[webhacking.kr] old-44

name : submit

view-source

문제에 주어진 사이트 화면은 위와 같고, view-source를 누르면 php 소스코드가 나온다.

```
<?php
  if($_GET['view_source']){ highlight_file(__FILE__); exit; }
?><html>
<head>
<title>Challenge 44</title>
</head>
<body>
<?php
  if($_POST['id']){
    $id = $_POST['id'];
    $id = substr($id,0,5);
    system("echo 'hello! {$id}'"); // You just need to execute ls
  }
?>
<center>
<form method=post action=index.php name=htmlfrm>
name : <input name=id type=text maxlength=5><input type=submit value='submit'>
</form>
<a href=./?view_source=1>view-source</a>
</center>
</body>
</html>
```

소스코드에는 system 함수 옆에 ls를 실행시키라는 힌트가 나와 있다.

---

hello! flag_29cbb98dafb4e471117fec409148e9386753569e index.php

';ls'를 id에 입력하면 ls의 결과가 출력되어서 index.php와 다른 파일을 찾아냈다.

FLAG{y2u.be/sW3RTOtFO2O}

url에 index.php 대신 위 파일 이름을 입력해서 flag를 찾을 수 있었다.