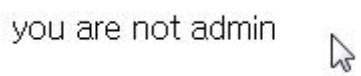
webhacking.kr 웹해킹 가입문제

B1ackZer0
2011.04.04

가입문제를 보면 다음과같은 폼이 있다.
기본값이 admin이다. 쿼리를 전송해보자.

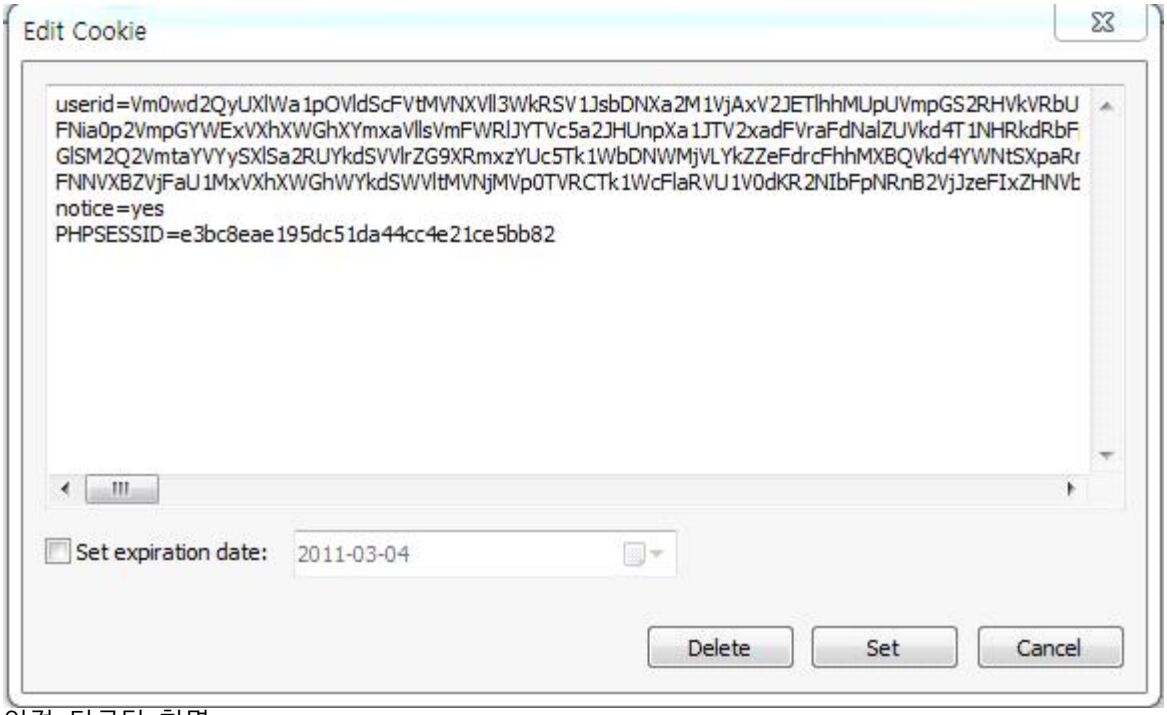
admin이 아니라고 뜬다.



그렇다면 값을 바꿔 쿼리 전송을 해보자.

adin으로 로그인은 되지만 반응은 없다.

쿠키를 보니까 userid에 base64가 있다.
base64 디코딩을 해주자.
하면 할수록 계속 base64가 나오고, 11번 하게 되면 대충
0cc175b9c0f1b6a831c399e2697726618277e0910d750195b448797616e091ad865c0c0b4ab0e063e5caa3387c1a87417b8b965ad4bca0e41ab51de7b31363a1d41d8cd98f00b204e9800998ecf8427e
이런 값이 나온다.
(admi으로 입력했을시)
md5같아 보인다. 32자리로 끊어보자.
0cc175b9c0f1b6a831c399e269772661
8277e0910d750195b448797616e091ad
865c0c0b4ab0e063e5caa3387c1a8741
7b8b965ad4bca0e41ab51de7b31363a1
d41d8cd98f00b204e9800998ecf8427e



이걸 디코딩 하면,
각각 a,d,m,i,알수없는 md5가 나온다.

대충 유추해봤을때 넣은 값+알수없는md5를 11번 base64인코드한 값이 쿠키에 저장되는 것같다.
여러 시도를 해본 결과, admi가 아닌 다른 값을 넣어도 넣은 값+알수없는md5를 11번 base64인코드한 값이 쿠키에 저장된다.
자, 그러면 역으로, admin+알수없는md5를 11번 base64인코드해서 쿠키에 넣어보자.
이렇게 admin으로 로그인이 되고, 회원가입을 할 수 있다.