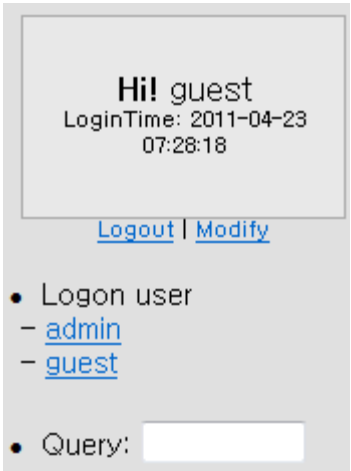
wowhacker webgame 4번문제

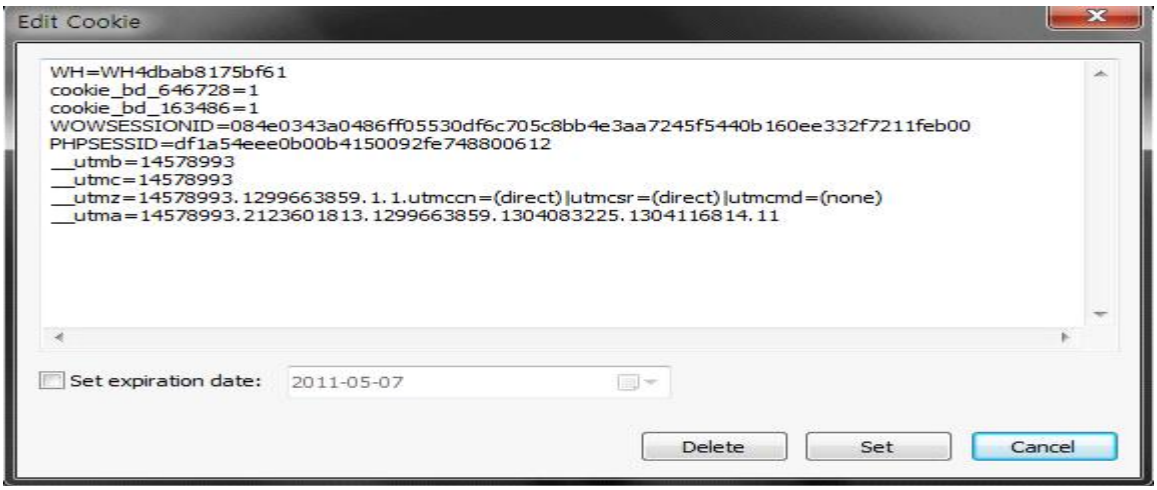
B1ackZer0
2011.04.29

다음과 같은 폼과 Notice가 보인다.

다음은 Notice의 2번대로 guest/guest로 로그인했을때의 모습이다.

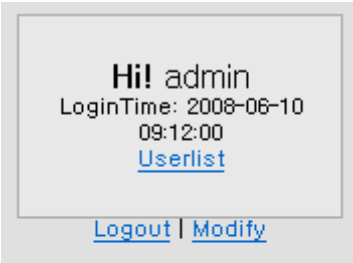


WOWSESSIONID에 md5로 예상되는 문자가 있다.
WOWSESSIONID가 64자이므로 32자로 나누어 디코드를 해본다.
그러면 guest/디코드불가 가 나온다.
계속 시간을 바꾸며 로그인을 해본 결과, 뒤쪽의 디코드불가 md5는 계속 변하는것을 알았다.
Login Time을 타임스탬프시켜 디코드해본결과 뒤쪽의 md5와 맞아떨어졌고, guest/로그인시간 타임스탬프 md5 라는 공식이 성립했다.
그렇다면 WOWSESSIONID=아이디/로그인시간 타임스탬프 md5 이다.
그렇다면 우리는 admin/admin의 로그인 시간 타임스탬프 md5 를 WOWSESSIONID에 넣으면 된다.



Notice에 1.Open! 이라는 글을 쓴 시간이 보인다.
글을 쓰려면 로그인을 해야한다고 생각했고, 그렇다면 1.Open! 이라는 글을 쓴 시간인 2008.06.10 09:12:21 이전에 로그인을 했다고 생각했다.
그래서 그때부터 1초씩 감소시키면서 타임스탬프 md5를 해서 넣어보았다.

계속 하다가 2008.06.10 09:12:00 의 타임스탬프 md5가 admin이 로그인한 시간이란걸 알아냈다.
21232f297a57a5a743894a0e4a801fc367c90cd08d7a3d88f90e63fe768f5a8c 이 admin/admin의 로그인시간 타임스탬프 md5 값이다.
위의 값을 WOWSESSIONID에 넣으면 다음과 같이 admin으로 로그인된다.



한번 Userlist를 보자.

패스워드를 얻었고 인증에 성공했다.

```
guest:guest
admin:nologin
level4:VeRY Good! My Friend!
```