1、知识点

知识点	说明
extract()	使用数组键名作为变量名，使用数组键值作为变量值
file_get_contents()	把文件的内容读入到一个字符串中

2、源码

```
<?php

$flag='xxx';
extract($_GET);
 if(isset($shiyan))
 {
    $content=trim(file_get_contents($flag));
    if($shiyan==$content)
    {
        echo'ctf{xxx}';
    }
   else
   {
    echo'Oh.no';
   }
   }

?>
```

3、分析

1）通过GET接收用户传入的参数，并使用extract函数将传入的键作为变量名，值作为变量值。

2）如果设置了$shiyan变量，就将$flag文件中的内容作为字符串返回给$content。

3）最后比较$shiyan和$content的值是否相等，相等即返回flag。

4）此时$shiyan是没有被定义，需要我们通过GET传入；$content是从$flag中得到的，我们也可以通过GET传入。也就是说，需要通过GET传入shiyan和flag参数。

5）那么这里的判断是shiyan和flag文件中的内容相等。服务器中的文件我们并不了解，如果这里如果$flag的值为空，或者为其他值，$content读取到的就是空值；然后定义shiyan参数的值也为空，经过判断后，就会输出flag。

4、利用

```
?shiyan=&flag=x
```