webhack.teamtmp 14 번문제

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

다음과 같이 소스가 주어진다.

SQL Injection
hint : select m_idx,m_id,m_point from m__member where m_idx=$num
if(@eregi('48',$_GET[num])) exit('no hack'); // admin의 m_idx는 48

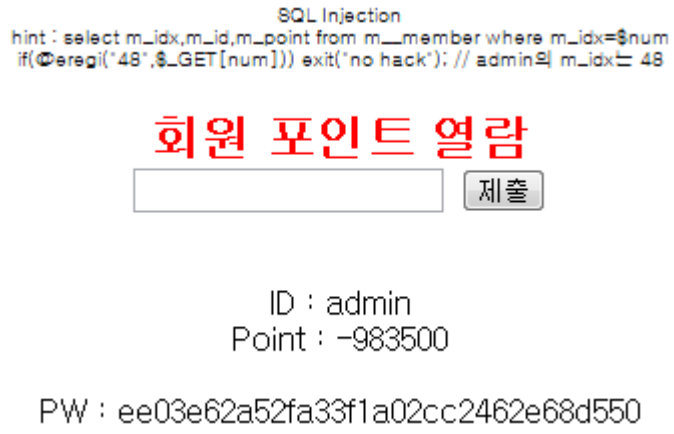
회원 포인트 열람

제출

ID :
Point :

입력받은 값이 48 이 되면 admin 의 정보를 출력하고 답을 출력한다.
48 을 필터링하고, +, - 등 여러 연산들을 필터링했다.
그러다 &는 필터링하지 않는 것을 발견하고 &연산자를 이용해 48 을 우회하기로 했다.

48 은 2 진수로 나타내면 110000 이다.
111100 과 110011 을 &연산자로 110000 으로 만들어 우회하기로 했다.
그래서 60&51 를 입력하니 다음과 같이 답이 출력되었다.



Key : ee03e62a52fa33f1a02cc2462e68d550