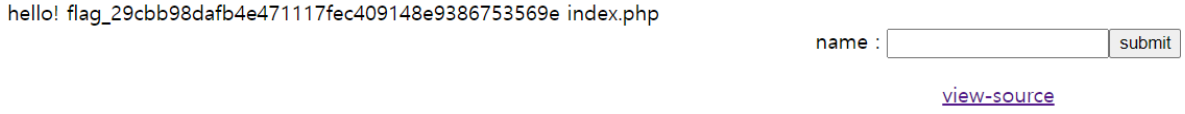
[webhacking.kr] old 44

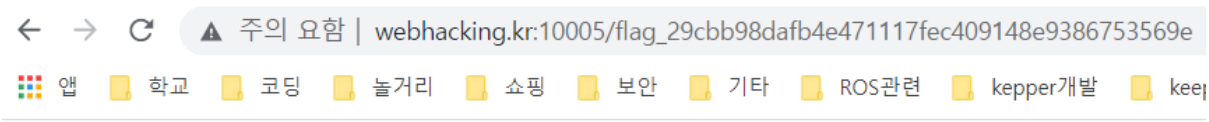
첫 화면

```
<?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>
```

소스코드를 보면 너무 간단하다 id 값을 5바이트로 제한해서 입력받고 그걸 system함수에서 echo에 넣어서 보여준다 '이거로 hello를 닫고 ;이거로 ls를 연달아 실행시킨 후 뒤의 '를 닫아주면 된다 즉 ';ls'를 입력하면 된다.



그러면 위와 같은 결과가 나온다. 딱 봐도 flag뭐시기 하는 파일에 flag값이 있어 보인다. url창에 저 파일명을 넣어보면



Flag가 나온다

FLAG{y2u.be/sW3RTOtFO2O}