

webhack.teamtmp 3 번문제

Xero

박준혁 (한국디지털미디어고등학교 2 학년)

2012-06-04

wnsgurzxc@nate.com

폼 하나가 주어지고 Hint 로 Source View 와 Cookie 를 이용하라고 한다.

ID:

Auth

Hint : Source View/Cookie

Thanks to imslow

소스를 보니 또 hint 로 @dmin 으로 auth 를 하라고 한다.

```

<head>
<meta http-equiv="Content-Type" content="text/html; charset=euc-kr">
<title>Level 3</title>
</head>

<!-- hint: @dmin으로 auth하세요 -->
<form action="/level3/index.php" method="post" name="login" id="login">
ID: <input type="text" name="uid" maxlength="5" width="5" /><br />
<input type="submit" value="Auth" /><br><br>Hint : Source View/Cookie<br><br>Thanks to imslow
</form>

```

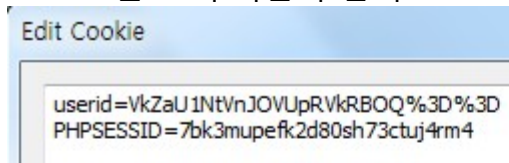
@dmin 으로 auth 를 하니 Access Denied!가 뜨며 auth 되지 않았다.
Access Denied!

ID:

Hint : Source View/Cookie

Thanks to imslow

Cookie 를 보니 다음과 같이 userid 에 base64 암호 같아 보이는 값이 있었다.



URL 인코딩이 되어 있기에 URL 디코드를 하고 base64 디코드를 4 번 하니 입력한 값이 나왔다.

결국 값을 넣고 auth 를 하면 쿠키에 넣은 값의 base64 인코딩 4 번 한 값이 들어간다는 것을 알 수 있다.

거꾸로 @dmin 을 base64 인코딩을 4 번 하여 cookie 에 넣으니 다음과 같이 답이 출력되었다.

Congratulation!
 Keycode is 69601f5f57b37e14b64cf38d2e5a1c4d

Key : 69601f5f57b37e14b64cf38d2e5a1c4d