webhacking.kr 53번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-03
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

다음과 같이 hello world만 출력된다.

hello world

소스를 보면 index.phps를 가르킨다.

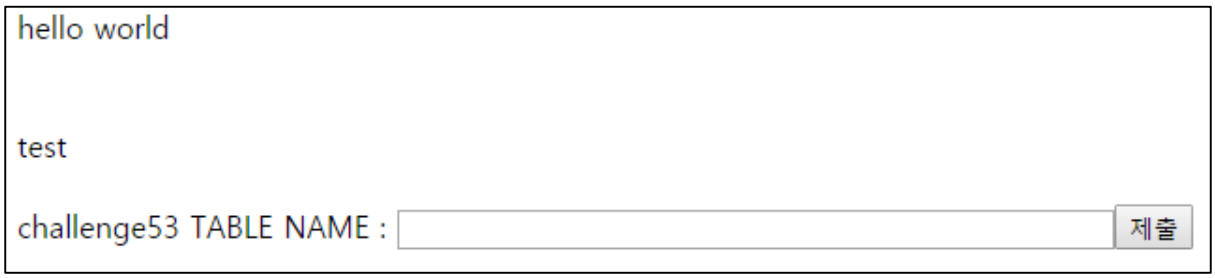
다음은 index.phps의 소스이다.

```php
<?

if(time()<1260615600) exit();
$hidden_table="????";
if($_GET[answer]==$hidden_table)
{
@solve();
exit();
}
if(eregi("union",$_GET[val])) exit();
if(eregi("select",$_GET[val])) exit();
if(eregi("from",$_GET[val])) exit();
if(eregi("/",$_GET[val])) exit();
if(eregi("\*",$_GET[val])) exit();
if(eregi("#",$_GET[val])) exit();
if(eregi("-",$_GET[val])) exit();
if(eregi(",",$_GET[val])) exit();
if(eregi("=",$_GET[val])) exit();
if(eregi("!",$_GET[val])) exit();
if(eregi("\|",$_GET[val])) exit();
if(eregi("by",$_GET[val])) exit();
$f=@mysql_fetch_array(mysql_query("select test1 from $hidden_table where
test2=$_GET[val]"));
echo($f[0]);
if($f)
{
echo("<br><br><form method=get action=index.php>challenge53 TABLE NAME : <input type=text
name=answer size=50><input type=submit></form>");
}
?>
```

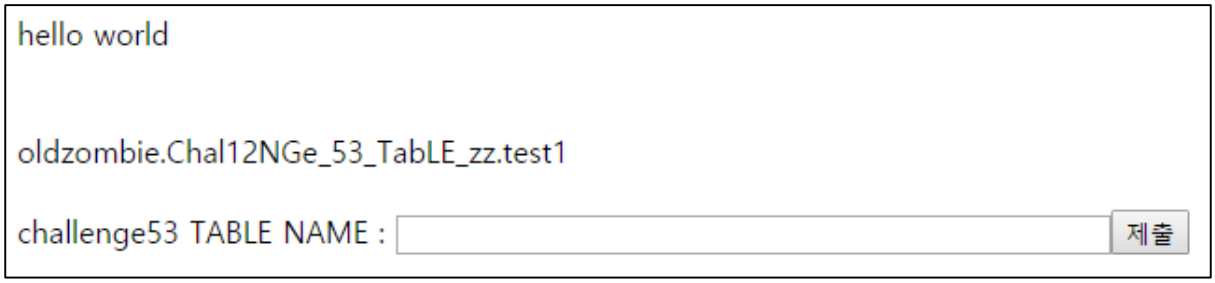
소스를 보면 쿼리문에 GET형식으로 val값을 넘겨주는 부분이 있다.

1을 넘겨주니 다음처럼 test와 입력 창이 나왔다.



그러다가 procedure analyse()라는 함수를 알게 되었다.
이는 테이블 속의 데이터를 분석해서 알려준다.
다음과 같은 값을 보내보았다.
?val=1 procedure analyse()

그러면 다음처럼 테이블 명을 알려준다.



Chal12NGe_53_TabLE_zz 를 테이블 이름으로 제출하면 클리어된다.