LOS 풀이 문서

이진하

문제 4번



올바른 pw를 입력하면 문제를 풀 수 있다.

[풀이]

if(($result['pw']) && ($result['pw'] == $\_GET['pw'])) solve("orc"); 부분을 보면 이전 문제처럼 id, pw를 참으로 만든다고 문제를 clear할 수 있는 게 아니라 정확한 pw 값을 입력해야만 해결 가능하다. 이를 위해서는 pw의 길이, pw의 값을 알아야 한다.

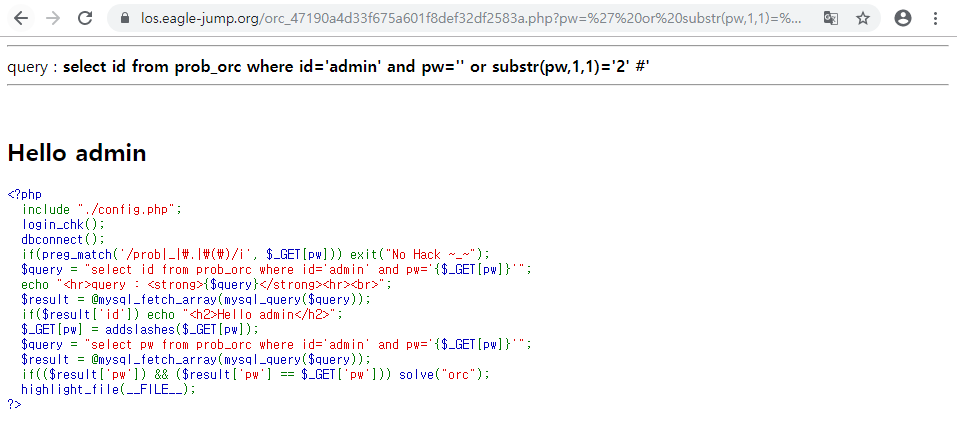
먼저 pw의 길이를 알기 위해 ?pw=%27%20or%20length(pw)%20=@20%23의 @ 부분의 숫자를 하나씩 증가시키면서 길이를 찾았다.



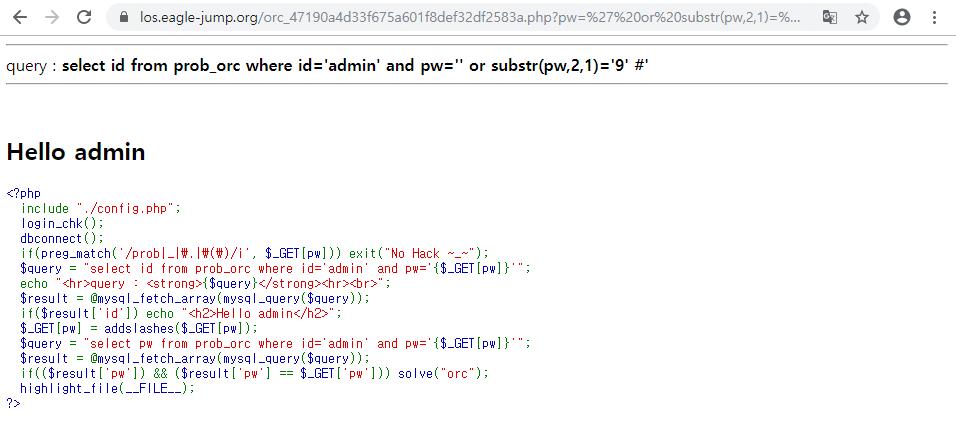
위와 같이 pw는 8자리임을 알 수 있다.

그리고 substr을 이용해 pw의 각 자리의 값을 알아보려고 했다.

