webhack.teamtmp 2 번문제

Xero
박준혁 (한국디지털미디어고등학교 2 학년)
2012-06-04
wnsgurzxc@nate.com

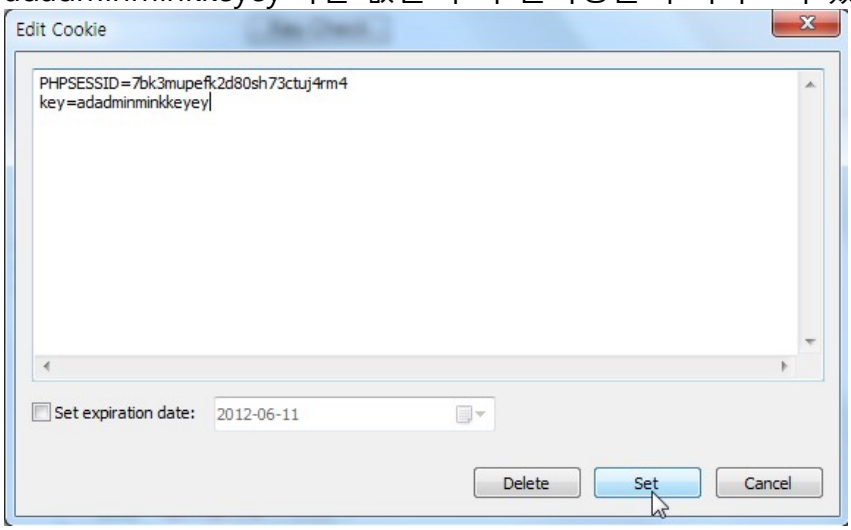
다음과 같이 php 소스를 보여준다.

Key Check

'' and '' : incorrect key

```
<html>
<title>Level 2</title>
<form method="post" action="index.php">
    <input type="text" name="key">
    <input type="submit" value="Key Check">
</form>
</html>
<?php
    extract($_COOKIE);
    $key=$_POST[key];
    $key=str_replace("admin","",$key);
    $key=str_replace("key","",$key);
    $key2=$_COOKIE[key];
    $key2=str_replace("admin","",$key2);
    $key2=str_replace("key","",$key2);
    if($key=="adminkey" && $key2=="adminkey")
    {
        echo "<br><br>PW : ????";
    }
    else
    {
        echo "'$key' and '$key2' : incorrect key";
    }
?>
```

소스를 해석해 보면 POST 형식으로 전달되는 key 값과 cookie 의 key 값을 필터링하고 필터링한 값이 adminkey 라는 값이면 답을 출력한다.
다음과 같이 우선 cooxie 툴바를 이용해 cookie 에 key 변수를 만들어 adadminminkkeyey 라는 값을 주어 필터링을 우회하도록 했다.



그리고 다음과 같이 POST 로 전달되는 key 값도 adadminminkkeyey 값을 주었다.

adadminminkkeyey Key Check

'adminkey' and '' : incorrect key

```
<html>
<title>Level 2</title>
<form method="post" action="index.php">
    <input type="text" name="key">
    <input type="submit" value="Key Check">
</form>
</html>
<?php
    extract($_COOKIE);
    $key=$_POST[key];
    $key=str_replace("admin","",$key);
    $key=str_replace("key","",$key);
    $key2=$_COOKIE[key];
    $key2=str_replace("admin","",$key2);
    $key2=str_replace("key","",$key2);
    if($key=="adminkey" && $key2=="adminkey")
    {
        echo "<br><br>PW : ????";
```

그러자 다음과 같이 패스워드가 나왔다.

Key Check

PW : 2a3afc9027a6f19cc3a8b2428be5003c

Key : 2a3afc9027a6f19cc318b2428be5003c