a%25

위의 값을 주소에 입력하면 주소는 다음과 같이 된다.
http://webhack.teamtmp.org/level13/index.php?id='%0a||%0aid%0alike%0a'%25a%25

위의 주소로 들어가면 다음과 같이 답이 출력된다.



PW : this_is_medium1eve1_SQL1njecti0n

Key : this_is_medium1eve1_SQL1njecti0n