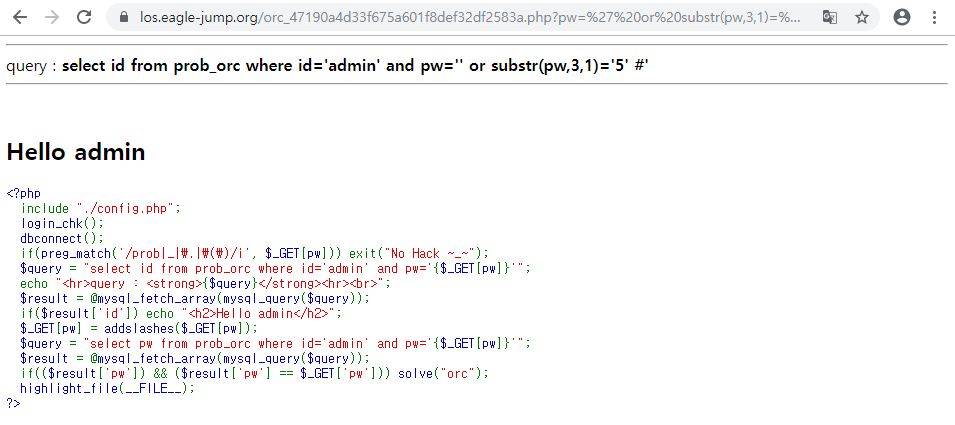
?pw=%27%20or%20substr(pw,@,1)=%27\*%27%20%23 의 코드에서 @에는 각 자리 숫자, \*에는 확인할 변수의 값을 넣어 8자리 pw 값을 찾아낸다.



