<Webhacking 4번 & 32번> 김수현

4번 문제를 클릭해서 들어가면 이상한 문자열이 나와있는 걸 확인할 수 있다. 하지만 저 문자열이 무엇을 의미하는 지는 모르기 때문에 view-source 를 통해 파악해야 될 것 같다고 생각했다.


```php
<?php
  include "../../config.php";
  if($_GET['view-source'] == 1) view_source();
?><html>
<head>
<title>Challenge 4</title>
<style type="text/css">
body { background:black; color:white; font-size:9pt; }
table { color:white; font-size:10pt; }
</style>
</head>
<body><br><br>
<center>
<?php
  sleep(1); // anti brute force
  if((isset($_SESSION['chall4'])) && ($_POST['key'] == $_SESSION['chall4'])) solve(4);
  $hash = rand(10000000,99999999)."salt_for_you";
  $_SESSION['chall4'] = $hash;
  for($i=0;$i<500;$i++) $hash = sha1($hash);
?><br>
<form method=post>
<table border=0 align=center cellpadding=10>
<tr><td colspan=3 style=background:silver;color:green;><b><?=$hash?></b></td></tr>
<tr align=center><td>Password</td><td><input name=key type=text size=30></td><td><input type=submit></td></tr>
</table>
</form>
<a href=?view-source=1>[view-source]</a>
</center>
</body>
</html>
```

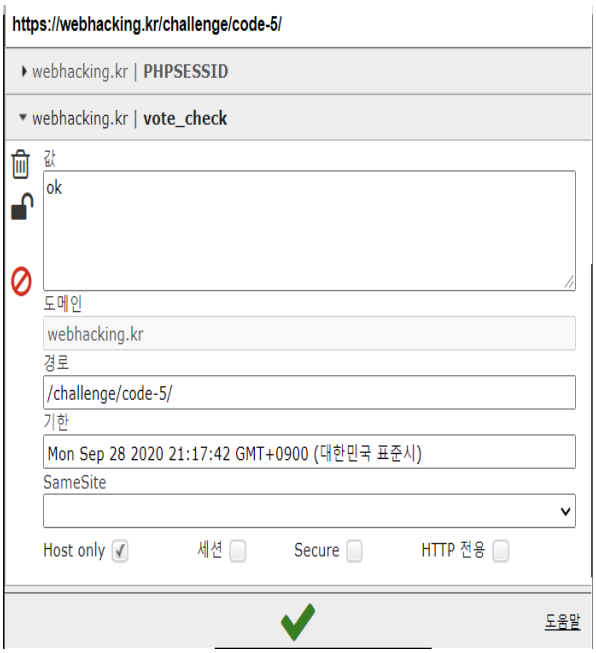
일단, <?php 가 있는 자리가 주요 포인트라고 생각했다. 그리고 코드를 하나 하나씩 뜯어 생각해보고, 구글링을 해보니 hash 변수에 10000000부터 99999999까지의 임의의 랜덤 값에 salt_for_you를 붙인 값을 저장해야 한다는 생각이 들었다. 그러면 10000000salt_for_you ~ 99999999salt_for_you 중 하나가 hash에 대입이 되는 것이다. 그런 다음, sha1 함수에 hash 변수를 넣고 500번 실행하고 500번 실행된 값을 출력해야 한다. 하지만 막상 위와 같이 하려고 하니까 의문이 생겼다. 어떻게 500번을 실행해야 하지..?? 인터넷에 sha1함수를 암호화 해주는 사이트에 들어가서 해보려고 했지만 500번을 해야 되는데에 있어서 중간에 하다가 결국 하지 못했다.

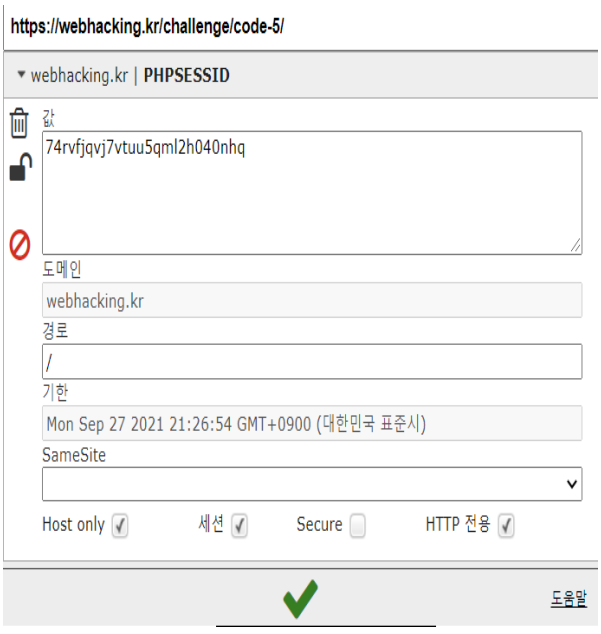
-32번-

이번 문제는 무슨 랭킹이 엄청 길게 늘어져 있는데 클릭할 때마다 순위가 바뀌는 것을 보고 쿠키와 관련된 문제라고 생각이 들었다. 하지만 거기까지였다.

RANK	NAME	Hit
1	nego	52 / 100
2	yunaseol	41 / 100
3	ImUB	29 / 100
4	bona0124	28 / 100
5	yd0384	27 / 100
6	kaka08	27 / 100
7	coals91	25 / 100
8	sunchoi	25 / 100
9	ww0jeff	25 / 100
10	dhw6801	24 / 100
11	chiduc97z	17 / 100
12	hyoseon94	16 / 100
13	in_reason	15 / 100
14	whc8862	14 / 100
15	GODYYT1	14 / 100
16	omh9805	14 / 100
17	tarunkant	13 / 100
18	ReGenToK	13 / 100
19	wlrnjs95	12 / 100
20	dkdldjtm	12 / 100
21	junhe2584	12 / 100
22	inpereal	11 / 100
23	dino7000	11 / 100
24	azazel02	11 / 100

한번 투표를 한 순간 위와 같은 창이 뜬다. 이미 한번 투표했다는 창이다. 다른 사람들은 자신의 아이디가 몇 등에 있는 지 찾았다고 하는데 내 아이디는 찾지 못했다. 그래도 쿠키 창은 확인해 보았다.





첫번째 사진은 투표를 하고 난 후 쿠키 창을 확인해본 결과이다. 쿠키의 값이 ok로만 떠있는 걸 확인할 수 있다. 혹시 몰라서 체크버튼을 누르고 새로고침하고 했더니 유효하지 않은 값이라고 떠서 다시 로그인을 하고 들어가서 쿠키 값을 확인해보았다. 그랬더니 쿠키 값이 이상한 문자열의 값으로 바뀌어져 있는 것을 확인할 수 있었다. 하지만 이걸 어떻게 확인해야 할 지 몰라서 여기까지만 생각하였다. 도대체 어떻게 접근해야 풀 수 있는 지 잘 모르겠다. 너무 어렵다.