HGAME WEEK1 (seadom)

WEB3: very easy web

真的 easy`````` QAQ

1. 百度“CTF WEB 代码审计”并点进其中一个结果，发现相似题型：

八、PHP大法

1、打开题目发现：Can you authenticate to this website? index.php.txt

构造url：http://ctf5.shiyanbar.com/DUTCTF/index.php.txt

得到php代码

```
<?php
if(eregi("hackerDJ",$_GET[id])) {
  echo("<p>not allowed!</p>");
  exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
  echo "<p>Access granted!</p>";
  echo "<p>flag: *****************} </p>";
}
?>
```

2、对输入的id进行url解码，如果解码的结果是hackerDJ就可以得到flag

因为地址栏会自动进行一次url解码，所以需要对hackerDJ进行两次url编码，然后构造url：

http://ctf5.shiyanbar.com/DUTCTF/index.php?

id=%25%36%38%25%36%31%25%36%33%25%36%62%25%36%35%25%37%32%25%34%34%25%34%61

```php
$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "vidar")
{
  echo $flag;
}
```

2. 跟着例子操作，得到 flag。