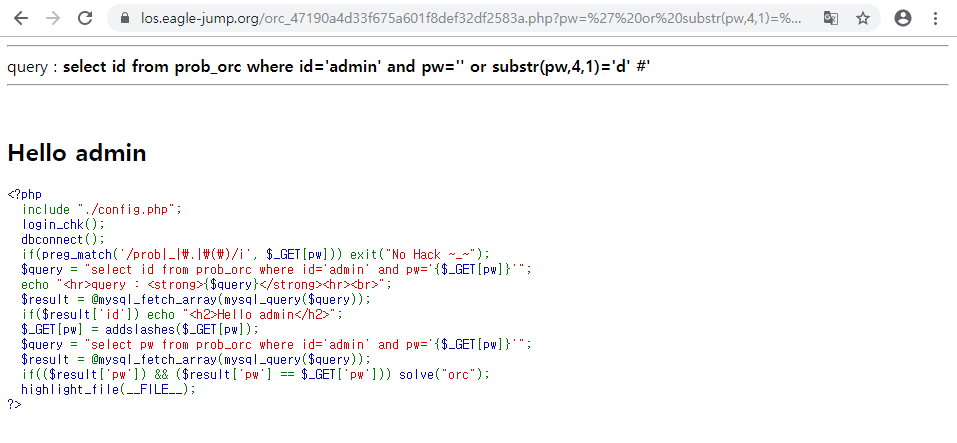
첫 번째 자리 값: 2



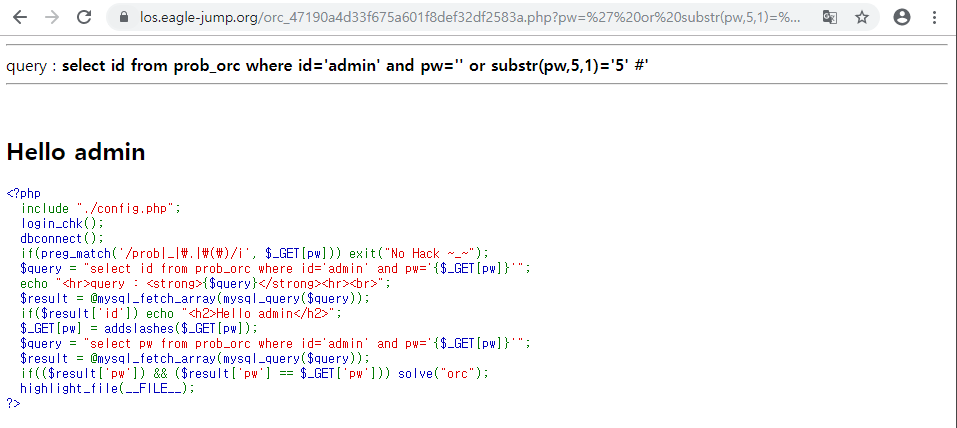
두 번째 자리 값: 9



세 번째 자리 값: 5



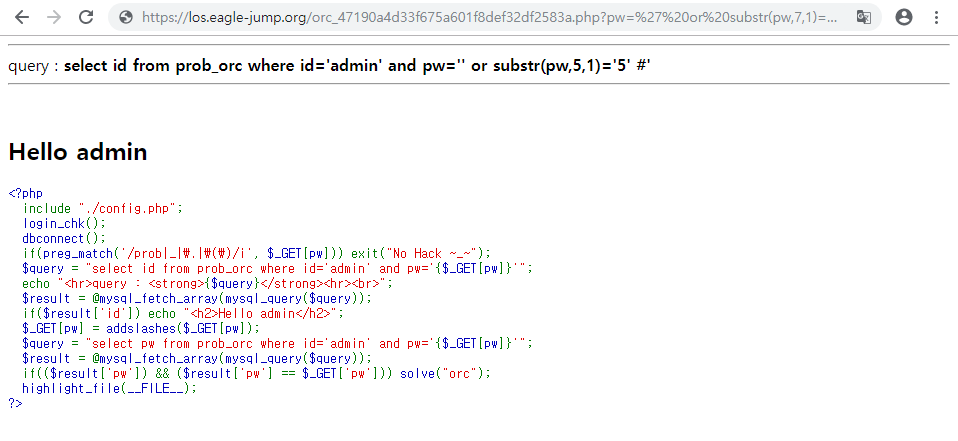
네 번째 자리 값: d



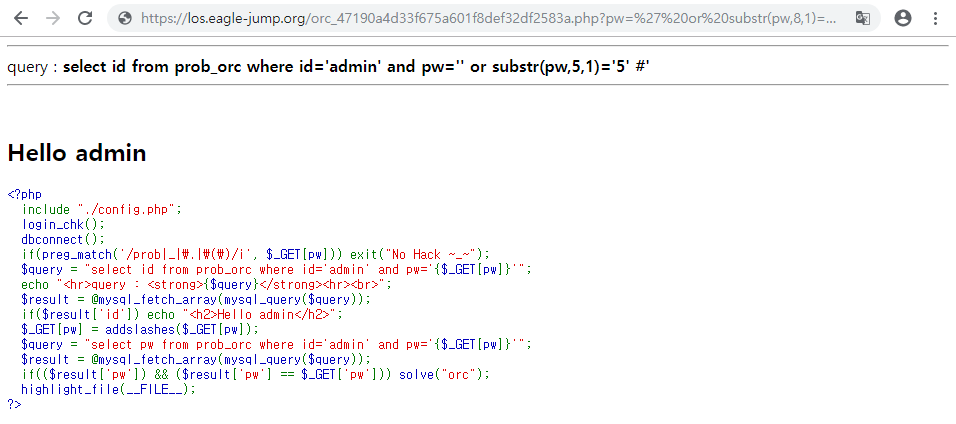
다섯 번째 자리 값: 5



여섯 번째 자리 값: 8

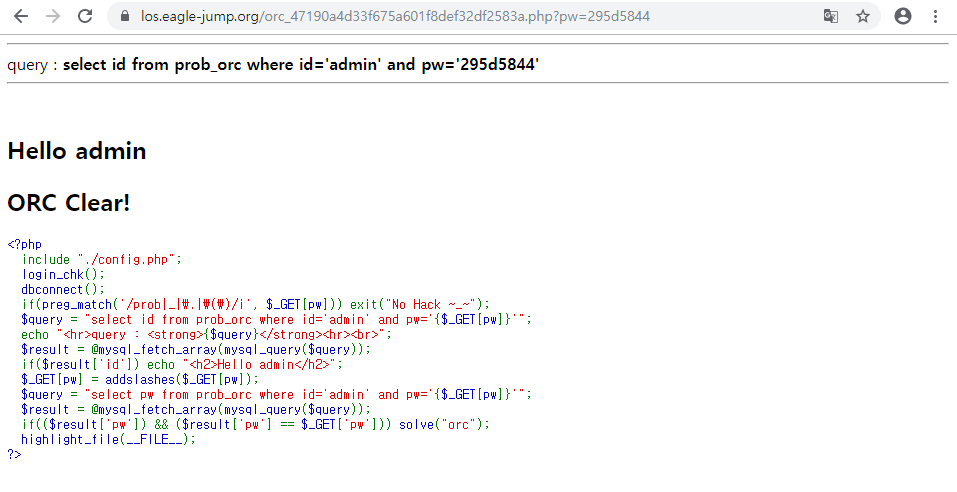


일곱 번째 자리 값: 4



여덟 번째 자리 값: 4

따라서 pw 값을 넣으면



ORC Clear!