webhack.teamtmp 19 번문제

Xero
박준혁 (한국디지털미디어고등학교 2 학년)
2012-06-05
wnsgurzxc@nate.com

다음과 같이 php 소스가 보인다.

No

```
if($_POST[pst]=="pos₩tme")
{
        echo("PW : $pw");
}else{
        echo("No");
}
```

POST 형식으로 pst 변수에 "pos₩tme" 값이 전달되면 답을 출력한다.
파로스로 잡아보면 다음과 같이 GET 형식으로 잡히는 것을 볼 수 있다.

```
GET http://webhack.teamtmp.org/level19/index.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://webhack.teamtmp.org/allprob.php
Accept-Language: ko-KR
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0) Paros/3.2.13
Host: webhack.teamtmp.org
Proxy-Connection: Keep-Alive
Cookie: PHPSESSID=fip9vluearbp23v2aljhgtgs96
```

POST 형식으로 전달하기 위해 다음과 같이 GET 을 POST 로 바꾸고 Content-Type: application/x-www-form-urlencoded 를 추가하고 pst 변수에 pos me 값을 전달하였다.

Request | Response

```
POST http://webhack.teamtmp.org/level19/index.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://webhack.teamtmp.org/allprob.php
Accept-Language: ko-KR
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0) Paros/
3.2.13
Host: webhack.teamtmp.org
Proxy-Connection: Keep-Alive
Pragma: no-cache
Cookie: PHPSESSID=janeva5fl00d90vbg3et2kfms1

pst=pos me
```

그러자 다음과 같이 답이 출력되었다.

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=euc-kr">
<title>Level 19</title>
</head>

PW : 23cf809ce3a0da9e39fc215440951d61<html>
</center>
<hr>
<pre>
if($_POST[pst]=="pos\tme")
{
        echo("PW : $pw");
}else{
        echo("No");
}
```

Key : 23cf809ce3a0da9e39fc215440951d61