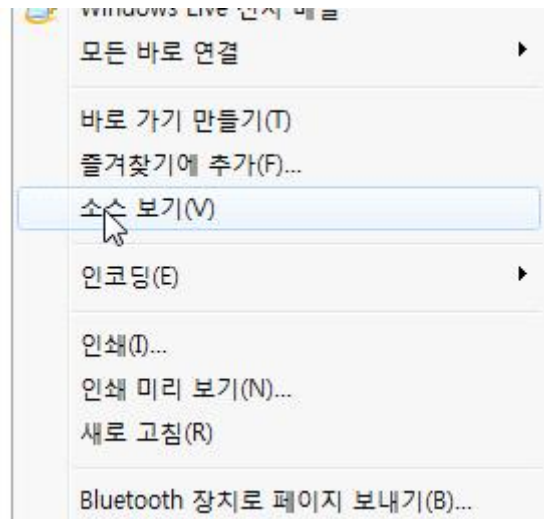


다음과 같은 폼이 있다.

우선 소스를 보자.




아래가 소스이다.

```
<html>
<head>
<title>Challenge 39</title>
</head>
<body>
<!-- index.php -->

<form method=post action=index.php>
<input type=text name=id maxlength=15 size=30>
<input type=submit>
</form>
</body>
</html>
```

index.php로 들어가서 실제 소스를 보자.

 <http://webhacking.kr/challenge/bonus/bonus-10/index.php>

필터링을 거치고 15개의 글자만 뽑아낸다.

```
<html>
```

```
<head>
```

```
<title>Challenge 39</title>
```

```
</head>
```

```
<body>
```

```
<?
```

```
$pw="????";
```

```
if($_POST[id])
```

```
{
```

```
$_POST[id]=str_replace("\\","",$_POST[id]);
```

```
$_POST[id]=str_replace("'", "",$_POST[id]);
```

```
$_POST[id]=substr($_POST[id],0,15);
```

```
$q=mysql_fetch_array(mysql_query("select 'good' from zmail_member where  
id='$_POST[id]"));
```

```
if($q[0]=="good") die("Password is $pw");
```

```
}
```

```
?>
```

```
<form method=post action=index.php>
```

```
<input type=text name=id maxlength=15 size=30>
```

```
<input type=submit>
```

```
</form>
```

```
</body>
```

```
</html>
```

쿼리에 admin ' 를 입력해보자.

A screenshot of a web form. On the left is a text input field with a light gray border, containing the text "admin ". To the right of the input field is a blue button with white text that says "쿼리 전송". A mouse cursor is pointing at the button.

그렇게되면 '(싱글쿼터)'가 ''(더블쿼터)로 바뀌게되어서 admin '' 이 되지만,
15자리까지 끊으므로 admin ' 가 되고, html이므로 공백은 아무리 많아도 한 개로
치게된다.

그에의해 쿼리문은 admin ' 이 되고, 잘못된 쿼리문이 인젝션에 의해 옳게 바뀌면서 답이
출력된다.

Password is 0314c4ff61acd2172fb175b8fbd8e314