原生类与$a($b)

Eval(echo new $a($b))可以使用原生类进行构造从而输出flag的值。

什么是原生类？原生类就是php内置类，不用定义php自带的类，即不需要在当前脚本写出，但也可以实例化的类

1）遍历文件的原生类

<?php

$a = new DirectoryIterator("glob://f\*");

echo $a;

以上是经常使用的DirectoryIterator类，可以配合glob伪协议遍历目录里的文件

如果想显示所有的文件可以用foreach函数来遍历，比如

<?php

$a = new DirectoryIterator("/");

foreach($a as $f){

echo($f.'<br>');

}

DirectoryIterator类：里面包含\_\_tostring

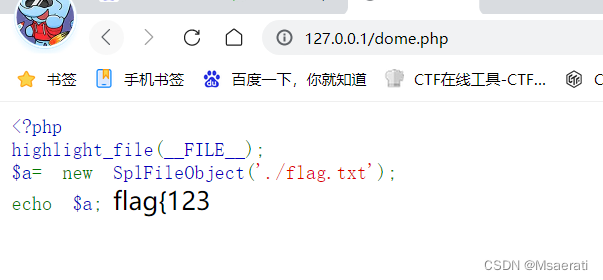
当执行echo函数时 会触发\_\_toString()方法，输出指定目录里面经过排序之后的第一个文件名

说人话：echo能输出文件名

1. 输出文件的原生类

SplFileObject

当用文件目录遍历到了敏感文件时，可以用SplFileObject类，同样通过echo触发SplFileObject中的\_\_toString()方法。



也可以通过SplFileObject类以及联合伪协议进行读取。php://filter

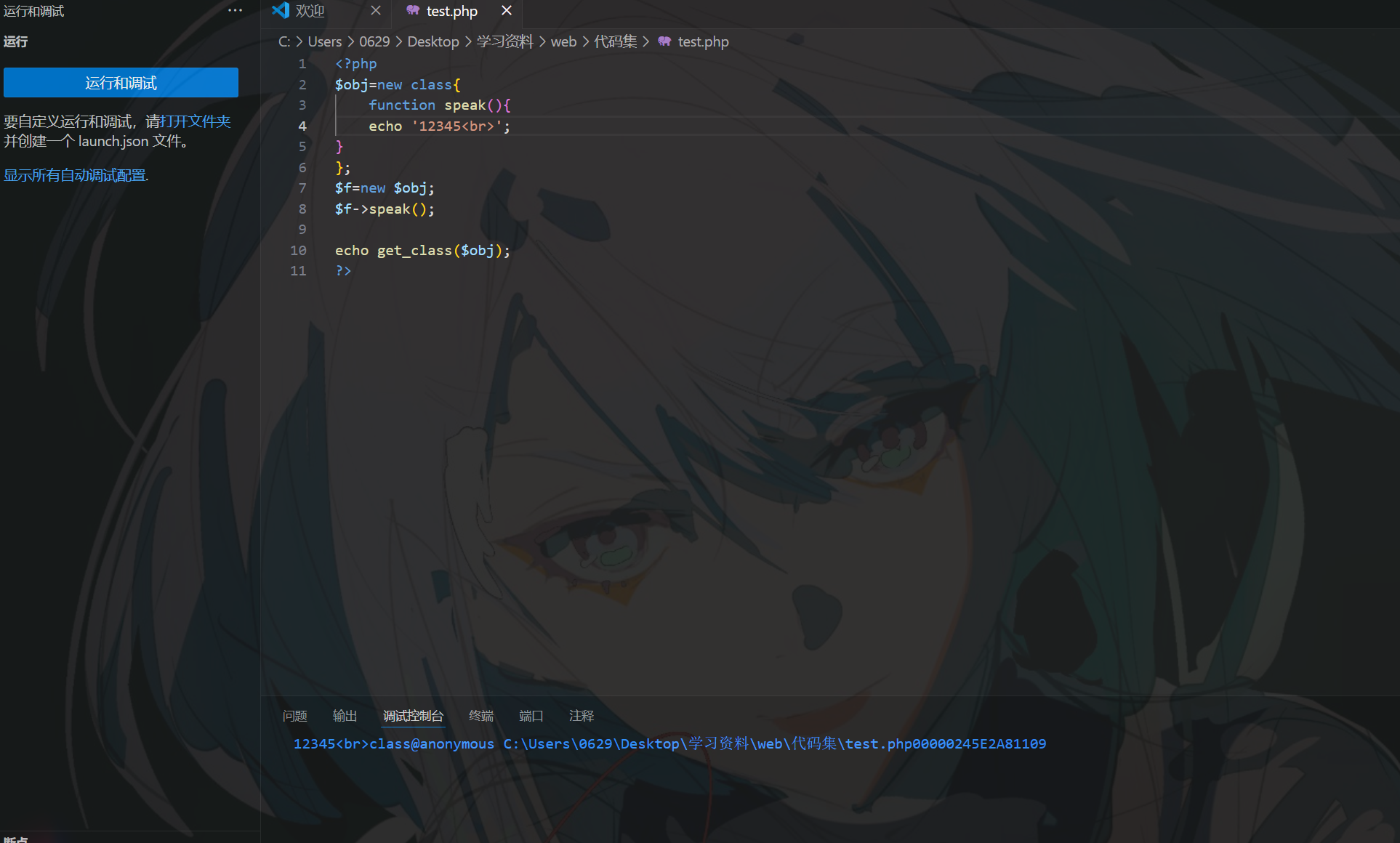
匿名类

New class{args1，args2，func1，func2}

echo get\_class($obj);

可以看出类名与文件所在行列相关,即同一个位置实例出来的类为同一个类.

即class@anonymous 文件路径+行数$列数



例题见红明谷2024ezphp